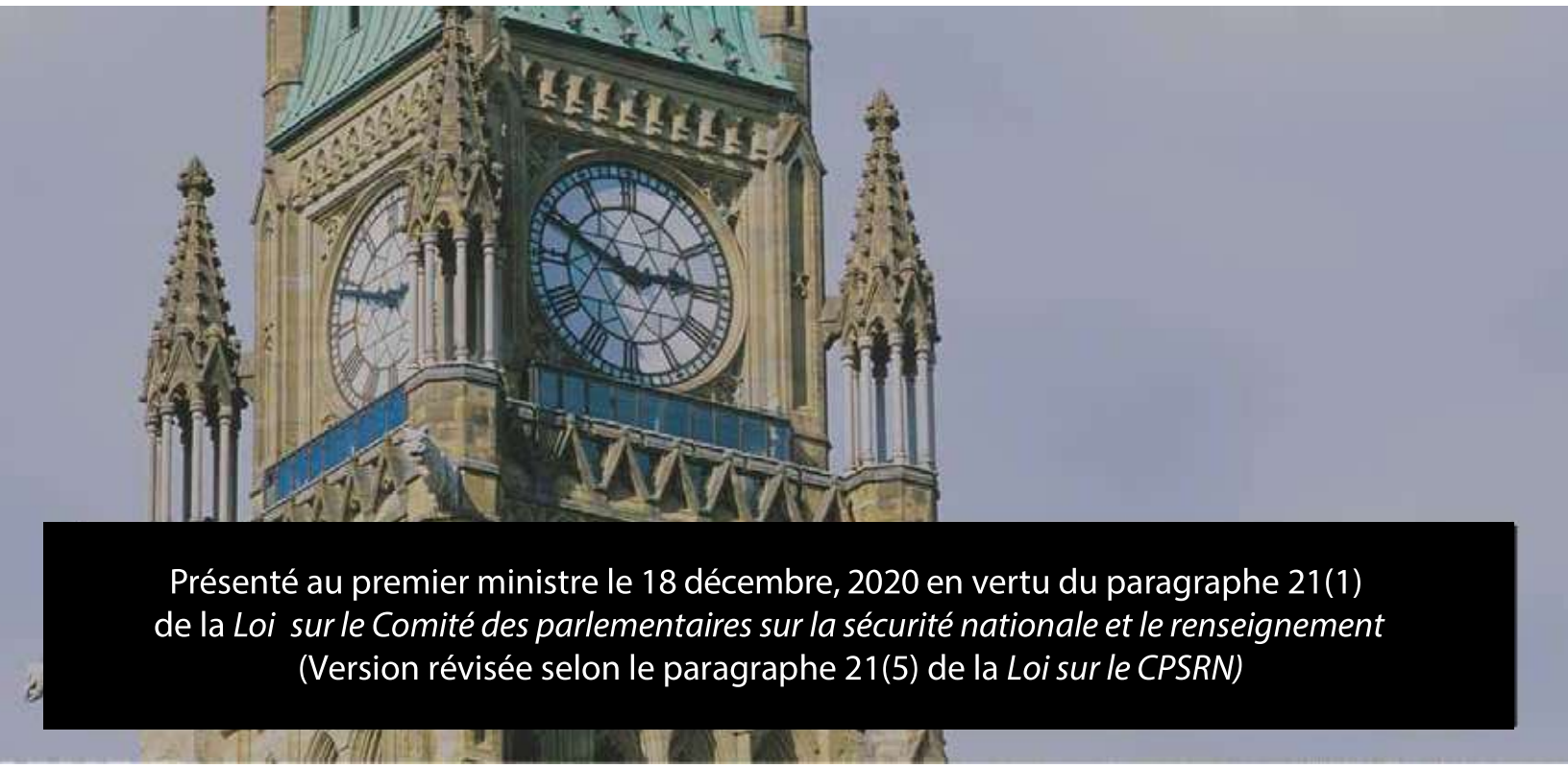
Le Comité des parlementaires sur la sécurité nationale et le renseignement

Rapport annuel 2020



Présenté au premier ministre le 18 décembre, 2020 en vertu du paragraphe 21(1) de la *Loi sur le Comité des parlementaires sur la sécurité nationale et le renseignement*
(Version révisée selon le paragraphe 21(5) de la *Loi sur le CPSRN)*

Canada

Ottawa, ON.

Le Comité des parlementaires sur la sécurité nationale et le renseignement

Rapport annuel 2020 (Version révisée selon le paragraphe 21(5) de la Loi sur le CPSNR)
CP100F (Imprimé)
ISSN 2562-5128 (Imprimé)

CP100F-PDF (En ligne)
ISSN 2562-5136 (En ligne)

RAPPORT ANNUEL 2020

Le Comité des parlementaires sur la sécurité nationale et le renseignement

L'honorable David McGuinty, C.P., député
Président

Présenté au premier ministre le 18 décembre 2020
Version révisée déposée au Parlement en mars 2021

Révisions

En application du paragraphe 21(1) de la *Loi sur le Comité des parlementaires sur la sécurité nationale et le renseignement* (Loi sur le CPSNR), le Comité doit présenter au premier ministre un rapport annuel. Conformément au paragraphe 21(5) de la Loi sur le CPSNR, le premier ministre peut, après consultation du président du Comité, ordonner au Comité de lui présenter un rapport révisé qui ne contient pas de renseignements dont la communication porterait atteinte à la sécurité ou à la défense nationales ou aux relations internationales, ou qui sont protégés par le secret professionnel de l'avocat, selon le premier ministre.

Le présent document constitue une version révisée du Rapport annuel fourni au premier ministre le 18 décembre 2020. Les révisions ont été apportées de façon à retirer l'information dont la communication, selon le premier ministre, porterait atteinte à la sécurité ou à la défense nationales ou aux relations internationales ou qui est protégée par le secret professionnel de l'avocat. Lorsque la suppression n'affecte pas la lisibilité du texte, le Comité a signalé la suppression par trois astérisques (***) dans le texte du présent document. À l'inverse, le Comité a révisé le document pour résumer l'information retirée. Ces passages sont signalés par trois astérisques au début et à la fin du résumé et sont placés entre crochets (voir l'exemple ci-dessous).

EXEMPLE: [*** Les passages révisés sont signalés par trois astérisques en début et en fin de phrase, et le résumé est placé entre crochets. ***]

Message du président

Ottawa (Ontario) – 18 décembre 2020

La dernière année fut marquée par les défis et l'adaptation pour le Comité, l'appareil de la sécurité nationale et du renseignement, le gouvernement, les Canadiens et les citoyens du monde entier. La pandémie a eu une incidence importante sur tous les aspects de nos vies, mais nous continuons de persévérer.

Ce rapport annuel – notre troisième – est un exemple de cette persévérance.

Le Comité a été reconstitué en février 2020 à la suite de sa dissolution avant les élections fédérales de 2019. Nous avons accueilli de nouveaux membres de tous les partis et groupes reconnus des deux chambres du Parlement. Au cours des semaines suivant leur nomination, les nouveaux membres se sont consacrés à en apprendre plus sur le monde complexe de la sécurité et du renseignement et à se familiariser avec les examens antérieurs du Comité. Ensemble, les nouveaux et les anciens membres ont démontré leur dévouement envers le mandat du Comité et ont mis de côté leurs divergences partisanes pour travailler sur des questions ayant une incidence sur la sécurité et les droits de tous les Canadiens.

En mars 2020, le Rapport spécial sur la collecte de renseignements sur les Canadiens par le ministère de la Défense nationale et les Forces armées canadiennes ainsi que le Rapport annuel 2019 du Comité ont été déposés devant le parlement. Ces rapports démontrent la capacité du Comité d'étudier des questions complexes et sensibles. Nous espérons que nos conclusions et nos recommandations contribueront à renforcer la responsabilisation et l'efficacité de l'appareil de la sécurité et du renseignement. Dans ce contexte, le Comité a été encouragé de voir le premier ministre demander aux ministres de la Sécurité publique et de la Protection civile, et de la Défense nationale de mettre en place un nouveau cadre régissant les activités de renseignement de défense, conformément aux recommandations formulées par le Comité en 2018 et en 2019.

Au cours des jours suivant le dépôt du Rapport annuel 2019 et du Rapport spécial, un arrêt des activités à l'échelle nationale est entré en vigueur en vue « d'aplatir la courbe » de la COVID-19. Nos activités ont été restreintes et notre plan de travail a été interrompu pendant les premières semaines de la pandémie en raison des contraintes liées à la distanciation physique et aux rassemblements. Le Comité est demeuré en contact de manière régulière et a saisi des occasions d'engagement sécuritaires, comme participer à des balados au Canada et à l'étranger pour discuter des examens du Comité. Le Comité se réjouit de voir plus de renvois à ses rapports dans les médias, chez les universitaires et au Parlement; nous croyons que cela permettra aux Canadiens de mieux comprendre l'appareil de la sécurité et du renseignement, et les défis auxquels il fait face.

Depuis septembre, le Comité a recommencé à tenir des réunions régulières, mais à un nouveau rythme et à l'aide de différents supports. Le Rapport annuel 2020 est différent des rapports précédents. Même si les membres du Comité avaient convenu de réaliser deux examens importants en 2020, au sujet des activités d'Affaires mondiales Canada liées à la sécurité nationale et au renseignement ainsi que des activités et du cadre du gouvernement visant à protéger ses systèmes et ses réseaux contre les cyberattaques, ces examens ne seront terminés qu'en 2021. Actuellement, nous examinons activement les documents et nous organisons des séances d'information et des audiences avec les ministères et organismes concernés, ainsi qu'avec des universitaires et de la société civile.

Par conséquent, le présent Rapport annuel consiste à faire le point sur l'importante évaluation des menaces lancée par le Comité dans son Rapport annuel 2018. Plus précisément, l'évaluation porte sur les menaces envers le Canada liées au terrorisme, à l'ingérence étrangère et l'espionnage, aux cyberattaques, au crime organisé et aux armes de destruction massive. Malgré les défis que représente l'atténuation des risques liés à la pandémie, les membres dévoués de l'appareil de la sécurité nationale et du renseignement ont fourni des documents pertinents et utiles à la préparation de l'évaluation des menaces. Le Comité tient à les remercier pour leur soutien.

L'avant-propos du Rapport annuel 2019 du Comité portait sur les leçons tirées et les défis du Comité pendant ses deux premières années. En effet, le Comité et l'appareil de la sécurité et du renseignement avaient beaucoup à apprendre sur la nouvelle réalité de l'examen parlementaire. Au cours de la dernière année, des discussions productives avec le conseiller à la sécurité nationale et au renseignement (CSNR) au premier ministre ont aidé à résoudre des défis considérables et très préoccupants auxquels le Comité faisait face en ce qui a trait à l'obtention de renseignements « qui sont liés à l'exercice de son mandat et qui relèvent d'un ministère », comme l'indique le paragraphe 13(1) de la Loi sur le CPSNR. Le Comité est persuadé que le CSNR continuera de jouer un rôle de chef afin de contribuer à l'accès large et sans restrictions du Comité aux renseignements, sauf les exceptions prévues dans la loi.

Enfin, je tiens à remercier sincèrement mes collègues du Comité pour leur dévouement à l'important travail du Comité, et le Secrétariat pour leur dévouement intarissable envers notre travail et pour leur résilience en cette période difficile.

L'honorable David McGuinty, C.P., député
Président
Comité des parlementaires sur la sécurité nationale et le renseignement

LE COMITÉ DES PARLEMENTAIRES
SUR LA SÉCURITÉ NATIONALE ET LE RENSEIGNEMENT

L'honorable David McGuinty, C.P., député (président)

Monsieur Don Davies, député

L'honorable Dennis Dawson, sénateur

Monsieur Ted Falk, député

L'honorable Frances Lankin, C.P., C.M., sénatrice

L'honorable Vernon White, sénateur

Monsieur Glen Motz, M.O.M., député

Madame Christine Normandin, députée
(a démissioné le 20 février 2020)

Madame Jennifer O'Connell, députée

Madame Brenda Shanahan, députée

National Security and Intelligence Committee of Parliamentarians

Comité des parlementaires sur la sécurité nationale et le renseignement

Chair

Président

Mars 2021

Le très honorable Justin Trudeau, C.P., député
Premier ministre du Canada
Bureau du Premier ministre et du Conseil privé
Ottawa (Ontario) K1A 0A2

Monsieur le Premier ministre,

Au nom du Comité des parlementaires sur la sécurité nationale et le renseignement, j'ai le plaisir de vous présenter la version révisée de notre rapport annuel pour 2020. Ce rapport comprend une mise à jour de l'évaluation des menaces à la sécurité nationale, présentée pour la première fois dans le rapport annuel du Comité en 2018. Cet aperçu examine les principales menaces, notamment le terrorisme, l'espionnage et l'ingérence étrangère, les cybermenaces, le crime organisé d'envergure et les armes de destruction massive.

Conformément au paragraphe 21(5) de la *Loi sur le Comité des parlementaires sur la sécurité nationale et le renseignement*, le rapport a été révisé pour en exclure des renseignements dont la communication porterait atteinte à la sécurité ou à la défense nationales ou aux relations internationales ou des renseignements protégés par le secret professionnel de l'avocat.

Je vous prie d'agréer, Monsieur le Premier ministre, l'expression de ma très haute considération.

L'honorable David McGuinty, C.P., député
Président
Comité des parlementaires sur la sécurité nationale et le renseignement

P.O. Box 8015, Station "T" / C.P. 8015, Succursale « T »
Ottawa, Canada K1G 5A6

TABLE DES MATIÈRES

Introduction

1. Le Comité des parlementaires sur la sécurité nationale et le renseignement (le Comité) est heureux de présenter son troisième Rapport annuel au premier ministre. Le style et le contenu du rapport de cette année diffèrent des autres rapports produits par le Comité. Il tient compte des événements sans précédent de 2020 et des contraintes qui en résultent, et marque également le début de la seconde itération du Comité. Le Comité a été reconstitué en février 2020, et le Rapport spécial ainsi que le Rapport annuel 2019 ont été déposés devant le Parlement en mars 2020. Peu de temps après, un confinement à l'échelle nationale a été imposé, ce qui a forcé le Comité à interrompre ses activités en vue de juguler la propagation de la COVID-19. Le Comité a modifié son plan de travail dans les mois qui ont suivi le confinement et a recommencé à tenir des réunions régulières lorsqu'il était sécuritaire de le faire.

Activités du Comité en 2020

2. Conformément à la *Loi sur le Comité des parlementaires sur la sécurité nationale et le renseignement* (la loi sur le CPSNR), la dissolution du Comité a eu lieu en septembre 2019 lors du déclenchement des élections fédérales. En février 2020, le Comité a été reconstitué, et il a accueilli cinq nouveaux membres et quatre anciens membres, qui représentent les principaux partis et groupes reconnus du Sénat et de la Chambre des communes. Entre février et mars 2020, le Comité a tenu sept réunions visant à informer les membres au sujet du mandat du Comité ainsi que des rôles et des pouvoirs des principales organisations de l'appareil de la sécurité et du renseignement. Plusieurs réunions du Comité ont servi à préparer le dépôt des rapports de 2019, notamment pour discuter en profondeur du processus du gouvernement visant à cerner les informations dont la communication porterait atteinte à la sécurité ou à la défense nationale ou aux relations internationales, ou des renseignements protégés par le privilège relatif au litige, et ensuite de déterminer comment retirer ces informations avant le dépôt des rapports. Pendant cette période, le Comité a été en mesure de visiter les bureaux du Service canadien du renseignement de sécurité (SCRS) et de rencontrer des universitaires afin de discuter de questions importantes auxquelles l'appareil de la sécurité nationale et du renseignement fait face. Les nouveaux membres du Comité ont passé du temps supplémentaire, en dehors des réunions régulières, pour se familiariser avec les rapports précédents du Comité et pour en apprendre plus au sujet de la loi régissant le Comité et de ses procédures.

3. Le 12 mars 2020, le gouvernement a déposé le Rapport annuel 2019 du Comité ainsi que son Rapport spécial sur la collecte, l'utilisation, la conservation et la diffusion de renseignements sur les Canadiens dans le contexte des activités du renseignement de défense du ministère de la Défense nationale et des Forces armées canadiennes. Au total, les deux rapports contiennent quatre examens approfondis. Le dépôt des rapports coïncidait avec le début d'un confinement à l'échelle nationale visant à freiner la propagation de la COVID-19. Les rapports ont tout de même fait l'objet d'une couverture médiatique à l'échelle nationale et internationale à ce moment, et le président du Comité a mené des activités de sensibilisation auprès d'universitaires et d'autres Canadiens au cours des mois

suivants. L'intérêt soutenu des médias envers les examens du Comité, surtout ceux concernant l'ingérence étrangère ainsi que la diversité et l'inclusion, souligne leur pertinence continue aux yeux des Canadiens. Le président a mené d'autres activités de sensibilisation lorsqu'il a pris la parole au sujet des rapports de 2019 du Comité devant le Comité permanent de la sécurité publique et nationale de la Chambre des Communes le 23 novembre 2020.

4. Le confinement à l'échelle nationale a interrompu les activités du Comité et l'ont forcé à modifier son plan de travail pour 2020. Les directives en matière de santé publique empêchaient le Comité de se réunir en personne, et la nature sensible de ses travaux ainsi que ses exigences en matière de sécurité ont limité la capacité du Comité de se réunir virtuellement. Le Secrétariat du Comité a poursuivi les travaux au nom du Comité pendant les mois d'avril, de mai et de juin. Durant cette période, le Comité s'est réuni à trois reprises pour préciser ses intentions relativement à son Rapport annuel 2020 ainsi qu'à son plan d'examen pour 2021. La souplesse des membres durant cette période a permis de poursuivre les travaux du Comité, à un rythme plus lent, jusqu'à ce que toutes les mesures soient en place pour reprendre de manière sécuritaire les réunions sécurisées.

5. Depuis le début de la pandémie, le Comité a réduit la fréquence et la durée de ses réunions. Néanmoins, à l'aide du soutien du SCRS en ce qui a trait à la technologie et aux locaux, le Comité s'est réuni 16 fois en 2020 pour un total de 54 heures. Pendant cette période, le Comité a lancé deux examens, a rencontré des cadres supérieurs de l'appareil de la sécurité et du renseignement, a organisé trois audiences et a rédigé le présent Rapport annuel. Le Comité a des projets ambitieux pour 2021, et les travaux relatifs à ces examens vont bon train.

Le point sur la réponse du gouvernement aux recommandations du Comité

6. À la suite de sa reconstitution en 2020, le Comité a pris le temps de se pencher sur la réponse du gouvernement concernant les travaux que le Comité a réalisés au cours de ses deux premières années d'existence. Depuis le dépôt de son premier Rapport spécial en décembre 2019, le Comité a formulé 23 recommandations à l'intention du gouvernement visant à renforcer l'efficacité et la responsabilisation de l'appareil de la sécurité et du renseignement[1].

7. La réponse du gouvernement aux rapports du Comité a été limitée. Juste avant sa dissolution en septembre 2019, le Comité a reçu une lettre du premier ministre reconnaissant son travail et indiquant qu'il se penchait sur ses recommandations. Les lettres de mandat à l'intention des ministres de la Sécurité publique et de la Protection civile, et de la Défense nationale remises par le premier ministre en

---

[1] Pour une liste complète des recommandations du Comité, veuillez consulter les rapports suivants: Comité des parlementaires sur la sécurité nationale et le renseignement (CPSNR), *Rapport spécial sur le voyage du Premier ministre en Inde en février 2018*, 3 décembre 2018, p.43, https://nsicop-cpsnr.ca/reports/rp-2018-12-03/intro-fr.html; CPSNR, *Rapport annuel 2018*, 9 avril 2019, pp. 123-124, https://nsicop-cpsnr.ca/reports/rp-2019-04-09/intro-fr.html; CPSNR, *Rapport spécial sur la collecte, l'utilisation, la conservation et la diffusion de renseignements sur les Canadiens dans le contexte des activités de renseignement de défense du ministère de la Défense nationale et des Forces armées canadiennes*, 12 mars 2020, p. 50, https://nsicop-cpsnr.ca/reports/rp-2020-03-12-sr/intro-fr.html ; et CPSNR, *Rapport annuel 2019*, 12 mars 2020, pp. 199-201, https://nsicop-cpsnr.ca/reports/rp-2020-03-12-ar/intro-fr.htm

décembre 2019 leur demandait de : « mettre en place un nouveau cadre régissant la collecte, la gestion et l'utilisation des renseignements de défense par le Canada, comme le recommande le Comité des parlementaires sur la sécurité nationale et le renseignement[2]. » Le Comité a reçu une copie d'une lettre du Commissariat à la protection de la vie privée du Canada envoyée au ministère de la Défense nationale et des Forces armées canadiennes (MDN/FAC) lui offrant de l'aide et son expertise afin que le MDN/FAC mette en œuvre cet engagement. Le Comité et son Secrétariat ont également reçu de la rétroaction informelle de la part de cadres supérieurs concernant certains aspects des examens du Comité.

8. Les membres du Comité passent beaucoup de temps à délibérer des recommandations pour s'assurer qu'elles sont raisonnables, applicables et efficaces. Les examens sont le produit d'un travail notable de la part du Comité et des organisations de l'appareil de la sécurité et du renseignement. Le Comité reconnaît que le gouvernement n'est pas tenu de répondre aux recommandations. Toutefois, le Comité estime que des réponses régulières et concrètes contribueraient à renforcer la responsabilisation et la transparence de l'appareil de la sécurité et du renseignement. À ce sujet, il convient de noter que le comité parlementaire sur le renseignement et la sécurité du Royaume-Uni, l'homologue international du Comité, reçoit régulièrement des réponses du gouvernement concernant ses rapports. Par conséquent, nous demandons au gouvernement d'envisager de répondre officiellement aux examens du Comité, de la même façon qu'il répond à des organisations comme le Bureau du vérificateur général et les comités parlementaires.

Planification des activités à venir

9. Le plan d'action du Comité est ambitieux, et le Comité a annoncé le début de ses prochains examens en septembre 2020. La seconde itération du Comité continuera d'effectuer des examens concernant des cadres et des activités en vertu des alinéas 8(1)a) et 8(1)b) de sa loi habilitante. En effet, il examinera le **cadre** du gouvernement visant à protéger ses systèmes et ses réseaux contre les cyberattaques, ainsi que les **activités** d'Affaires mondiales Canada liées à la sécurité nationale et au renseignement. Les deux examens sont en cours et le Comité se réjouit à l'idée d'étudier ces questions au cours de l'année à venir. Le Comité s'engage toujours à nouer le dialogue avec la société civile et les universitaires afin de veiller à ce que ses travaux tiennent compte d'une multitude de points de vue.

Exigences en matière d'établissement de rapports

10. La loi sur le CPSNR impose un certain nombre d'obligations en matière d'établissement de rapports au Comité. Conformément à l'alinéa 21(1), le Comité doit présenter ses conclusions et ses recommandations de la dernière année dans son rapport annuel. Comme susmentionné, le Comité n'a

---

[2] Premier ministre Justin Trudeau, « Lettre de mandat du ministre de la Défense nationale », 13 décembre 2019, https://pm.gc.ca/fr/lettres-de-mandat/2019/12/13/lettre-de-mandat-du-ministre-de-la-defense-nationale; et premier ministre Justin Trudeau, « Lettre de mandat du ministre de la Sécurité publique et de la Protection civile », 13 décembre 2019, https://pm.gc.ca/fr/lettres-de-mandat/2019/12/13/lettre-de-mandat-du-ministre-de-la-securite-publique-et-de-la-protection-civile.

pas réalisé d'examen en 2020 et n'a donc aucune conclusion et recommandation à présenter. La Loi sur le CPSNR stipule aussi que le Comité doit indiquer le nombre de fois où, au cours de l'année précédente, un ministre compétent a déterminé qu'un examen des activités proposé par le Comité porterait atteinte à la sécurité nationale. Le Comité doit également indiquer le nombre de fois où un ministre compétent a refusé de communiquer un renseignement au Comité car, selon lui, le renseignement est un renseignement opérationnel spécial ou sa communication porterait atteinte à la sécurité nationale. En 2020, il n'a pas été déterminé qu'un examen présenté par le Comité porterait atteinte à la sécurité nationale, et aucun ministre n'a refusé de communiquer un renseignement au Comité avec comme motif qu'il s'agit d'un renseignement opérationnel spécial et que sa communication porterait atteinte à la sécurité nationale.

11. Le Comité indique également qu'il a reçu des rapports annuels de treize organisations concernant leurs applications de la Directive ministérielle : Éviter la complicité dans les cas de mauvais traitements par des entités étrangères, conformément au paragraphe 8(1) de la *Loi visant à éviter la complicité dans les cas de mauvais traitements infligés par des entités étrangères*. Cette directive oblige les ministères et les organismes de mettre en place ou de mettre à jour leurs politiques et leurs procédures afin d'assurer leur conformité à la loi. Le Comité a reçu des rapports de la part d'Affaires mondiales Canada, de l'Agence des services frontaliers du Canada, de l'Agence du revenu du Canada, du Centre d'analyse des opérations et déclarations financières du Canada (CANAFE), du Centre de la sécurité des télécommunications (CST), de la Gendarmerie royale du Canada, d'Immigration, Réfugiés et Citoyenneté Canada, du ministère de la Défense nationale et des Forces armées canadiennes, de Pêches et Océans Canada, du SCRS, de Sécurité publique Canada et de Transports Canada. Le Comité n'a pas reçu de rapports de la part du Bureau du Conseil privé.

12. En septembre 2020, le gouvernement a fourni au Comité la version classifiée du *Rapport sur l'évaluation du protocole public en cas d'incident électoral majeur*. Le protocole public et le Rapport ont été demandés dans le cadre d'une directive du Cabinet de juillet 2019, qui présentait une approche visant à informer le public des incidents en matière d'ingérence étrangère menaçant l'intégrité des élections fédérales de 2019. L'approche prévoyait notamment l'établissement d'un groupe d'experts composé de cinq hauts fonctionnaires qui seraient chargés de décider d'informer les Canadiens de ces incidents. La directive demandait également qu'un examen indépendant du protocole soit effectué afin d'évaluer sa mise en œuvre et son efficacité, de déterminer s'il devrait être établi de manière permanente et de cerner de possibles améliorations. De plus, la directive imposait aussi de fournir au Comité un rapport final de cet examen. Jim Judd, un ancien directeur du SCRS et un ancien sous-ministre de la Défense nationale, a effectué l'examen.

13. Le Comité a examiné attentivement le rapport de Jim Judd. Il était encouragé de voir le gouvernement prendre des mesures concrètes pour lutter contre l'ingérence étrangère. Comme indiqué dans le Rapport annuel 2019 du Comité, le Canada est la cible d'activités d'ingérence étrangère substantielles et soutenues. Des acteurs étrangers cherchent à perturber le processus politique du Canada à tous les niveaux du gouvernement, ce qui pose un risque pour la souveraineté du pays et l'intégrité des institutions démocratiques. Par conséquent, le Comité appuie les principales

recommandations du rapport de Jim Judd, notamment celles portant sur le rétablissement du mécanisme du protocole bien avant les prochaines élections fédérales et sur l'élargissement du mandat pour comprendre la période préélectorale.

14. Le Comité estime que le gouvernement devrait envisager quatre questions au moment de délibérer des recommandations du Rapport :

- En premier lieu, le mandat du protocole devrait porter sur toutes les formes d'ingérence étrangère, de la cyberingérence aux méthodes plus traditionnelles. D'après l'examen de 2019 du Comité, les formes traditionnelles d'ingérence étrangère sont omniprésentes dans la sphère politique du Canada et représentent une menace considérable pour les droits et les libertés des Canadiens.
- En deuxième lieu, la composition du groupe d'experts pourrait bénéficier de l'inclusion de Canadiens éminents, possiblement des juristes retraités. Le Comité redoute que les hauts fonctionnaires nommés pour le groupe d'experts soient préoccupés par la préparation de la transition durant la période électorale, et souligne qu'une intervention par un groupe qui comprend des Canadiens éminents non-partisans et de grande notoriété pourrait avoir une plus grande incidence dans le contexte hautement politisé des élections.
- En troisième lieu, le gouvernement devrait discuter fréquemment et en profondeur avec les partis politiques sur le but et le fonctionnement du Protocole afin d'assurer la compréhension la plus vaste sur le rôle non partisan du groupe d'experts et le processus d'intervention.
- En dernier lieu, on devrait étudier plus en profondeur la manière dont le groupe d'experts informerait les Canadiens d'un incident d'ingérence étrangère, notamment les questions touchant les attributions.

15. Le Comité a fait part de son opinion au sujet du rapport Judd dans une lettre au premier ministre en décembre 2020 et poursuivra ses discussions sur le protocole avec le greffier du Conseil privé en sa qualité de président du groupe d'experts.

Structure du Rapport annuel

16. Le Rapport annuel 2020 est différent des autres rapports du Comité. Puisque le Comité a été reconstitué en février 2020, et en raison des perturbations causées par la pandémie, le Comité n'a pas été en mesure d'achever un examen approfondi en 2020 à inclure dans son rapport annuel. Après avoir délibéré longuement, le Comité a plutôt décidé de faire le point sur l'évaluation de la menace présentée dans son premier rapport annuel datant de 2018, et ce, pour plusieurs raisons. D'abord, le gouvernement ne rédige pas d'aperçu disponible au public sur les principales menaces pour la sécurité nationale du Canada. Le Comité a relevé cette lacune dans son Rapport annuel 2018 et il estime toujours qu'un tel aperçu sensibiliserait davantage la population aux menaces pour la sécurité du Canada. Ensuite, le Comité s'attend à ce que sa mise à jour de 2020 continuera d'éclairer le débat sur les enjeux importants en matière de sécurité et de renseignement au Canada. Enfin, au cours des deux dernières années, d'importants changements se sont produits dans le milieu de la sécurité à l'échelle nationale et internationale, y compris des défis imposés par la pandémie de COVID-19.

17. Le chapitre suivant fait le point sur les principales menaces en matière de sécurité envers le Canada : le terrorisme, l'espionnage et l'ingérence étrangère, les cyberactivités malveillantes, le crime organisé d'envergure et les armes de destruction massive. Cette mise à jour donnera le ton aux prochains examens du Comité.

18. L'aperçu des menaces pour la sécurité nationale du Canada présenté par le Comité en 2018 n'inclut pas les menaces militaires qui pèsent sur le pays. Le Comité note que le MDN/FAC a demandé au Comité d'inclure une description de ces menaces dans son aperçu de 2020. Selon le MDN/FAC [traduction] « au cours des dernières années, nos adversaires, notamment la Russie et la Chine, ont fortement priorisé leurs appareils de défense et ils s'affirment de plus en plus dans leurs efforts visant à remettre en cause l'ordre international fondé sur des règles, avec l'intention claire de contrer l'influence et les intérêts occidentaux. Les adversaires du Canada ont étudié nos capacités militaires et ils ont développé des armes précisément conçues pour déjouer nos défenses et exploiter nos vulnérabilités[3]. » Le Comité envisage de faire un suivi avec le MDN/FAC et d'autres organismes de sécurité à l'avenir afin de mieux comprendre la nature et la portée des menaces militaires à la sécurité du Canada.

[3] Ministère de la Défense nationale et les Forces armées canadiennes (MDN/FAC), lettre de la sous-ministre du ministère de la Défense nationale à la directrice générale du Secrétariat du CPSNR, 27 novembre 2020.

Menaces envers le Canada : un aperçu

19. Dans son Rapport annuel 2018, le Comité a souligné certaines menaces pour la sécurité nationale du Canada. En 2018, le Bureau du Conseil privé a informé le Comité de ces menaces, et l'appareil de la sécurité et du renseignement a validé leur pertinence continue en 2020. Cette année, le Comité a décidé de faire le point sur les menaces et de les exposer en détail, particulièrement en ce qui a trait aux cinq questions cernées par l'appareil de la sécurité et du renseignement : le terrorisme, l'espionnage et l'ingérence étrangère, les cyberactivités malveillantes, le crime organisé d'envergure, et les armes de destruction massive. Le Comité a étudié certaines de ces questions de façon plus approfondie dans ses examens. Par exemple, le Comité s'est penché sur l'ingérence étrangère dans son Rapport spécial de 2018 sur le voyage du premier ministre en Inde, ainsi que dans son examen de 2019 de la réponse du gouvernement à l'ingérence étrangère, et il publiera son examen des moyens de cyberdéfense du gouvernement en 2021.

20. Le chapitre qui suit porte sur les cinq menaces successivement. Chaque section décrit la menace et son évolution depuis 2018, ainsi que les répercussions de la pandémie s'il en est, puis présente les principales conclusions.

Terrorisme

Aperçu

21. Dans son Rapport annuel 2018, le Comité a souligné que l'appareil de la sécurité nationale et du renseignement a défini le terrorisme comme étant la principale menace pour la sécurité nationale. Le gouvernement a également déclaré que des personnes ou des groupes inspirés par l'idéologie salafiste-jihadiste représentent la plus grande menace terroriste pour le Canada. Toutefois, cette évaluation a évolué sur la base de plusieurs tendances et événements. On compte notamment la libération du territoire sous le joug de Daech en Irak et en Syrie, la détention subséquente des voyageurs extrémistes canadiens (aussi connus sous le nom de combattants étrangers) en Syrie, des attaques contre des Canadiens par des individus et des organisations extrémistes, et la montée de l'extrémisme violent à caractère idéologique. Ces enjeux sont décrits ci-dessous.

Description de la menace

22. Dans son rapport public de 2018, le Service canadien du renseignement de sécurité (SCRS) indiquait que le terrorisme était la principale menace pour la sécurité nationale du Canada[4]. La même année, Sécurité publique Canada mentionnait dans son Rapport public sur la menace terroriste pour le Canada que des individus ou des groupes inspirés par l'idéologie salafiste-jihadiste violente, comme celle de Daech ou d'al-Qaïda, posaient la menace terroriste la plus grande pour le Canada et les intérêts canadiens. Depuis octobre 2014, le niveau de menace terroriste nationale du Canada est resté à *modéré*, c'est-à-dire qu'un attentat terroriste violent pourrait survenir et que des mesures supplémentaires sont en place pour assurer la sécurité des Canadiens[5]. De juillet 2018 à septembre 2020, la GRC a mené *** une/des enquête(s) prioritaire(s) liée(s) au terrorisme.[6] Pour la même période, le SCRS a mené une/des enquête(s) faisant l'objet d'un mandat contre *** cible(s) et *** organisation(s). Le SCRS a également déclaré au Comité qu'un seul complot terroriste a été déjoué au Canada pendant cette période.[7]

23. La nature de la menace terroriste mondiale change. La libération du territoire contrôlé par Daech en Irak et en Syrie en 2019 a été une grande victoire pour la lutte contre le terrorisme à l'échelle mondiale. Toutefois, elle a entraîné son lot de défis en ce qui a trait à la déradicalisation des voyageurs extrémistes et au rapatriement de ces individus et de leurs familles. (Le SCRS définit un voyageur extrémiste comme étant un individu ayant un lien avec le Canada, comme un citoyen, un résident permanent ou un détenteur de visa, qui est soupçonné de s'être rendu à l'étranger pour mener une

---

[4] Service canadien du renseignement de sécurité (SCRS), *Rapport public du SCRS 2018*, 2018. www.canada.ca/content/dam/csis-scrs/documents/publications/2018-PUBLIC_REPORT_FRENCH_Digital.pdf

[5] Centre intégré d'évaluation du terrorisme (CIET), *Niveaux nationaux de la menace terroriste*, 2020. www.canada.ca/fr/services/defense/securitenationale/niveau-menace-terroriste.html.

[6] Gendarmerie Royale du Canada (GRC), *Tiered Project Activity Report*, 27 novembre 2020.

[7] SCRS, réponse par courriel au Secrétariat du CPSNR, 10 décembre 2020.

activité liée au terrorisme[8].) En Afrique de l'Ouest, les groupes alignés sur Daech et al-Qaïda continuent de représenter une menace pour le personnel des Forces armées canadiennes, les civils et les entreprises. Des personnes au Canada continuent de financer des groupes terroristes, comme le Hezbollah et ceux associés ***. En même temps, de nouvelles menaces ont fait surface. Une série d'attaques d'extrémisme violent à caractère idéologique au Canada et ailleurs dans le monde a montré manifestement que ce type d'extrémisme représente une menace grandissante pour la sécurité nationale du Canada.

Contexte international du terrorisme

24. Les tendances et événements de la scène internationale ont des répercussions sur le contexte de la menace terroriste du Canada. L'un des plus importants événements liés au terrorisme des dernières années a été l'émergence de Daech et l'apparition connexe de conflits en Irak et en Syrie en 2011. À son paroxysme, Daech contrôlait environ le tiers du territoire syrien et 40 % du territoire irakien[9]. Seulement en 2015, le revenu du groupe variait entre 1 et 2,4 milliards de dollars américains[10]. Le succès initial de Daech, illustré par ses victoires sur le terrain, le contrôle de territoires et ses ressources financières, lui a permis de créer un lieu sûr pour la planification terroriste, d'étendre son réseau de groupes affiliés au-delà des frontières de l'Irak et de la Syrie, et d'inspirer des personnes partout sur la planète à perpétrer des attentats en appui de l'organisation et de ses objectifs. D'après les estimations, plus de 40 000 combattants étrangers de plus de 110 pays, dont le Canada, se sont rendus sur le territoire contrôlé par Daech en Irak et en Syrie[11].

25. En 2019, le territoire en Irak et en Syrie a été libéré de l'emprise de Daech. L'organisation terroriste avait désigné ce territoire comme le califat et s'en servait pour amasser des fonds, faire de l'entraînement, accroître son influence et diriger des attentats. La libération du territoire a porté un coup au moyens de Daech et a poussé 100 000 combattants et leurs familles derrière les barreaux d'établissements de détention des Forces démocratiques syriennes[12]. Cette situation pose un défi sur le plan de la politique étrangère et de la lutte contre le terrorisme pour les états, qui doivent décider s'ils veulent rapatrier les personnes détenues et la façon de gérer le risque que représentent les personnes de retour.

---

[8] SCRS, *Rapport public du SCRS 2018*, 2018. www.canada.ca/content/dam/csis-scrs/documents/publications/2018-PUBLIC_REPORT_FRENCH_Digital.pdf.

[9] Wilson Center, *Timeline: The Rise, Spread, and Fall of the Islamic State*, 28 octobre 2019.

[10] Colin P. Clarke et autres, *Financial Futures of the Islamic State of Iraq and the Levant*, RAND Corporation, 2017.

[11] Richard Barrett, *Beyond the Caliphate: Foreign Fighters and the Threat of Returnees*, The Soufan Center, octobre 2017; et Conseil de sécurité des Nations Unies, *Dixième rapport du Secrétaire générale sur la menace que représente l'EIIL (Daech) pour la paix et la sécurité internationales et sur l'action menée par l'Organisation des Nations Unies pour aider les États Membres à contrer cette menace*, février 2020, https://undocs.org/fr/S/2020/95.

[12] États-Unis, Bureau of Counterterrorism, *Country Reports on Terrorism 2018*, octobre 2019, https://www.state.gov/wp-content/uploads/2019/11/Country-Reports-on-Terrorism-2018-FINAL.pdf ; Conseil de sécurité des Nations Unies, *Dixième rapport du Secrétaire générale sur la menace que représente l'EIIL (Daech) pour la paix et la sécurité internationales et sur l'action menée par l'Organisation des Nations Unies pour aider les États Membres à contrer cette menace*, février 2020, https://undocs.org/fr/S/2020/95; Leah West, Amarnath Amarasingam et Jessica Davis, « Where's the Plan for Canadian ISIS Members in Custody Overseas? », *Policy Options*, juin 2019.

26. Les voyageurs extrémistes constituent toujours une préoccupation sur le plan de la sécurité. Le SCRS estime qu'au moins 200 voyageurs extrémistes ayant un lien avec le Canada se sont rendus à l'étranger pour se joindre à Daech et à d'autres groupes terroristes depuis 2013, dont 122 en Syrie, en Irak et en Turquie, et le reste en Afghanistan, au Pakistan, au Liban et en Somalie[13]. En effet, comme l'a indiqué le ministre de la Sécurité publique et de la Protection civile, « [c]ertains d'entre eux sont devenus des combattants sur le champ de bataille. D'autres ont effectué des collectes de fonds, de la planification opérationnelle, de la propagande en ligne, du recrutement, de la formation et d'autres activités connexes » tandis que d'autres « n'étaient que des sympathisants[14]. » Néanmoins, leur retour au Canada ou la poursuite de leurs activités à l'étranger représentent encore un obstacle pour la sécurité. Des quelque 200 extrémistes du Canada qui se sont rendus à l'étranger, 61 sont de retour[15]. Selon le SCRS, en date de novembre 2020, 122 voyageurs extrémistes se trouvent en Turquie, en Syrie et en Irak. De ce nombre, *** seraient morts. Des autres ***, *** sont en Syrie (*** détenu(s) et *** en liberté), *** en Turquie (***détenu(s) et *** en liberté), et *** sont en Irak (*** détenu(s) et *** en liberté)[16]. Affaires mondiales Canada et Sécurité publique Canada continuent de gérer le processus lié aux voyageurs extrémistes qui souhaitent revenir au pays et collaborent avec la Gendarmerie royale du Canada (GRC) et d'autres services de police canadiens pour réduire les risques connexes potentiels. À ce jour, aucun voyageur de retour n'a perpétré d'attentat au Canada, mais des individus qui voulaient se rendre à l'étranger ou dont leur plan de le faire a été déjoué en ont perpétrés.

27. Malgré leur affaiblissement graduel, Daech et al-Qaïda poursuivent leurs opérations. Ils dirigent des groupes affiliés et inspirent des groupes et des personnes de partout dans le monde à se livrer au terrorisme. Daech est toujours actif dans certaines parties de l'Irak et de la Syrie, et la protection de la frontière qui sépare les deux pays est un défi constant[17]. Les combattants de Daech constituent une menace au personnel des Forces armées canadiennes en Irak, où le Canada appuie actuellement deux missions : son Opération IMPACT et la mission de l'OTAN en Irak. Bien que les FAC aient retiré des membres de son personnel en Irak, *** membres restent au pays pour soutenir les deux missions. À l'extérieur de l'Irak et de la Syrie, les ramifications de Daech en Afghanistan, en Indonésie, en Malaisie et dans les Philippines font planer des menaces constantes pour la sécurité nationale et régionale[18]. Les affiliés de Daech en Afrique de l'Ouest et dans le Grand Sahara et les affiliés d'al-Qaïda dans le Sahel sont également particulièrement actifs.

---

[13] SCRS, *Rapport annuel au ministre sur les activités opérationnelles 2018-2019*, 19 décembre 2019; CIET, réponse par courriel au Secrétariat du CPSNR, 30 novembre 2020.

[14] L'honorable Ralph Goodale, allocution à la Shoyama Graduate School of Public Policy, Saskatchewan, 15 janvier 2019, https://www.canada.ca/fr/securite-publique-canada/nouvelles/2019/01/discours-sur-levolution-de-larchitecture-de-securite-nationale-du-canadadans-un-monde-tres-difficile-en-constante-evolution.html.

[15] CIET, réponse par courriel au Secrétariat du CPSNR, 30 novembre 2020.

[16] CIET, réponse par courriel au Secrétariat du CPSNR , 30 novembre 2020.

[17] Conseil de sécurité des Nations Unies, *Dixième rapport du Secrétaire générale sur la menace que représente l'EIIL (Daech) pour la paix et la sécurité internationales et sur l'action menée par l'Organisation des Nations Unies pour aider les États Membres à contrer cette menace*, février 2020, https://undocs.org/fr/S/2020/95.

[18] Conseil de sécurité des Nations Unies, *Dixième rapport du Secrétaire générale sur la menace que représente l'EIIL (Daech) pour la paix et la sécurité internationales et sur l'action menée par l'Organisation des Nations Unies pour aider les États Membres à contrer cette menace*, février 2020, https://undocs.org/fr/S/2020/95.

28. Les affiliés de Daech et d'al-Qaïda en Afrique représentent une menace pour les Canadiens. D'août 2018 à août 2019, les FAC ont déployé une force opérationnelle d'aviation au Mali pour appuyer une mission de maintien de la paix des Nations Unies. Le Canada contribue actuellement à de nombreuses opérations de maintien de la paix au Mali, notamment jusqu'à 10 membres des FAC et des officiers de police civils. Au Burkina Faso, un attentat contre un convoi transportant des travailleurs d'une mine appartenant à des intérêts canadiens en 2019a tué 39 personnes et en a blessé 60 autres, forçant l'entreprise à suspendre ses opérations, ce qui a eu des incidences négatives sur des intérêts commerciaux canadiens. De plus, des Canadiens ont été enlevés et, parfois même, assassinés dans la région. Par exemple, Daech a revendiqué l'assassinat d'un Canadien en janvier 2019 enlevé d'une mine appartenant à des intérêts canadiens au Burkina Faso. Dans un autre exemple, une Canadienne a été enlevée au Burkina Faso en décembre 2018 [*** Deux phrases ont été revues pour supprimer l'information préjudiciable ou privilégiée. Elles décrivent des renseignements liés à l'enlèvement et une évaluation du SCRS. ***][19] ***[20]

29. L'activité terroriste se poursuit au Canada[21]. Depuis 2018, deux attaques fatales ont mené à des accusations d'activité terroriste, comme définies à l'article 83.01 du *Code criminel*. En février 2020, un individu a été accusé de meurtre au premier degré et d'activité terroriste à la suite d'une attaque au marteau inspirée par Daech qui a tué une femme à Toronto[22]. En mai 2020, les mêmes accusations ont été portées contre un individu inspiré par l'idéologie des Célibataires involontaires (ou les « incels »), une sous-culture de la misogynie violente, qui a poignardé une femme à mort dans un salon de massage de Toronto[23]. Le *Code criminel* comporte aussi des dispositions liées à des infractions pour ce qui est de faciliter une activité terroriste, de quitter le Canada pour se joindre à un groupe terroriste et de participer aux activités d'un groupe terroriste. Depuis 2018, cinq individus ont été accusés de telles infractions : un à Kingston, en Ontario, en janvier 2019; un à Guelph, en Ontario, en décembre 2019, et sa conjointe à Markham, en Ontario, en août 2020; un à Calgary, en Alberta, en juillet 2020; et un cas connexe à Calgary, en Alberta, en septembre 2020[24]. Le CIET estime que [traduction] « la plus grande menace terroriste pour le Canada continue d'être les extrémistes nationaux inspirés par Daech, al-Qaïda ou le milieu extrémiste à caractère idéologique[25] ».

30. Le Canada continue également de faire face à des risques de financement terroriste. Dans son Rapport public sur la menace terroriste pour le Canada, Sécurité publique Canada a inscrit Daech, al-

---

[19] SCRS, *** 2 juillet 2020.
[20] SCRS, *** 19 décembre 2019.
[21] Sécurité publique Canada, *Rapport public de 2016 sur la menace terroriste pour le Canada*, 2016, https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2016-pblc-rpr-trrrst-thrt/2016-pblc-rpr-thrt/index-fr.aspx
[22] Stewart Bell, « Suspect's Alleged Statements About ISIS led to Terrorism Charge Over Toronto Hammer Attack: Sources », *Global News*, mars 2020, www.globalnews.ca/news/6661038/toronto-hammer-attack-by-isis-supporter/.
[23] Stewart Bell, Andrew Russell et Catherine McDonald, « Deadly Attack at Toronto Erotic Spa was Incel Terrorism, Police Allege », *Global News*, mai 2020, https://globalnews.ca/news/6910670/toronto-spa-terrorism-incel/.
[24] The Canadian Press, « Youth arrested in Kingston terrorism case appears for bail hearing », *Global News*, 12 mars 2019, https://ctvnews.ca/canada/youth-arrested-in-kingston-terrorism-case-appears-for-bail-hearing-1.4332212; Rachel Browne, « Guelph man now facing terrorism charges », *Global News*, 6 décembre 2019, https://globalnews.ca/news/6263053/ikar-mao-terrorism-charges/; et Demi Knight, « RCMP lay terrorism charges against 2nd Calgary man in ongoing investigation », *Global News*, 25 septembre 2020, https://globalnews.ca/news/7359488/2nd-calgary-man-facing-terrorism-charges/.
[25] CIET, *Le Niveau national de la menace terroriste au Canada*, EM 20/45-F, 30 juillet 2020.

Qaïda et le Hezbollah comme étant les groupes suscitant les préoccupations les plus élevées sur le plan du financement terroriste. Le Rapport note aussi que certains Canadiens continuent de soutenir des groupes associés ***, y compris par le financement de présumés groupes terroristes[26]. Le CIET estime qu'un petit nombre d'extrémistes au Canada soutiennent des activités terroristes, *** [27].

Extrémisme violent à caractère idéologique

31. L'extrémisme violent à caractère idéologique est en croissance depuis 2018. Il comprend la violence xénophobe, la violence contre l'autorité, la violence fondée sur le sexe et la « violence fondée sur d'autres récriminations ou idéologies[28] ». Selon le SCRS, ce qui unit ces groupes et personnes est une croyance commune que « la réussite ou la survie de la société ou de la civilisation est indissociable du recours permanent à la violence contre un ou plusieurs groupes perçus comme menaçant (l'élite, les minorités visibles, les groupes religieux, les entreprises, les immigrants, les capitalistes, le gouvernement, etc.)[29] ». Bien que le SCRS emploie le terme *extrémisme violent à caractère idéologique* pour décrire les attaques motivées par les idéologies extrémistes de l'ensemble de l'éventail politique, sa reconnaissance par le SCRS est en partie une réponse à la menace changeante de l'extrémisme de droite.

32. Au Canada, des personnes ou des groupes qui nourrissent de telles opinions sont particulièrement actifs en ligne. Ils utilisent des salles de clavardage, des plateformes de réseaux sociaux conventionnelles ou dédiées à l'extrémisme violent à caractère idéologique, ainsi que des réseaux en ligne pour s'échanger des idées[30]. Selon une étude menée par l'Institute for Strategic Dialogue en 2020, les Canadiens sont très actifs sur les 6 600 voies de communication, pages, groupes et comptes d'extrémisme de droite trouvés, et même plus actifs que les utilisateurs américains ou britanniques dans un cas[31].

33. En règle générale, les individus inspirés par l'extrémisme violent à caractère idéologique sont généralement moins affiliés officiellement à un groupe que ceux inspirés par l'idéologie de Daech ou d'al-Qaïda. Cela dit, la recherche donne à penser qu'en date de 2015, au moins 100 groupes suprématistes blancs et néonazis existaient dans l'ensemble du Canada, dont la vaste majorité des activités d'extrémisme violent à caractère idéologique au Canada étaient dans le sud-ouest de l'Ontario, le sud du Québec et le sud de l'Alberta[32]. Selon les dernières estimations, il y aurait autour de 300 groupes de ce genre au Canada[33].

---

[26] Sécurité publique Canada, *Rapport public sur la menace terroriste pour le Canada de 2018*, 2019.
[27] CIET, *** 29 mars 2019.
[28] SCRS, *Rapport public de 2019*, 2020.
[29] SCRS, *Définition de l'extrémisme violent dans le contexte de la menace en évolution au Canada*, *** 16 octobre 2019.
[30] Sécurité publique Canada, *Rapport public sur la menace terroriste pour le Canada de 2018*, 2019.
[31] Jacob Davey, Mackenzie Hart et Cécile Guerin, « An Online Environmental Scan of Right-win Extremism in Canada », *Institute for Strategic Dialogue*, 2020, https://www.isdglobal.org/wp-content/uploads/2020/06/An-Online-Environmental-Scan-of-Right-wing-Extremism-in-Canada-ISD.pdf.
[32] Barbara Perry et Ryan Scrivens, *Right-Wing Extremism in Canada*, Palgrave Macmillan, 2019.
[33] Alex Boutilier, « Researchers to probe Canada's evolving far-right movements », *Toronto Star*, 6 mars 2019, https://www.thestar.com/politics/federal/2019/03/06/researchers-to-probe-canadas-evolving-far-right-movements.html.

34. Les groupes néonazis grossissent et sont actifs. Le SCRS indique que l'un de ces groupes, l'Atomwaffen Division, [*** La phrase suivante a été revue pour supprimer l'information préjudiciable ou privilégiée. Elle résume une évaluation du groupe par le SCRS. ***][34] D'autres groupes d'extrémisme violent à caractère idéologique au Canada comme l'Azov Battalion en Ukraine semblent vouloir créer un mouvement transnational plus uni au moyen des médias sociaux. L'Agence des services frontaliers du Canada (ASFC) souligne qu'un rapport du groupe de recherche à but non lucratif Soufan Center indique qu'au moins 14 Canadiens se sont rendus en Ukraine pour s'entraîner avec des extrémistes[35].

35. La menace de l'extrémisme violent à caractère idéologique au Canada s'amplifie à travers le monde. Selon l'Indice mondial de terrorisme de 2019, les incidents de ce genre d'extrémisme en Occident ont augmenté de 320 % de 2013 à 2018[36]. Un rapport publié en avril 2020 par la direction exécutive du Comité contre le terrorisme des Nations Unies lance un avertissement similaire à savoir que [traduction] « la fréquence et la létalité [des attaques extrémistes violentes à caractère idéologique] a connu une hausse récente[37] ». Depuis le dernier survol du Comité en 2018, de nombreuses attaques extrémistes violentes à caractère idéologique ont été perpétrées. Les plus importantes d'entre elles sont énumérées ci-dessous. En mars 2019, à Christchurch, en Nouvelle-Zélande, une personne a tué 51 personnes et blessé 49 autres dans deux attaques consécutives contre des mosquées. Les attaques ont été citées comme étant l'inspiration d'une attaque raciste anti-immigrants perpétrée à El Paso, au Texas, en août 2019, qui a fait 22 morts et 26 blessés. En octobre 2019, à Halle, en Allemagne, un individu aux motifs antisémites d'extrême droite a tué deux personnes après avoir tenté de prendre d'assaut une synagogue. Quatre mois plus tard, l'auteur d'un attentant raciste et anti-immigrant a tué par balles neuf personnes à Hanau, en Allemagne.

36. Les attaques violentes perpétrées par des extrémistes inspirés par les incels constituent aussi une menace grandissante. La sous-culture incel est en croissance et chevauchent de plus en plus d'autres types d'extrémisme violent. Le SCRS indique que « la violence misogyne se réclame aussi d'autres aspects des idéologies extrémistes violentes (IEV), notamment le suprématisme blanc. Beaucoup de tenants de la suprématie de la race blanche, d'incels et d'autres groupes ou membres de l'homosphère ont en commun la haine des femmes[38]. » La mobilisation de ces personnes et groupes a été largement influencée par les médias sociaux, qui servent en sorte de chambre d'écho pour possiblement radicaliser et enhardir des acteurs vers la violence[39]. Le Canada a aussi été victime de trois attentats perpétrés par des incels au cours des deux dernières années. En avril 2018, un membre du mouvement misogyne des incels a tué 10 personnes et en a blessé 16 autres dans une attaque à la

---

[34] SCRS, *** 2019.

[35] Agence des services frontaliers du Canada (ASFC), *La nature de plus en plus transnationale de l'extrémisme de droite*, DOAR_2020-January-001, janvier 2020.

[36] Institute for Economics & Peace, *Global Terrorism Index 2019,* 2019, www.visionofhumanity.org/app/uploads/2019/11/GTI-2019web.pdf

[37] Direction exécutive du Comité contre le terrorisme du Conseil de sécurité des Nations Unies, *Member States Concerned by the Growing and Increasingly Transnational Threat of Extreme Right-Wing Terrorism*, avril 2020, https://www.un.org/sc/ctc/wp-content/uploads/2020/04/CTED_Trends_Alert_Extreme_Right-Wing_Terrorism.pdf.

[38] SCRS, *La violence misogyne dans la sous-culture incel*, ***, 15 janvier 2020.

[39] CIET, *Le niveau national de la menace terroriste au Canada*, TA 19/127-Corrigé, 5 décembre 2019.

fourgonnette-bélier à Toronto, en Ontario[40]. En juin 2019, inspiré par l'attentat de 2018 à la fourgonnette-bélier, un individu a poignardé une mère et a blessé son enfant à Sudbury, en Ontario[41]. En février 2020, un individu motivé par l'idéologie des incels a poignardé et tué une personne et en a blessé une autre à Toronto, en Ontario[42]. Ce dernier incident a marqué la première accusation d'une infraction pour terrorisme pour une attaque liée aux incels (voir le paragraphe 29).

37. Des états ont adopté certaines mesures pour régler la menace croissante de l'extrémisme violent à caractère idéologique au Canada. Le Royaume-Uni a inscrit National Action (aussi connu sous les noms Scottish Dawn, NS131 et System Resistance Network) et Sonnenkrieg Division comme entités terroristes[43]. En avril 2020, les États-Unis ont inscrit le Russian Imperial Movement et, en 2019, le Canada a ajouté Blood & Honour et Combat 18 à sa liste des entités terroristes (un lien vers la liste complète des entités terroristes inscrites se trouvent en note de bas de page)[44]. À la suite des attentats contre les mosquées à Christchurch, la Nouvelle-Zélande a ciblé l'utilisation d'Internet par les extrémistes de droite en criminalisant la possession et la distribution du manifeste et de l'enregistrement en direct de l'auteur[45]. De même, l'Australie a adopté une loi qui impose des amendes et des peines d'emprisonnement pour les entreprises qui ne suppriment pas promptement le [traduction] « contenu violent odieux » de leurs sites Web[46].

Tactiques et cibles terroristes

38. Au Canada, la principale menace terroriste, d'un groupe ou d'un individu, demeure les attentats peu sophistiqués contre des lieux publics non protégés. De tels attentats demandent des compétences et des ressources minimes, mais peuvent entraîner beaucoup de morts et attirer l'attention du public. Des cibles vulnérables, comme des hôtels, des centres commerciaux et des restaurants, sont facilement accessibles et souvent bondées[47]. Selon le CIET, même si la plupart des extrémistes préfèrent perpétrer un attentat de grande envergure et très sophistiqué, ils en viendront probablement à choisir un attentat

---

[40] « Toronto van attack: 'Incel' killer Minassian pleads not criminally responsible », *BBC*, 10 novembre 2020. https://www.bbc.com/news/world-us-canada-54895219.

[41] Arron Pickard, « Sudbury 'incel' knife attacker told police he was 'out to murder a little white girl' », *Timmins Today*, 13 janvier 2020, https://www.timminstoday.com/local-news/sudbury-incel-knife-attacker-told-police-he-was-out-to-murder-a-little-white-girl-2018572.

[42] Nick Boisvert, « Homicide at Toronto massage parlour was an act of incel terrorism, police say », *CBC*, 19 mai 2020. https://www.cbc.ca/news/canada/toronto/incel-terrorism-massage-parlour-1.5575689.

[43] Home Office, Royaume-Uni, *Proscribed Terrorist Groups or Organizations*, février 2020, https://www.gov.uk/government/publications/proscribed-terror-groups-or-organisations--2.

[44] Voir la liste complète des entités terroristes inscrites ici: Sécurité publique Canada, *Entités inscrites*, 2020, www.securitepublique.gc.ca/cnt/ntnl-scrt/cntr-trrrsm/lstd-ntts/index-fr-.aspx ; Département d'État, États-Unis, *United States Designates Russian Imperial Movement an Leaders as Global Terrorists*, 7 avril 2020, https://www.state.gov/united-states-designates-russian-imperial-movement-and-leaders-as-global-terrorists/;

[45] Damien Cave, « New Zealand Bans the Christchurch Suspect's Manifesto », *The New York Times*, 22 mars 2019, https://www.nytimes.com/2019/03/22/world/asia/new-zealand-christchurch-shooter-manifesto.html.

[46] « Australia Targets Tech Firms with 'Abhorrent Material' Laws », *BBC News*, 4 avril 2019, https://www.bbc.com/news/world-australia-47809504.

[47] Sécurité publique Canada, *Rapport public sur la menace terroriste pour le Canada de 2018*, 2019.

qu'ils seront en mesure de perpétrer, c'est-à-dire des attentats demandant peu de compétences contre des cibles vulnérables[48].

Pandémie de COVID-19

39. La pandémie a eu des répercussions sur l'accessibilité aux cibles, la planification des extrémistes violents et la radicalisation de personnes. Le CIET estime que les diminutions des grands rassemblements et la fermeture de lieux publics pousseront les attaquants potentiels à ajuster le tir dans leur planification, plutôt que de renoncer à un attentat. Dans certains cas, la pandémie et les manifestations en parallèle contre le racisme ont amplifié la rhétorique antigouvernementale en ligne lié à l'extrémisme violent à caractère idéologique[49]. Le SCRS souligne que les restrictions mises en place en raison de la pandémie, y compris les restrictions de voyage, ont perturbé les efforts de facilitation terroriste ***. Cependant, ces groupes se réajustent afin d'exploiter les mesures liées à la pandémie *** afin de faire avancer leurs objectifs[50].

40. Même si les extrémistes violents ont adapté leurs activités, il est aussi possible que la radicalisation augmente. Selon la GRC, les restrictions mises en place durant la pandémie, dont les mesures de confinement, pourraient inciter des individus à chercher des conseils ou de l'information sur Internet et faire en sorte qu'ils accèdent à des chambres d'écho extrémistes. Ce risque est amplifié par les défis de l'isolement social et des difficultés financières imposés par les restrictions. Ces mêmes restrictions rendent encore plus difficile de déterminer si une personne emprunte la voie de la radicalisation[51].

Principales conclusions

41. Les individus ou les groupes inspirés par l'idéologie salafiste-jihadiste, comme celle de Daech et d'al-Qaïda, représentaient la menace terroriste la plus importante de 2018. Même si Daech et al-Qaïda ont été relativement affaiblis au cours des deux dernières années, ils constituent encore une menace pour le Canada et les intérêts canadiens au pays et à l'étranger. En même temps, le SCRS a découvert d'importantes activités liées à l'extrémisme violent à caractère idéologique au cours des deux dernières années (notamment les groupes d'extrême droite), comme en témoignent l'activité en ligne et les attaques. L'augmentation importante des activités extrémistes violentes à caractère idéologique en 2020 donne à penser que le contexte de la menace terroriste amorce un virage. La principale menace physique au Canada demeure les attentats peu sophistiqués contre les lieux publics non protégés. Ces tendances sont à l'image des tendances discernées chez les plus proches alliés du Canada.

---

[48] CIET, *Le niveau national de la menace terroriste au Canada*, EM 19/127-Corrigée, 5 décembre 2019.
[49] CIET, *Le point : Le niveau national de la menace terroriste au Canada*, TA 20/45-E, 30 juillet 2020.
[50] SCRS, *COVID-19: The Evolving Terrorism Threat*, *** 2020.
[51] GRC, *Potential for Radicalization to Violence due to COVID-19*, 1er mai 2020.

Espionnage et ingérence étrangère

Aperçu

42. En 2018, le Comité a défini que l'espionnage et l'ingérence étrangère étaient des menaces grandissantes pour lesquelles il faudra probablement prendre des mesures non négligeables au cours des années à venir. L'espionnage et l'ingérence étrangère menace la souveraineté, la prospérité et les intérêts nationaux du Canada. Ces menaces visent les collectivités, les gouvernements, les entreprises, les universités et la technologie. En 2019, le Comité a examiné la réponse du gouvernement à l'ingérence étrangère et a constaté que les activités d'ingérence étrangère représentent un risque considérable pour la sécurité nationale, principalement parce qu'elles portent atteinte aux institutions fondamentales du Canada et fragilisent les droits et libertés des Canadiens. En 2020, le SCRS a déclaré que les acteurs des états hostiles posaient le danger le plus important pour la sécurité nationale du Canada. Des reportages dans les médias, des discours de dirigeants et des informations sur des dossiers criminels montrent tous que la menace continue d'évoluer non seulement au Canada, mais également chez ses alliés.

Description de la menace

43. L'espionnage a longtemps constitué une menace majeure pour la sécurité du Canada et celle d'autres nations. Même si l'espionnage a joué un rôle essentiel durant la Guerre froide, la menace qu'il représente maintenant a évolué. De plus, la croissance d'Internet et le fait que la société et l'économie soient de plus en plus interreliées ont mené à la prolifération des cyberactivités comme mode d'espionnage, ainsi qu'une augmentation du risque que représentent les personnes non traditionnelles qui recueillent des renseignements, comme les étudiants et les chercheurs.[52] Les activités d'espionnage consistent principalement en des états étrangers qui tentent d'obtenir des informations politiques, économiques et militaires, ou encore des renseignements commerciaux exclusifs, par des moyens cachés.

44. L'ingérence étrangère continue de représenter une menace importante pour la sécurité du Canada. Les états étrangers ont recours à des contacts directs et indirects pour influencer les institutions et les processus démocratiques et électoraux en manipulant les communautés ethnoculturelles, les personnes en position d'autorité ou d'influence, ainsi que les médias. Dans un discours prononcé devant l'Economic Club of Canada à la fin de 2018, David Vigneault, directeur du SCRS, a défini l'ingérence étrangère et l'espionnage comme les menaces les plus grandes pour la prospérité nationale et les intérêts nationaux du Canada. L'espionnage parrainé par l'État contre le Canada se classe en deux catégories qui peuvent être jumelées ou non : l'espionnage employant des cyberméthodes et l'espionnage humain traditionnel[53]. On relève plusieurs exemples récents d'espionnage au Canada qui

---

[52] SCRS, *** 2019.

[53] David Vigneault, Allocution devant le Economic Club of Canada, décembre 2018, www.canada.ca/fr/service-renseignement-securite/nouvelles/2018/12/allocution-pour-david-vigneault-au-economic-club-of-canada.htm.

démontrent que la menace qu'il fait planer demeure omniprésente. De juillet 2018 à septembre 2020, la GRC a mené *** enquête(s) prioritaire(s) liée(s) à l'espionnage et à l'ingérence étrangère[54]. Pour la même période, le SCRS a mené une/des enquête(s) faisant l'objet d'un mandat contre *** cible(s) et *** organisation(s).[55]

Espionnage

45. Les états étrangers prennent de plus en plus pour cible le secteur des sciences et de la technologie du Canada, dans lequel le pays est reconnu comme un chef de file mondial. Selon le SCRS, les acteurs de la menace étrangers représentent une menace importante pour les intérêts économiques et nationaux à long terme du Canada. Ces acteurs emploient une combinaison de méthodes de collecte de renseignements traditionnelles et non traditionnelles pour accéder à une expertise, à des données et à des organisations. Cette préoccupation grandissante a poussé le gouvernement à mettre sur pied l'Équipe spéciale des sous-ministres sur la science et la sécurité nationale en octobre 2019 pour évaluer et aborder les vulnérabilités en matière de sécurité dans le secteur des sciences du gouvernement[56].

46. Le SCRS estime que même si des pays comme la Fédération de Russie, *** ont pris pour cible le secteur de la science et de la technologie du Canada, *** la menace en provenance de la Chine *** Dans nombre de cas, ces acteurs prennent pour cible la science et la technologie dans lesquelles le gouvernement du Canada investit. La Chine utilise des « programmes de talents » et des échanges universitaires pour exploiter l'expertise canadienne. Son programme des « mille talents », créé en 2008 pour encourager les scientifiques chinois à l'étranger à apporter leurs recherches en Chine, est actuellement au cœur d'une enquête menée par le département de la justice américain[57]. [***La phrase suivante a été revue pour supprimer l'information préjudiciable ou privilégiée. Elle décrit les circonstances au Canada. ***] De plus, le programme entraîne souvent un transfert de propriété intellectuelle en Chine, *** [*** La phrase a été revue pour supprimer l'information préjudiciable ou privilégiée. Elle décrit une évaluation du SCRS. ***][58]

47. Les états étrangers prennent de plus en plus pour cible les nouvelles technologies. Le SCRS souligne que les domaines essentiels à l'économie du savoir au Canada, comme l'intelligence artificielle, la technologie quantique, la 5G et la biopharmaceutique, sont activement pris pour cible[59]. Le rapport public de 2018 du SCRS décrivait également l'espionnage économique comme étant une menace

---

[54] GRC, *Tiered Project Activity Report*, 27 novembre 2020.
[55] SCRS, réponse par courriel au Secrétariat du CPSNR, 10 décembre 2020.
[56] SCRS, *Foreign Threats to Canadian Science and Technology*, *** 2019; et SCRS, réponse par courriel au Secrétariat du CPSNR, 10 décembre 2020.
[57] Barry, Ellen et Gina Kolata, « China's Lavish Funds Lured US Scientists. What did it get in return? », *The New York Times*, 6 février 2020.
[58] SCRS, *Foreign Threats to Canadian Science and Technology*, *** 2019; SCRS, *** 2020; et SCRS, *** 2020.
[59] David Vigneault, Allocution devant le Economic Club of Canada, décembre 2018, www.canada.ca/fr/service-renseignement-securite/nouvelles/2018/12/allocution-pour-david-vigneault-au-economic-club-of-canada.htm.

d'importance ayant des conséquences graves sur l'économie du Canada, notamment la perte d'emplois, la perte de revenus fiscaux et la diminution d'un avantage concurrentiel[60].

Menaces internes

48. Les menaces internes sont une autre forme d'espionnage qui consiste en une personne ayant des connaissances ou un accès à une organisation et qui, intentionnellement ou à son insu, emploie improprement son accès pour nuire à l'organisation, notamment à son personnel, à ses biens, à ses intérêts ou à sa réputation[61]. Au Canada, deux récents exemples d'activités de menaces internes présumées ont entraîné des accusations criminelles : Cameron Ortis et Qing Quentin Huang.

49. Cameron Ortis, un directeur général du renseignement à la GRC, a été arrêté le 12 septembre 2019. Il a d'abord été accusé conformément à trois articles de la *Loi sur la protection de l'information* et à deux articles du *Code criminel*, mais trois autres chefs d'accusation ont été déposés au titre de la *Loi sur la protection de l'information* en janvier 2020[62]. Il a été accusé de communiquer des informations opérationnelles spéciales à une entité étrangère et de se préparer à communiquer des informations sensibles à une entité étrangère. Les chefs d'accusation se rapportent à des incidents s'étant déroulés entre 2015 et 2019. La GRC a reconnu publiquement qu'Ortis avait accès à des renseignements nationaux et d'alliés[63].

50. Au départ, Qing Quentin Huang a été accusé en 2013 d'avoir tenté de communiquer des secrets à une entité étrangère. Plus précisément, Huang, qui était employé de Lloyd's Register[64] à l'époque, a été accusé de comploter de vendre des secrets militaires (de la marine) à la Chine[65]. En novembre 2019, le procureur général du Canada a émis un certificat empêchant la divulgation d'informations et infirmant la décision d'un juge de la cour fédérale qui aurait révélé des informations sensibles issues d'opérations de collecte du SCRS contre l'ambassade de la Chine en 2013. Un tel certificat est du jamais

---

[60] SCRS, *Rapport public du SCRS 2018*, juin 2018. www.canada.ca/content/dam/csis-scrs/documents/publications/2018-PUBLIC_REPORT_FRENCH_Digital.pdf.

[61] Sécurité publique Canada, *Renforcer la résilience des infrastructures essentielles du Canada aux risques internes*, 2019, https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/nhncgn-crtcl-nfrstrctr/index-fr.

[62] *Loi sur la protection de l'information*, L.R.C., 1985, paragraphe 14(1), et alinéas 22(1)b) et 22(1)e); et *Code criminel*, L.R.C. 1985, ch. C-46, article 122, et paragraphe 342.1(1).

[63] Leyland Cecco, « Canada: arrest of ex-head of intelligence shocks experts and alarms allies », *The Guardian*, 16 septembre 2019, https://www.theguardian.com/world/2019/sep/16/concern-mounts-after-canadas-ex-head-of-intelligence-accused-of-leaking; Catharine Tunney, « Alleged RCMP spy Cameron Ortis faces 3 new charges under Canada's secrets act », *CBC*, 27 janvier 2020, https://www.cbc.ca/news/politics/cameron-ortis-espionage-rcmp-1.5442231; et Amanda Connolly, Mercedes Stephenson, Stewart Bell, Sam Cooper et Rachel Browne, « RCMP intel director charged in major case was top adviser to former force head: sources », *Global News*, 13 septembre 2019, https://globalnews.ca/news/5899146/senior-rcmp-arrested-charged/.

[64] Lloyd's Register est un « fournisseur international expert dans les services de classification, de conformité et d'inspection à l'attention des secteurs maritimes et offshore. » Voir : Lloyd's Register, « Marine et Expédition », https://www.lr.org/fr-fr/maritime-expedition/.

[65] The Canadian Press, « Case of Hamilton man allegedly spying for China, tangled in secrecy », *CBC*, 28 juin 2019, https://www.cbc.ca/news/canada/hamilton/case-of-hamilton-man-allegedly-spying-for-china-tangled-in-secrecy-1.5193658.

vu[66]. En septembre 2020, deux accusations contre Huang ont été levées pour protéger les renseignements. Au moment de la rédaction du présent rapport, Huang était libéré sous caution et deux accusations criminelles pesaient toujours contre lui[67].

51. [*** Le paragraphe a été revu pour supprimer de l'information préjudiciable ou privilégiée. Il décrit des enquêtes menées par la GRC et le SCRS. ***][68]

Ingérence étrangère

52. En 2019, le Comité a réalisé un examen de la réponse du gouvernement à l'ingérence étrangère. Dans cet examen, le Comité a conclu que certains états étrangers menaient des activités d'ingérence étrangère sophistiquées et omniprésentes contre le Canada. Ces activités constituent un risque considérable pour la sécurité nationale, principalement parce qu'elles portent atteinte aux institutions fondamentales du Canada et fragilisent les droits et libertés des Canadiens. Le Comité a recommandé que le gouvernement élabore une stratégie exhaustive pour lutter contre l'ingérence étrangère et renforcer la résilience institutionnelle et publique, et appuie cette stratégie exhaustive au moyen d'une direction et d'une coordination centrales.

53. Le Comité a souligné que des états prennent le Canada pour cible et cherchent à tirer profit de l'ouverture de sa société et à s'immiscer au sein de ses institutions fondamentales pour atteindre leurs objectifs. Ils ciblent les communautés ethnoculturelles, cherchent à corrompre le processus politique, manipulent les médias et tentent de manipuler des débats sur les campus postsecondaires. Chacune de ces activités pose un risque important pour les droits et les libertés des Canadiens et la souveraineté du pays. Le Comité a donc conclu qu'ils constituent une menace manifeste pour la sécurité du Canada.

54. Depuis l'examen du Comité présenté dans son rapport de 2019, la menace persiste. La Chine *** [*** Deux phrases ont été revues pour supprimer l'information préjudiciable ou privilégiée. Elles décrivent une enquête menée par le SCRS. ***][69] Au pays, à la suite des élections fédérales de 2019, [*** Trois phrases ont été revues pour supprimer l'information préjudiciable ou privilégiée. Elles décrivent une évaluation du SCRS. ***][70]

55. La Fédération de Russie continue aussi à exploiter la diaspora russe et les organisations compatriotes au Canada. [*** Deux phrases ont été revues pour supprimer l'information préjudiciable ou privilégiée. Elles décrivent les objectifs et les méthodes de la Russie. ***][71]

---

[66] Andrew Russell, « Canada's attorney general blocks disclosure of evidence in case of Ontario man accused of spying », *Global News*, 21 novembre 2019, https://globalnews.ca/news/6199672/attorney-general-blocks-disclosure-of-evidence-ontario-spying-case/.

[67] Colin Freeze, « Prosecutors stay charges against Qing Quentin Huang in probe of naval leaks to China », *The Globe and Mail*, 18 septembre 2020, https://www.theglobeandmail.com/canada/article-prosecutors-stay-charges-against-qing-quentin-huang-in-probe-of-naval/.

[68] SCRS, *Rapport annuel au ministre sur les activités opérationnelles 2018-2019,* 19 décembre 2019.

[69] SCRS, *Rapport annuel au ministre sur les activités opérationnelles 2018-2019,* 19 décembre 2019.

[70] SCRS, *** 2020.

[71] SCRS, *** 2019.

56. D'autres états continuent de se livrer activement à de l'ingérence étrangère au Canada. [*** Trois phrases ont été revues pour supprimer l'information préjudiciable ou privilégiée. Elles décrivent une évaluation par le SCRS des méthodes et des objectifs d'un état. ***][72]

Pandémie de COVID-19

57. L'espionnage lié à la science et à la technologie, surtout sur l'élaboration d'un vaccin contre la COVID-19, a augmenté pendant la pandémie. Les réseaux de recherche aux États-Unis, au Canada et au Royaume-Uni ont été la cible d'efforts de collecte de renseignements de la part de la Chine, de la Russie et de l'Iran. Le New York Times a écrit que la pandémie a [traduction] « entraîné l'un des virages de mission menée en temps de paix les plus rapides de notre époque pour les services de renseignement du monde, les opposant les uns aux autres dans une nouvelle stratégie d'espion contre espion[73]. » Le Centre de la sécurité des télécommunications (CST) indique que la Russie est la principale responsable de cet espionnage, qu'elle exerce au moyen de cyberopérations secrètes pour voler des données exclusives[74].

58. Au Canada, le SCRS a déterminé que *** exploite mondialement la pandémie pour obtenir un avantage économique et technologique. [*** Le paragraphe a été revu pour supprimer de l'information préjudiciable ou privilégiée. Il décrit l'évaluation du SCRS des méthodes et des objectifs d'un état. Le paragraphe note aussi la vulnérabilité accrue des petites entreprises canadiennes et les secteurs biopharmaceutique et de santé aux efforts de cet état. ***][75] ***[76]

Principales conclusions

59. La menace de l'espionnage et de l'ingérence étrangère est substantielle et continue de s'accroître. Plusieurs états se livrent à de telles activités au Canada, mais le renseignement indique que la Chine et la Russie sont toujours les principales coupables. Même si les effets de l'espionnage et de l'ingérence étrangère ne sont pas aussi rapidement manifestes que ceux du terrorisme, ils représentent les menaces à long terme les plus lourdes de conséquences pour la souveraineté et la prospérité du Canada. La pandémie, quant à elle, a incité de nouveau les états étrangers à se livrer à de l'espionnage contre le secteur de la santé du Canada et des organisations canadiennes qui travaillent dans le domaine de la science et de la technologie.

---

[72] SCRS, *** 2019.
[73] Julian E Barnes et Michael Venutolo-Mantovani, « Race for Coronoavirus Vaccine Pits Spy Against Spy », *The New York Times*, 5 septembre 2020, https://nyti.ms/2F2oAPd.
[74] Centre de la sécurité des télécommunications (CST), *Déclaration du CST sur les menaces visant le développement d'un vaccin contre la COVID-19*, 16 juillet 2020, https://www.cse-cst.gc.ca/fr/media/2020-07-16.
[75] SCRS, *** 2020.
[76] SCRS, *** sans date.

Cyberactivités malveillantes

Aperçu

60. Dans son survol de 2018, le Comité indiquait que les cyberactivités malveillantes constituaient un risque considérable pour la sécurité nationale et il attirait précisément l'attention sur la menace que font planer la Chine et la Russie sur les réseaux gouvernementaux. Les cybermenaces se font sentir un peu partout; elles touchent les systèmes gouvernementaux, les fournisseurs d'infrastructures essentielles, le secteur privé, ainsi que les Canadiens. Les acteurs de cybermenaces varient de cybercriminels peu sophistiqués à des acteurs étatiques très capables. Leurs motivations sont aussi diversifiées, comme le vol de renseignements personnels dans un dessein de fraude ou de propriétés intellectuelles et d'informations d'entreprise confidentielles dans un but d'espionnage industriel, ou encore l'interruption de services essentiels. En 2020, les cybermenaces figurent encore parmi les préoccupations en matière de sécurité nationale du Canada, et la Russie et la Chine sont toujours les acteurs étatiques les plus perfectionnés qui prennent pour cible les systèmes du gouvernement du Canada[77]. Au cours de la dernière année, les acteurs de cybermenaces ont également pris avantage de la crise sanitaire mondiale causée par la pandémie de COVID-19 pour faire avancer leurs objectifs. Des acteurs malveillants étatiques et non étatiques ont pris pour cible le secteur de la santé et les services gouvernementaux et ont mené des campagnes de désinformation en ligne pour manipuler l'opinion publique et saper la confiance de la population dans le fonctionnement des systèmes de santé publique clés.

Description de la menace

61. Pour le Canada, *** états représentent les cybermenaces les plus importantes. En effet, en 2019 et 2020, le CST a déterminé que les cybermenaces étatiques les plus importantes provenaient de la Chine, de la Fédération de Russie, de l'Iran, de la République démocratique populaire de la Corée (Corée du Nord), ***[78]. Le CST a été continuellement témoin de cyberactivités correspondant aux objectifs stratégiques nationaux de chaque acteur, notamment les cyberactivités contre les réseaux gouvernementaux du Canada, les systèmes et les industries du secteur privé et les systèmes des infrastructures essentielles.

62. La Chine et la Russie continuent d'être les principaux moteurs des cyberactivités ciblant le gouvernement depuis 2018. Année après année, cette activité a été constante et axée sur de nombreux secteurs gouvernementaux, notamment : [*** Le paragraphe a été revu pour supprimer de l'information préjudiciable ou privilégiée. Il énumère les secteurs et les organisations gouvernementales. ***][79]

---

[77] Centre canadien pour la cybersécurité (CCC), *Portrait des cybermenaces qui pèsent sur le Canada : Le point sur 2019 et prévisions pour 2020*, 1er décembre 2019.
[78] CCC, *Portrait des cybermenaces qui pèsent sur le Canada : Le point sur 2019 et prévisions pour 2020*, 1er décembre 2019.
[79] CCC, *Portrait des cybermenaces qui pèsent sur le Canada : Le point sur 2019 et prévisions pour 2020*, 1er décembre 2019.

63. Le CST a relevé une augmentation des cyberattaques parrainées par l'État contre des cibles canadiennes dans la première moitié de 2020[80]. Entre janvier et juin 2020, le CST a observé *** tentatives de compromission de cibles canadiennes par *** des acteurs de la Chine. Environ ***, dont *** compromissions ont réussi, prenaient pour cible *** le secteur ***. Pendant cette période, *** acteurs de la Russie ont tenté de compromettre *** cibles canadiennes et, selon le CST, la compromission de *** de ces cibles était probablement réussie. Bien que *** le secteur *** représente une partie des activités de ciblage de *** les cybereffortts de cette nation visaient aussi [*** La phrase a été revue pour supprimer l'information préjudiciable ou privilégiée. Elle décrit des domaines ciblés. ***]

64. L'*Évaluation des cybermenaces nationale* de 2020 du CST décrit plusieurs tendances clés dans le contexte de la cybermenace[81]. Premièrement, le CST estime que les acteurs de cybermenace augmentent en nombre et en complexité. Deuxièmement, le CST est d'avis que des programmes étatiques de la Chine, de la Russie, de l'Iran et de la Corée du Nord représentent la menace stratégique la plus importante pour le Canada et que les acteurs parrainés par l'état tentent probablement de développer des cybercapacités pour perturber les infrastructures essentielles. Troisièmement, il fait remarquer que les acteurs parrainés par l'état continueront de mener des activités d'espionnage commercial contre des entreprises, des universitaires et le gouvernement pour voler de la propriété intellectuelle et des informations. Quatrièmement, le CST déclare que les campagnes d'ingérence étrangère se poursuivent et ne se limitent pas aux grands événements politiques comme les élections. Finalement, il indique que le cybercrime est toujours la menace qui toucherait le plus les Canadiens et les organisations canadiennes, et que les grandes entreprises canadiennes et infrastructures essentielles continueraient d'être la cible d'attaques par rançongiciel. De juillet 2018 à septembre 2020, la GRC a enregistré *** enquête(s) prioritaire(s) liée(s) au cybercrime[82]. Pour la même période, le SCRS a mené une/des enquête(s) liée(s) aux cybermenaces faisant l'objet d'un mandat contre *** cible(s) et *** organisation(s).[83]

65. Parmi les grandes tendances relatives aux activités cybermenace, celles qui correspondent le plus étroitement à la sécurité nationale et au renseignement sont le vol d'information à des fins d'espionnage, la compromission de réseaux des infrastructures essentielles, les campagnes d'ingérence étrangère en ligne par l'entremise de la manipulation coordonnée des réseaux sociaux et des opinions, et le cybersuivi et la cybersurveillance de dissidents et d'autres personnes. Ces points sont traités ci-dessous.

---

[80] CCC, *Cyber Threat Brief: State Activity against Canada January to June 2020*, 26 juin 2020.
[81] CCC, *Évaluation des cybermenaces nationale 2020*, https://cyber.gc.ca/fr/orientation/evaluation-des-cybermenaces-nationales-2020.
[82] GRC, *Tiered Project Activity Report*, 27 novembre 2020.
[83] SCRS, réponse par courriel au Secrétariat du CPSNR, 10 décembre 2020.

Vol d'informations à des fins d'espionnage

66. Le vol d'information parrainé par l'État peut toucher tant les réseaux du gouvernement que ceux d'autres institutions publiques. Ces réseaux sont des cibles précieuses en raison de la nature essentielle de leurs services et de la nature délicate des renseignements qu'ils gèrent[84]. En ce qui a trait particulièrement aux réseaux du gouvernement, le CST a noté que les acteurs de cybermenace prenaient pour cible les renseignements confidentiels et sensibles, comme *** ou des détails sur ***. La numérisation continue des services gouvernementaux présente de nouvelles vulnérabilités pour les renseignements confidentiels et sensibles, y compris le virage en croissance vers l'infonuagique[85]. Le CST et ses homologues alliés estiment que les adversaires étatiques ont l'intention et les plus grands moyens pour diriger des cyberopérations contre les réseaux du gouvernement.

67. Le Canada et ses alliés ont imputé des activités de cyberespionnage à la Chine et à la Russie. D'après le CST, les cybermoyens de ces deux pays sont parmi les plus sophistiqués au monde[86]. La Chine utilise ses cyberopérations pour s'en prendre aux gouvernements, aux entreprises et aux établissements universitaires à l'échelle mondiale afin d'obtenir des renseignements commerciaux, diplomatiques et militaires à l'appui de ses objectifs stratégiques[87]. Selon le CST, les cybermoyens de la Chine sont [*** Deux phrases ont été revues pour supprimer l'information préjudiciable ou privilégiée. Elles décrivent une évaluation du CST. ***][88] ***[89] Même si la Russie emploie également des tactiques sophistiquées de cyberespionnage pour contribuer à ses objectifs stratégiques, le CST est d'avis que [*** La phrase suivante a été revue pour supprimer l'information préjudiciable ou privilégiée. Elle décrit une évaluation du CST. ***][90]

68. L'espionnage étatique contre des réseaux privés soulève également de grandes préoccupations. La propriété intellectuelle, les renseignements d'entreprise confidentiels et les informations sur les partenariats stratégiques ou les plans de recherche et de développement d'une entreprise peuvent servir directement à un état étranger et à ses industries. Les activités de cyberespionnage prenant pour cible le secteur privé peuvent entraîner la perte d'un avantage concurrentiel, surtout dans des domaines spécialisés de recherche et de développement. Pour des économies avancées comme le Canada et ses alliés, le cyberespionnage contre les réseaux privés comporte d'importants risques.

---

[84] CST, « Institution publiques et information sensible », *Évaluation des cybermenaces nationales 2018*, décembre 2018, https://www.cyber.gc.ca/fr/orientation/institutions-publiques-et-information-sensible.

[85] CST, « Institution publiques et information sensible », *Évaluation des cybermenaces nationales 2018*, décembre 2018, https://www.cyber.gc.ca/fr/orientation/institutions-publiques-et-information-sensible.

[86] CCC, *Portrait des cybermenaces qui pèsent sur le Canada : Le point sur 2019 et prévisions pour 2020*, 1er décembre 2019.

[87] CCC, *Canada's Cyber Threat Landscape: Overview and Outlook for 2019*, 30 janvier 2019; CCC, *Portrait des cybermenaces qui pèsent sur le Canada : Le point sur 2019 et prévisions pour 2020*, 1er décembre 2019.

[88] CCC, *Canada's Cyber Threat Landscape: Overview and Outlook for 2019*, 30 janvier 2019.

[89] CCC, *Canada's Cyber Threat Landscape: Overview and Outlook for 2019*, 30 janvier 2019.

[90] CCC, *Gouvernement du Canada Rapport sur les Cybermenaces – T3 & T4 2018*, sans date; et CCC, *Portrait des cybermenaces qui pèsent sur le Canada : Le point sur 2019 et prévisions pour 2020*, 1er décembre 2019.

69. La Russie et la Chine ont mené des activités de cyberespionnage contre les secteurs canadiens ***[91]. Pour la Russie, ces efforts appuient les priorités en matière de renseignement liées ***[92]. Pour la Chine, ces activités contribuent [*** Le paragraphe a été revu pour supprimer de l'information préjudiciable ou privilégiée. Il décrit une évaluation du SCRS des objectifs de la Chine et un exemple spécifique du cyber-espionnage mené par la Chine. ***][93]

70. Les pays alliés ont probablement connu des expériences similaires avec le cyberespionnage par la Chine et la Russie. Au début de 2019, la Chine a lancé des cyberattaques contre le Parlement australien et ses trois principaux partis avant les élections générales du pays[94]. Plus récemment, en juin 2020, la Chine a probablement mené une autre cyberattaque d'envergure contre l'Australie, prenant pour cible des entreprises, des hôpitaux, des écoles et des représentants gouvernementaux australiens[95]. Pour cette attaque, des cyberacteurs parrainés par la Chine auraient apparemment employé des tactiques d'harponnage pour percer des réseaux sensibles et mener de la reconnaissance. En octobre 2020, le centre national de cybersécurité (National Cyber Security Centre) du Royaume-Uni a révélé que les services du renseignement militaire russes avaient mené des activités de cyberreconnaissance de grande envergure en préparation à une cyberattaque contre les Jeux olympiques et paralympiques de 2020 à Tokyo[96].

Compromission des infrastructures essentielles

71. Le ciblage des infrastructures essentielles peut compromettre la sécurité publique et la sécurité nationale. Ces systèmes, qui sont de plus en plus contrôlés par accès Internet à distance, soutiennent la prestation de services essentiels comme les réseaux de la santé et les systèmes des hôpitaux, du réseau électrique, du transport, de l'énergie et de la distribution alimentaire[97]. Le Canada et ses plus proches partenaires de la sécurité et du renseignement ont fait rapport sur des cyberattaques et des compromissions de réseaux des services publics du secteur de l'énergie, bancaires, des télécommunications et de l'infrastructure des communications, ainsi que des réseaux des fournisseurs de services d'infonuagique[98].

---

[91] CCC, *Portrait des cybermenaces qui pèsent sur le Canada : Le point sur 2019 et prévisions pour 2020*, 1er décembre 2019; et CST, « Cybermenace contre les infrastructures essentielles canadiennes », *Évaluation des cybermenaces nationales 2018*, décembre 2018, https://www.cyber.gc.ca/fr/orientation/cybermenaces-contre-les-infrastructures-essentielles-canadiennes.
[92] CCC, *Portrait des cybermenaces qui pèsent sur le Canada : Le point sur 2019 et prévisions pour 2020*, 1er décembre 2019.
[93] SCRS, *** 2020.
[94] Colin Packham, « Exclusive: Australia concluded China was behind hack on parliament, political parties – sources », *Reuters*, 15 septembre 2019, https://www.reuters.com/article/us-australia-china-cyber-exclusive/exclusive-australia-concluded-china-was-behind-hack-on-parliament-political-parties-sources-idUSKBN1W00VF.
[95] Charlie Moore et Tim Stickins, « China is blamed for huge cyber attack on Australian businesses, schools and hospitals amid increasing war of words between Canberra and Beijing over call for international inquiry into COVID-19 », *The Daily Mail*, 20 juin 2020, https://www.dailymail.co.uk/news/article-8438205/Huge-cyber-attack-aimed-Australian-government.html.
[96] Patrick Wintour, « Russia planned cyber-attack on Tokyo Olympics, says UK », *The Guardian*, 19 octobre 2020, https://www.theguardian.com/world/2020/oct/19/russia-planned-cyber-attack-on-tokyo-olympics-says-uk.
[97] Le Canada a défini 10 secteurs d'infrastructure essentielle. Sécurité publique Canada, *Infrastructure essentielles*, sans date, https://www.publicsafety.gc.ca/cnt/ntnl-scrt/crtcl-nfrstrctr/index-fr.aspx; et Sécurité publique Canada, *Stratégie nationale de cybersécurité*, 28 mai 2019, https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/index-fr.aspx.
[98] CST, « Cybermenace contre les infrastructure essentielles canadiennes », *Évaluation des cybermenaces nationales 2018*, décembre 2018, https://www.cyber.gc.ca/fr/orientation/cybermenaces-contre-les-infrastructures-essentielles-canadiennes;

72. Selon le CST, la Russie, la Chine et l'Iran ont montré une intention de développer des moyens de cyberattaque contre les systèmes de contrôle industriels liés aux infrastructures essentielles[99]. Le CST a déjà établi que *** contre ces systèmes, ***[100]. Un exemple notable de cette capacité remonte à 2017, lorsque le CST a alerté ses partenaires aux États-Unis d'une compromission d'un système de contrôle industriel dans le secteur de l'énergie. Les représentants du Département de la sécurité intérieure des États-Unis ont par la suite déclaré que des acteurs de cybermenace de la Russie avaient progressé jusqu'au point où ils auraient pu interrompre les réseaux d'électricité en Amérique du Nord[101]. D'après le CST, [*** Deux phrases ont été revues pour supprimer l'information préjudiciable ou privilégiée. Elles décrivent une évaluation du CST des méthodes, objectifs et cibles d'un état. ***][102] ***[103] Toutefois, il souligne qu'en l'absence d'une crise majeure ou d'un conflit armé avec le Canada ou les États-Unis, l'interruption intentionnelle des infrastructures essentielles du Canada demeure peu probable.

Campagnes d'ingérence étrangère en ligne

73. Les auteurs de cybermenaces avancées ont aussi perfectionné leur capacité de mener des campagnes de désinformation en ligne. Les auteurs de menaces mènent ces campagnes sur les réseaux sociaux pour accentuer les différences sociétales, semer la discorde et saper la confiance en les institutions gouvernementales fondamentales. Par exemple, le CST a par le passé remarqué des comptes Twitter liés à une armée de trolls russe publiant des gazouillis sur plusieurs événements d'envergure au Canada, y compris la fusillade dans une mosquée de Québec en janvier 2017 et l'augmentation du nombre de demandeurs d'asile qui ont traversé la frontière à l'été 2017[104]. Cependant, le CST estime que la majorité des campagnes de désinformation menées par la Russie et ayant un lien avec le Canada ***[105] Néanmoins, d'après le CST, le nombre d'états qui mènent des activités d'ingérence en ligne a augmenté depuis janvier 2019 et les activités en ligne parrainées par l'état continueront probablement à viser le discours politique du Canada[106].

CST, *Cyberactivité malveillante ciblant les fournisseurs de services gérés*, 4 avril 2017, https://www.cyber.gc.ca/fr/avis/cyberactivite-malveillante-ciblant-les-fournisseurs-de-services-geres; et PricewaterhouseCoopers, *Operation Cloud Hopper*, avril 2017, https://www.pwc.co.uk/cyber-security/pdf/cloud-hopper-report-final-v4.pdf.

[99] Selon le CST, l'Iran ***, et les acteurs de cybermenace chinois ont tenté d'obtenir accès ***. CCC, *Portrait des cybermenaces qui pèsent sur le Canada : Le point sur 2019 et prévisions pour 2020*, 1er décembre 2019; et CST, *** Strategic Cyber Threat Assessment, mars 2018.

[100] CST, *** Strategic Cyber Threat Assessment, mars 2018.

[101] Smith, Rebecca, « Russian Hackers Reach U.S. Utility Control Rooms, Homeland Security Officials Say », *The Wall Street Journal*, 24 juillet 2018, https://www.wsj.com/articles/russian-hackers-reach-u-s-utility-control-rooms-homeland-security-officials-say-1532388110; et département de la sécurité intérieure des États-Unis, Cybersecurity and Infrastructure Security Agency, « Russian Government Cyber Activity Targeting Energy Sector and Other Critical Infrastructure Sectors », 15 mars 2018, https://us-cert.cisa.gov/ncas/alerts/TA18-074A.

[102] CST, *** Strategic Cyber Threat Assessment, mars 2018.

[103] CCC, *Portrait des cybermenaces qui pèsent sur le Canada : Le point sur 2019 et prévisions pour 2020*, 1er décembre 2019.

[104] CST, « Activité malveillante d'influence en ligne », *Évaluation des cybermenaces nationales 2018*, 1er décembre 2019, https://www.cyber.gc.ca/fr/orientation/activites--malveillantes-dinfluence-en-ligne.

[105] Le CST indique que ***. CCC, *Canada's Cyber Threat Landscape: Overview and Outlook for 2019*, 30 janvier 2019.

[106] CCC, ***, octobre 2018; et CCC, *Portrait des cybermenaces qui pèsent sur le Canada : Le point sur 2019 et prévisions pour 2020*, 1er décembre 2019.

74. Les élections sont une cible précieuse de désinformation et l'influence en ligne. Par exemple, avant les élections présidentielles américaines de 2016, l'Internet Research Agency, un organisme de recherche sur Internet établi en Russie, a fait la promotion de contenu très controversé de nature à créer des divisions et pour lequel l'organisme et plusieurs de ses employés ont fait l'objet de chefs d'accusation déposés par le département de la justice américain pour des [traduction] « opérations qui perturbent les élections et les processus politiques[107] ». Les élections fédérales canadiennes de 2019 ne semblent pas avoir été une cible importante de désinformation et d'ingérence en ligne. Le *Rapport sur l'évaluation du protocole public en cas d'incident électoral majeur*, remis au Comité en septembre 2020, a conclu qu'il semble y avoir eu une activité d'origine étrangère dans les médias sociaux pendant la période électorale, mais que « les effets de cette activité, tout comme ceux de l'activité d'origine canadienne dans les médias sociaux durant cette période, ne semblent pas avoir été importants »[108].

Cybersuivi et cybersurveillance de dissidents et d'autres personnes

75. Les acteurs de cybermenace perfectionnés et parrainés par l'État ont développé des moyens sophistiqués afin de prendre pour cible des personnes, comme des adversaires politiques ou des dissidents. Ces activités de cybermenace exploitent les vulnérabilités dans les systèmes de communication mondiaux aux fins d'espionnage ou de géolocalisation, ou pour modifier, ajouter ou supprimer du contenu sur un appareil mobile d'un utilisateur ciblé[109].

76. D'après le CST, *** pour cibler des personnes d'intérêt au Canada[110]. Le CST estime que ***[111] [*** Trois phrases ont été revues pour supprimer l'information préjudiciable ou privilégiée. Elles décrivent une évaluation du CST sur le ciblage de personnes au Canada. ***][112] ***[113] De plus, l'assassinat du dissident saoudien Jamal Kashoggi en 2018 est un exemple horrible d'états qui ont recours à des moyens de cybermenace avancés pour s'en prendre à des activistes des droits de la personne, à des dissidents, à des avocats et à des journalistes[114]. Selon une étude sur un cybermoyen actuel pour les appareils mobiles, un cyberoutil a permis de faire le suivi, le ciblage et la surveillance par

---

[107] Département de la justice des États-Unis, *Grand Jury Indicts Thirteen Russian Individuals and Three Russian Companies for Scheme to Interfere in the United States Political System*, 16 février 2018, https://www.justice.gov/opa/press-release/file/1035562/download.

[108] Jim Judd, *Rapport sur l'évaluation du protocole public en cas d'incident électoral majeur*, mai 2020.

[109] CST, *Déclaration concernant la couverture actuelle consacré au SS7*, 25 avril 2014, https://www.cse-cst.gc.ca/fr/media/2018-04-25; et Brigitte Bureau, Catherine Cullen et Kristen Everson, « Hackers only needed a phone number to track this MP's cellphone », *CBC*, 22 novembre 2017, https://www.cbc.ca/news/politics/hackers-cellphone-security-1.4406338.

[110] CCC, *Portrait des cybermenaces qui pèsent sur le Canada : Le point sur 2019 et prévisions pour 2020*, 1er décembre 2019.

[111] CCC, *** 1er juillet 2019.

[112] CCC, *** 1er juillet 2019.

[113] CCC, *** 1er juillet 2019.

[114] Business and Human Rights Resource Centre, « NSO Group allegedly provided software to Saudi Govt. to spy on Khashoggi; Citizen Lab who reported it in turn targeted by undercover agents », 28 janvier 2019, https://www.business-humanrights.org/en/nso-group-allegedly-provided-software-to-saudi-govt-to-spy-on-khashoggi-citizen-lab-who-reported-it-in-turn-targeted-by-undercover-agents ; et Oren Liebermann, « How a hacked phone may have led killers to Khashoggi », *CNN*, 20 janvier 2019, https://www.cnn.com/2019/01/12/middleeast/khashoggi-phone-malware-intl/index.html.

des cybermoyens cachés de personnes dans 45 pays, ce qui est caractéristique de l'utilisation de ces technologies à l'échelle mondiale[115].

Pandémie de COVID-19

77. Les acteurs de cybermenace étatiques et non étatiques ont pris avantage de la crise sanitaire mondiale causée par la pandémie de COVID-19 pour faire avancer leurs intérêts stratégiques, menant à une augmentation des cyberactivités depuis janvier 2020. Le CST estime que les acteurs parrainés par l'État, principalement ***, ont pris pour cible le secteur de la santé du Canada pour obtenir de l'information, probablement en réponse à de nouvelles exigences en matière de collecte de renseignements liés à la COVID-19[116]. Plus précisément, le CST souligne que ces acteurs ont démontré un intérêt dans l'information liée à la recherche et au développement relatifs aux vaccins, à l'équipement médical et à la coordination des interventions. Le CST estime que la menace se poursuivra probablement pour la durée de la pandémie[117].

78. Depuis janvier 2020, le CST a remarqué une augmentation des cyberattaques *** contre des cibles canadiennes[118]. Les organisations de recherche et de développement liés à la COVID-19 (p. ex. sur les vaccins ou les tests rapides) ou qui détiennent des données sensibles liées à l'intervention du Canada par rapport à la COVID-19 courent particulièrement un risque. Le CST souligne qu'environ *** des tentatives de cybercompromission *** visaient le secteur de la santé[119]. Au cours de la même période, *** a concentré *** tentatives de compromission contre le secteur de la santé[120]. Dans l'ensemble, le CST estime que la pandémie [*** La phrase suivante a été revue pour supprimer l'information préjudiciable ou privilégiée. Elle décrit une évaluation du CST de l'impact de la pandémie sur les cyberactivités de certains états. ***][121]

79. La pandémie a eu des répercussions sur d'autres types d'activités de cybermenace. [*** Deux phrases ont été revues pour supprimer l'information préjudiciable ou privilégiée. Elles décrivent une évaluation du SCRS des impacts potentiels de la pandémie sur les opérations d'états étrangers hostiles. ***][122] ***[123] Enfin, le SCRS a attiré l'attention sur l'utilisation accrue de technologies de surveillance de masse dans plusieurs pays utilisées dans les applications de recherche des contacts liées à la COVID-19 et mentionne les risques à long terme pour la vie privée que représentent ces applications à l'extérieur du Canada[124].

---

[115] Bill Marczak, John Scott-Railton, Sarah McKune, Bahr Abdul Razzak et Ron Deibert, « Hide and Seek: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries », *Citizen Lab*, 18 septembre 2018, https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/.
[116] CCC, *Cyber Threat Brief: State Activity against Canada January to June 2020*, 26 juin 2020.
[117] CCC, *Cyber Threat Brief: State Activity against Canada January to June 2020*, 26 juin 2020.
[118] CCC, *Cyber Threat Brief: State Activity against Canada January to June 2020*, 26 juin 2020.
[119] CCC, *Cyber Threat Brief: State Activity against Canada January to June 2020*, 26 juin 2020.
[120] CCC, *Cyber Threat Brief: State Activity against Canada January to June 2020*, 26 juin 2020.
[121] CCC, *Cyber Threat Brief: State Activity against Canada January to June 2020*, 26 juin 2020.
[122] SCRS, *** 2020.
[123] SCRS, *** 2020; et SCRS, *** 2020.
[124] SCRS, *** 2020.

80. Les acteurs étatiques ont également déplacé l'objet de leur activités d'ingérence en ligne vers la pandémie. À la fin de février 2020, les représentants américains ont accusé la Russie d'avoir répandu de la fausse information sur la COVID-19 dans une campagne coordonnée. Au début de janvier, des milliers de comptes sur Twitter, Facebook et Instagram, dont plusieurs avaient déjà été liés à la Russie, ont commencé à publier en anglais, en allemand, en français et dans d'autres langues des messages presque identiques qui jetaient le blâme de la pandémie sur les États-Unis. Certains des messages indiquaient que le virus faisait partie d'un effort des États-Unis visant à faire une guerre économique à la Chine, tandis que d'autres disaient qu'il s'agissait d'une arme biologique créée par la Central Intelligence Agency (CIA)[125].

Principales conclusions

81. Les cybermenaces présentent un risque grave et croissant pour la sécurité nationale du Canada. Des acteurs étatiques, surtout la Chine et la Russie, continuent de prendre pour cible les réseaux gouvernementaux, les institutions publiques et les entreprises privées aux fins de cyberespionnage. Ces acteurs continuent de renforcer leurs moyens pour cibler les infrastructures essentielles, mener des campagnes d'ingérence en ligne et surveiller les dissidents à l'étranger. La pandémie a fait manifestement ressortir ces menaces, en particulier les menaces qui planent sur le secteur de la santé du Canada. Le Comité présentera son examen des cybermoyens de défense du gouvernement au premier ministre en 2021.

[125] Jessica Glenza, « Coronavirus: US says Russia behind disinformation campaign », *The Guardian*, 22 février 2020, https://www.theguardian.com/world/2020/feb/22/coronavirus-russia-disinformation-campaign-us-officials; et Bruce Schneier, « Security of Health Information », *Schneier on Security*, 5 mars 2020, https://www.schneier.com/blog/archives/2020/03/security_of_hea.html.

Crime organisé d'envergure

Aperçu

82. Dans son Rapport annuel 2018, le Comité a indiqué que les répercussions du crime organisé sont énormes et insidieuses. Les groupes du crime organisé mènent des activités criminelles traditionnelles, comme le trafic illégal de drogue, d'armes et de marchandises illicites; la traite de personnes; et les crimes financiers, comme la fraude, les activités de jeu illégales et la manipulation des marchés. Les activités illégales des groupes du crime organisé d'envergure continuent d'engendrer des coûts élevés pour la société et de présenter des risques importants pour le Canada. Au cours des deux dernières décennies, ces activités sont devenues de plus en plus complexes et recherchées. Toutefois, la nature de la menace n'a pas changé de façon marquée depuis 2018.

Description de la menace

83. Le crime organisé d'envergure demeure une menace importante pour la sécurité nationale. Les groupes du crime organisé continuent de mener des activités criminelles traditionnelles, comme le trafic illégal de drogue, d'armes et de marchandises illicites; la traite de personnes; et les crimes financiers, comme la fraude, les activités de jeu illégales et la manipulation des marchés. Les groupes du crime organisé se servent du blanchiment d'argent pour dissimuler les profits de leurs crimes et ont recours à de la violence extrême, y compris le meurtre, dans le cadre de leurs activités. De plus, au cours des deux dernières décennies, les activités de groupes du crime organisé d'envergure sont devenues de plus en plus complexes et recherchées[126]. Les mêmes avancées technologiques qui ont permis d'accélérer la circulation de personnes, d'argent, d'informations et de marchandises ont également permis aux groupes du crime organisé de tisser des réseaux criminels complexes à l'échelle mondiale. Comme l'a souligné l'Office des Nations Unies contre la drogue et le crime, ces réseaux ont fait en sorte que le crime organisé [traduction] « a prospéré, s'est diversifié et a élargi la portée de ses activités[127]. »

84. Le crime organisé comprend de nouveaux secteurs d'activité : la cybercriminalité, le crime contre l'identité, le trafic de biens culturels et le trafic d'organes[128]. Interpol a également souligné que « avec des revenus évalués en milliards de dollars, les activités des réseaux criminels se présentent comme celles de sociétés internationales légitimes. Elles s'appuient sur des modèles opérationnels, des stratégies à long terme, des hiérarchies, et même sur des alliances stratégiques, qui servent un seul et même but : générer le maximum de profits avec le minimum de risque[129]. »

---

[126] Canada, *Response to the Standing Committee on Justice and Human Rights Report entitled L'état du crime organisé*, le 18 juillet 2012, https://www.noscommunes.ca/DocumentViewer/fr/41-1/JUST/rapport-7/reponse-8512-411-700.
[127] Office des Nations Unies contre la drogue et le crime, *Organized Crime*, sans date, https://www.unodc.org/unodc/en/organized-crime/intro.html.
[128] Office des Nations Unies contre la drogue et le crime, *Emerging Crimes*, sans date, https://www.unodc.org/unodc/en/organized-crime/intro/emerging-crimes.html.
[129] Interpol, *Criminalité organisée*, sans date, https://www.interpol.int/fr/Infractions/Criminalite-organisee.

Le crime organisé au Canada

85. Au Canada, le crime organisé est omniprésent. Le *Code criminel* définit une organisation criminelle comme étant un groupe composé d'au moins trois personnes se trouvant au Canada ou à l'étranger dont l'un des principaux objectifs est de commettre ou de faciliter des infractions graves qui pourraient lui procurer un avantage matériel. Le Service canadien de renseignements criminels (SCRC) de la GRC a relevé plus de 1 850 groupes du crime organisé ayant sévi au Canada en 2019[130], ce qui représente une augmentation marquée par rapport à 2011, où on avait répertorié entre 700 et 900 groupes[131].

86. La majorité des groupes recensés par le SCRC ne présentent pas une menace à la sécurité nationale et ne relèvent pas du mandat du Comité. Toutefois, le SCRC a déterminé que 14 groupes du crime organisé constituent une grande menace, c'est-à-dire qu'ils comportent des réseaux interprovinciaux; qu'ils possèdent, dans presque tous les cas, des connections internationales; qu'ils ont pénétré de multiples marchés criminels; et qu'ils ont recours à la violence pour servir leurs intérêts criminels[132]. La définition des groupes représentant le plus haut niveau de menace selon le SCRC correspond à la définition des menaces pour la sécurité nationale selon le Comité, c'est-à-dire les menaces envers la sécurité du Canada telles qu'elles sont définies dans la Loi sur le SCRS ou une criminalité d'envergure ou de gravité nationale. Ces 14 organisations participent principalement au trafic de drogue et au blanchiment d'argent d'envergure, elles se servent de l'économie légale au profit de leurs intérêts criminels, et elles peuvent exercer leurs activités de l'étranger. Des 14 groupes répertoriés par le SCRC, 12 constituaient une menace modérée et sont devenues une grande menace au cours des cinq dernières années. Les deux autres groupes ont maintenu leur statut de grande menace et sont bien enracinés au Canada. De juillet 2018 à septembre 2020, la GRC a mené *** enquête(s) prioritaire(s) liée(s) au crime organisé grave transnational[133].

Le crime organisé d'envergure au Canada : le commerce illégal de drogue

87. Le commerce illégal de drogue est la source de financement la plus lucrative pour les groupes du crime organisé au Canada[134]. En 2018, plus de 90 % des groupes du crime organisé au Canada étaient impliqués dans au moins un marché de drogue illicite[135]. Il est indiqué dans le rapport sur le crime organisé de 2019 du SCRC que les cinq groupes présentant une grande menace font partie des plus importants réseaux d'importation de cocaïne au Canada, et collaborent notamment avec les cartels de

---

[130] Service canadien de renseignements criminels (SCRC), *Rapport public sur les crimes graves et le crime organisé 2019*, décembre 2019.
[131] SCRC, Témoignages devant le Comité permanent de la justice et des droits de la personne, le 16 février 2012, https://www.noscommunes.ca/DocumentViewer/fr/41-1/JUST/reunion-21/temoignages.
[132] SCRC, *Rapport public sur les crimes graves et le crime organisé 2019*, décembre 2019.
[133] GRC, *Tiered Project Activity Report*, 27 novembre 2020.
[134] SCRC, *Prévision nationale du renseignement criminel 2018-2019 sur les marchés criminels canadiens — Drogues illicites*, 29 avril 2019, https://cisc-scrc.gc.ca/nps-psn/ncie-pnrc-fra.htm.
[135] SCRC, *Prévision nationale du renseignement criminel 2018-2019 sur les marchés criminels canadiens — Drogues illicites*, 29 avril 2019, https://cisc-scrc.gc.ca/nps-psn/ncie-pnrc-fra.htm.

drogue du Mexique et de la Colombie. Ces groupes importent jusqu'à 1 000 kilogrammes de cocaïne au Canada par mois.

88. Selon le SCRC, le commerce illégal de drogue a pris de l'ampleur, surtout en ce qui a trait au fentanyl et à la méthamphétamine. Le marché illicite du cannabis a diminué depuis la légalisation du cannabis; et les groupes du crime organisé laissent l'héroïne de côté pour passer au fentanyl, surtout dans l'ouest du Canada[136]. Cinq groupes du crime organisé présentant une grande menace font partie d'importants réseaux de méthamphétamine, ce qui comprend le détournement de produits chimiques non réglementés au Canada et l'importation de produits chimiques précurseurs de Chine et du Mexique pour la production de méthamphétamine et de fentanyl[137].

Crime organisé d'envergure : blanchiment d'argent

89. Le blanchiment d'argent au nom du crime organisé représente la plus grande menace de financement illicite envers le Canada. Le gouvernement prévoit une augmentation du nombre d'activités de blanchiment d'argent au cours des prochaines années[138]. Le blanchiment d'argent permet aux groupes du crime organisé d'envergure de blanchir leurs propres produits de la criminalité ou d'offrir le service à titre de fournisseur tiers à d'autres organisations criminelles. Il est indiqué dans le rapport sur le crime organisé de 2019 du SCRC qu'au moins quatre groupes qui constituent une grande menace fournissent des services de blanchiment d'argent à grande échelle au Canada pour les trafiquants de drogue internationaux. Les groupes du crime organisé mènent leurs activités de blanchiment d'argent par l'entremise de casinos, du système bancaire clandestin, des activités de jeu illégales (y compris les maisons de pari illicites et les sites Web d'activités de jeu illégales), des sociétés écran et des prête-noms, du blanchiment d'argent par voie commerciale et des investissements immobiliers[139]. L'intégration de recettes obtenues illégalement dans les marchés légaux compromet l'intégrité des systèmes financiers du Canada, altère les marchés, crée de l'instabilité et entraîne la corruption au sein de l'industrie et du gouvernement.

90. L'Office des Nations Unies contre la drogue et le crime estime que de 2 à 5 % du PIB mondial, ou entre 800 milliards et 2 billions de dollars américains, font l'objet de blanchiment d'argent dans le monde chaque année[140]. Au Canada, l'estimation la plus élevée de fonds blanchis au pays s'élève à 100 milliards de dollars canadiens[141]. Le blanchiment d'argent par des membres du crime organisé par

---

[136] SCRC, *Prévision nationale du renseignement criminel 2018-2019 sur les marchés criminels canadiens — Drogues illicites*, 29 avril 2019, https://cisc-scrc.gc.ca/nps-psn/ncie-pnrc-fra.htm.

[137] SCRC, *Prévision nationale du renseignement criminel 2018-2019 sur les marchés criminels canadiens — Drogues illicites*, le 29 avril 2019, https://cisc-scrc.gc.ca/nps-psn/ncie-pnrc-fra.htm.

[138] Bureau du Conseil privé, *National Intelligence Assessment: Global Illicit Financing Issues and Canadian Touchpoints*, NIA 9/2019, 2019.

[139] SCRC, *Rapport public sur les crimes graves et le crime organisé 2019*, décembre 2019.

[140] Office des Nations Unies contre la drogue et le crime, *Money-Laundering and Globalization*, sans date, https://www.unodc.org/unodc/en/money-laundering/globalization.html.

[141] Dans un commentaire pour C. D. Howe, Denis Meunier a indiqué que le montant de 100 milliards de dollars était l'estimation la plus élevée, alors que le Groupe d'experts sur le blanchiment d'argent dans le secteur immobilier en Colombie-Britannique a relevé une estimation « conservatrice » d'environ 46,7 milliards de dollars en 2018. Dans une autre publication de C. D. Howe, Kevin Comeau a fourni une estimation de 130 milliards de dollars, mais elle est [traduction] « très approximative, et

l'entremise de casinos et du marché immobilier en Colombie-Britannique constitue l'exemple le plus connu et discuté publiquement au Canada[142]. En 2018, le Groupe d'experts sur le blanchiment d'argent dans le secteur immobilier en Colombie-Britannique a estimé que 7,4 milliards de dollars avaient été blanchis dans la province, dont 5 milliards de dollars par l'entremise du marché immobilier[143]. Les membres du groupe d'experts ont constaté que les fonds blanchis ont fait monter le prix des habitations d'environ 5 % dans l'ensemble de la province, rendant le marché de l'habitation inaccessible pour de nombreux segments de la population[144].

91. Des augmentations semblables ont eu lieu au sein d'autres marchés immobiliers canadiens. Transparency International Canada estime que, entre 2008 et 2018, plus de 20 milliards de dollars sont entrés dans le marché immobilier de la région du Grand Toronto en dehors du régime législatif actuel et donc sans diligence raisonnable ou sans examen par le Centre d'analyse des opérations et déclarations financières du Canada (CANAFE). Cette estimation comprenait 9,8 milliards de dollars utilisés dans le cadre de transactions en argent comptant, et 10,4 milliards de dollars dans le cadre d'achats par des acheteurs commerciaux ayant recours à des prêteurs non réglementés qui mènent leurs activités en dehors du cadre de lutte contre le blanchiment d'argent au Canada[145]. Il ne s'agit que d'un seul exemple de la manière dont les groupes du crime organisé distribuent leurs actifs et répartissent leurs transactions financières dans le but de limiter la détection de leurs activités criminelles et de se soustraire au cadre de lutte contre le blanchiment d'argent au Canada[146].

92. Le blanchiment d'argent par voie commerciale constitue une question de plus en plus préoccupante pour le Canada. Le Groupe d'action financière, l'organisme international responsable d'établir les normes et les pratiques exemplaires mondiales en matière de lutte contre le blanchiment d'argent et le financement des activités terroriste, définit le blanchiment d'argent par voie commerciale comme étant [traduction] « un processus visant à dissimuler les produits de la criminalité et à se servir

---

on devrait seulement s'y fier à titre d'indice de l'ampleur du problème. » Néanmoins, ces montants représentent tous la dure réalité que d'importants montants d'argent sont blanchis au Canada. Denis Meunier, « Hidden Beneficial Ownership and Control: Canada as a Pawn in the Global Game of Money Laundering », *C.D. Howe Institute*, commentaire nº 519, septembre 2018, https://www.cdhowe.org/sites/default/files/attachments/research_papers/mixed/Final%20for%20advance%20release%20Commentary_519_0.pdf.

[142] Sam Cooper, « How Chinese gangs are laundering drug money through Vancouver real estate », *Global News*, 5 juin 2018. https://globalnews.ca/news/4149818/vancouver-cautionary-tale-money-laundering-drugs/; et Stephanie Ip, « Money Laundering in B.C.: Timeline of how we got here », *Vancouver Sun*, 15 mai 2019, https://vancouversun.com/news/local-news/money-laundering-in-b-c-timeline-of-how-we-got-here/.

[143] Le Groupe d'experts sur le blanchiment d'argent dans le secteur immobilier en Colombie-Britannique, *Combatting Money Laundering in BC Real Estate*, gouvernement de la Colombie-Britannique, 31 mars 2019, https://news.gov.bc.ca/files/Combatting_Money_Laundering_Report.pdf.

[144] Le Groupe d'experts sur le blanchiment d'argent dans le secteur immobilier en Colombie-Britannique, *Combatting Money Laundering in BC Real Estate*, gouvernement de la Colombie-Britannique, 31 mars 2019, https://news.gov.bc.ca/files/Combatting_Money_Laundering_Report.pdf.

[145] Transparency International Canada, *Opacity: Why Criminals Love Canadian Real Estate (And How to Fix It)*, 2019, https://static1.squarespace.com/static/5df7c3de2e4d3d3fce16c185/t/5e1e357c8460a6689db1c5f8/1579038078911/opacity.pdf.

[146] Comité permanent des finances de la Chambre des communes, *24e rapport : Lutte contre le blanchiment d'argent et le financement des activités terroristes : faire progresser le Canada*, 42e législature, 1re session, novembre 2018, https://www.ourcommons.ca/Content/Committee/421/FINA/Reports/RP10170742/finarp24/finarp24-f.pdf.

de transactions commerciales pour écouler des montants dans le but de rendre légale leur origine illicite[147]. » Selon le Groupe d'action financière, une méthode courante de blanchiment d'argent par voie commerciale implique une fausse déclaration sur le prix, la quantité ou la qualité des importations ou des exportations.[148] On ne connait pas l'ampleur du blanchiment d'argent par voie commerciale au Canada, mais l'ASFC estime qu'il s'élève au moins à quelques centaines de millions de dollars, et que cette activité se produit principalement à Toronto, à Montréal et à Vancouver[149]. Selon le renseignement, le blanchiment d'argent par voie commerciale est l'une des principales méthodes utilisées par les cartels de drogue du Mexique et de la Colombie[150].

93. La GRC est chargée de mener les enquêtes sur des cas de blanchiment d'argent par voie commerciale. Toutefois, cette méthode de blanchiment d'argent n'est pas très connue ou comprise, donc peu de cas sont renvoyés à la GRC. Par exemple, CANAFE n'a pas de pouvoirs conférés par la loi pour la collecte d'informations sur les transactions liées aux renseignements sur le crédit documentaire, ce qui crée des lacunes quant à la capacité de l'ASFC et des organismes de l'application de la loi d'établir des liens entre du financement douteux et des transactions commerciales. En réponse, le gouvernement a créé le Centre d'expertise sur la fraude commerciale et le blanchiment d'argent par voie commerciale au sein de l'ASFC en avril 2020, qui est chargé de repérer et d'intercepter la fraude commerciale complexe et de mener des enquêtes à ce sujet, et de renvoyer les dossiers de blanchiment d'argent par voie commerciale à la GRC[151].

Crime organisé d'envergure : pénétrer le marché légal

94. Les groupes du crime organisé participent activement à l'économie légale au profit du processus de blanchiment d'argent ou pour investir de l'argent soi-disant propre en vue de faire toujours plus de profits. En plus des activités criminelles variées susmentionnées, les groupes du crime organisé contrôlent des centaines d'entreprises de diverses industries, notamment les services alimentaires, le transport, la construction et le transport routier, la gestion immobilière, les finances et les prêts, les sociétés immobilières et les entreprises qui fonctionnent en argent comptant seulement[152]. Dans son message pour le rapport final de la *Commission d'enquête sur l'octroi et la gestion des contrats publics dans l'industrie de la construction*, France Charbonneau décrit clairement les défis liés au fait que le crime organisé s'incruste dans l'économie légale :

> Les répercussions de ce flux d'argent illicite dans l'économie légale sont dévastatrices à long terme. Les entreprises infiltrées par le crime organisé sont souvent converties en coquilles vides, privant la société de retombées liées à leurs activités, car elles sont transformées en investissements stériles, qui ne servent qu'à des fins de blanchiment d'argent. La présence du crime organisé dans certains secteurs

---

[147] Groupe d'action financière, *Trade Based Money Laundering*, 23 juin 2006.
[148] Groupe d'action financière, *Trade Based Money Laundering*, 23 juin 2006.
[149] ASFC, *Aperçu du blanchiment d'argent par voies commerciales*, CAPR_2020-JUIN-08, juin 2020.
[150] ASFC, *Aperçu du blanchiment d'argent par voies commerciales,* CAPR_2020-JUIN-08, juin 2020.
[151] ASFC, *Aperçu du blanchiment d'argent par voies commerciales,* CAPR_2020-JUIN-08, juin 2020.
[152] SCRC, *Rapport public sur les crimes graves et le crime organisé – Points saillants*, décembre 2019, https://cisc-scrc.gc.ca/media/2019/2019-12-06-fra.htm.

économiques décourage également les investisseurs. En s'immisçant dans l'économie légale, ces organisations criminelles blanchissent leur argent. Elles finissent par devenir intouchables alors que leur fortune est acquise illégalement par l'emploi de la violence [...][153]

Pandémie de COVID-19

95. La pandémie a offert des possibilités aux groupes du crime organisé. La GRC indique que le maintien des restrictions à la frontière pourrait entraîner une augmentation de la demande pour des marchandises licites et illicites, et le crime organisé pourrait en profiter[154]. La GRC souligne également une présence accrue des groupes du crime organisé sur le Web, surtout pour faciliter le trafic illégal de marchandises liées à la pandémie (c.-à-d. de l'équipement de protection individuelle, des masques et de l'équipement médical)[155]. L'ASFC estime que la pandémie a entraîné certains changements par rapport aux méthodes de contrebande des groupes du crime organisé, mais qu'il est peu probable que ces changements se traduisent en une diminution importante du trafic mondial de drogue au Canada au cours de la prochaine année. Selon l'ASFC, de petits groupes du crime organisé risquent d'être absorbés au sein de plus gros groupes, qui eux sont en mesure de s'adapter rapidement à l'évolution des restrictions liées à la pandémie[156].

Principales conclusions

96. Le crime organisé d'envergure présente toujours une menace importante pour la sécurité nationale. On estime que les produits de la criminalité se chiffrent dans les milliards de dollars, ce qui représente une importante perte de revenus pour les gouvernements et pourrait être la source d'autres activités criminelles. Au-delà de ces coûts se trouvent les ramifications sociétales et financières du crime organisé : il sape la primauté du droit, menace la sécurité publique et mine nos institutions financières, légales, politiques et sociales.

---

[153] France Charbonneau, *Rapport de la Commission d'enquête sur l'octroi et la gestion des contrats publics dans l'industrie de la construction*, Mot de la présidente, 24 novembre 2015, https://www.ceic.gouv.qc.ca/fileadmin/Fichiers_client/fichiers/Rapport_final/Rapport_final_CEIC_MotPresidente.pdf.
[154] GRC, *Impact of COVID-19 on Integrity, Organized Crime and Hostile State Activity*, 19 mars 2020.
[155] GRC, *Assessment of Federal Policing Priorities in the Age of COVID-19*, 15 mai 2020.
[156] ASFC, *Répercussions futures de la COVID-19 sur la contrebande de drogues au Canada*, ICAP_2020-SEP-003, août 2020.

Armes de destruction massive

Aperçu

97. Dans son Rapport annuel 2018, le Comité a indiqué que les armes de destruction massive et la prolifération de matériel et de technologies à double usage constituent une menace pour la sécurité nationale. Ces armes peuvent causer des accidents de masse aveugles ainsi que des dommages économiques et environnementaux à long terme. La menace envers le Canada que posent ces armes et leur prolifération est demeurée la même au cours des deux dernières années. Toutefois, certaines tendances, décrites plus loin, pourraient influencer cette évaluation. Voici les grandes lignes de ces tendances : le régime mondial de désarmement nucléaire s'est affaibli depuis 2018, et l'utilisation continue d'armes chimiques par des acteurs étatiques ou non étatiques a porté atteinte aux normes internationales; et les avancées technologiques ont facilité l'accès au matériel à double usage ainsi que la conception et la livraison d'armes chimiques et biologiques. De plus, le Canada demeure une cible d'approvisionnement illicite et clandestin de technologies à double usage par plusieurs acteurs étatiques. En outre, la pandémie de COVID-19 a permis de découvrir d'importantes vulnérabilités en ce qui a trait aux économies de l'état, aux secteurs de la santé et aux systèmes d'intervention.

Description de la menace

98. La conception, l'utilisation et la prolifération d'armes de destruction massive constituent une menace pour la sécurité du Canada et de ses alliés. Les armes chimiques, biologiques, radiologiques ou nucléaires peuvent causer des accidents de masse aveugles ainsi que des dommages économiques et environnementaux à long terme[157]. La prolifération de matériel et de technologies pouvant faciliter la conception et l'utilisation de ces armes par des acteurs étrangers étatiques ou non étatiques, notamment les systèmes de livraison, les articles à double usage ainsi que leur propriété intellectuelle connexe, constitue une autre question préoccupante[158].

99. Le désarmement et la non-prolifération des armes de destruction massive constituent une priorité pour l'Organisation des Nations Unies depuis sa création. Les traités internationaux visant à prévenir la prolifération des armes nucléaires, et, au bout du compte, à les éliminer complètement; de même que les conventions empêchant la conception, le transfert ou l'utilisation d'armes chimiques et biologiques, ont été acceptés presque à l'unanimité à l'échelle mondiale[159].

---

[157] Pour obtenir de plus amples renseignements : World Health Organization, « Biological Weapons », sans date, https://www.who.int/health-topics/biological-weapons#tab=tab_1 ; Organization for the Prohibition of Chemical Weapons, « What is a Chemical Weapon », sans date, https://www.opcw.org/work/what-chemical-weapon; et Nuclear Threat Initiative, « The Radiological Threat », 30 décembre 2015, https://www.nti.org/learn/radiological/.

[158] Sécurité publique Canada, *Renforcer le cadre canadien de lutte contre la prolifération*, 2018, https://www.securitepublique.gc.ca/cnt/rsrcs/pblctns/2018-strngthnng-cntr-prlfrtn-frmwrk/index-fr.aspx.

[159] Le Traité sur la non-prolifération des armes nucléaires est entré en vigueur en 1970 et 191 états en sont partie (l'Inde, Israël, la Corée du Nord et le Pakistan n'en sont pas partie). La Convention sur l'interdiction de la mise au point, de la fabrication et du stockage des armes bactériologiques (biologiques) ou à toxines et sur leur destruction est entrée en vigueur en 1975 et 182 états en font partie. La Convention sur l'interdiction de la mise au point, de la fabrication, du stockage et de l'usage des armes chimique et sur leur destruction est entrée en vigueur en 1997 et 193 états en font partie. Nuclear Threat Initiative, « Get the Facts NPT », novembre 2019, https://media.nti.org/documents/npt_fact_sheet.pdf; Arms Control Association,

100. Le Canada participe activement aux discussions concernant le désarmement à l'échelle internationale et a élaboré un cadre interministériel de lutte contre la prolifération en vue de prévenir l'acquisition, l'exportation ou le détournement d'articles préoccupants[160]. Les entreprises canadiennes et les établissements de recherche contribuent activement aux secteurs de l'énergie nucléaire, de la biotechnologie et des produits chimiques, devenant ainsi des cibles pour les proliférateurs et autres acteurs malveillants[161]. L'appareil de la sécurité et du renseignement tente d'éliminer la menace de prolifération en appliquant les lois visant à prévenir l'exportation de technologies à double usage, en examinant des investissements qui pourraient porter atteinte à la sécurité nationale et en menant des enquêtes sur des personnes ou des entreprises susceptibles de pratiquer des activités illicites dans ce domaine. La GRC *** enquête(s) sur cette question de juillet 2018 à septembre 2020[162]. Pour la même période, le SCRS a mené une/des enquête(s) liée(s) aux armes de destruction massive faisant l'objet d'un mandat contre *** cible(s) et *** organisation(s).[163]

101. Le désarmement et la non-prolifération se sont avérés plutôt efficaces depuis la mise en place d'un régime de contrôle des armes qui encadre ces armes. Seulement quatre états se sont procuré des armes nucléaires depuis l'entrée en vigueur du Traité sur la non-prolifération des armes nucléaires en 1970; le nombre total d'ogives nucléaires dans le monde a diminué; et aucune arme nucléaire n'a été utilisée dans le cadre d'un conflit depuis 1945[164]. Depuis que des conventions à ce sujet sont entrées en vigueur, aucune attaque d'envergure n'a été perpétrée à l'aide d'armes biologiques, et 96 % des réserves d'armes chimiques déclarées ont été éliminées[165]. Toutefois, des tendances des dernières années laissent croire que la situation pourrait se renverser. Selon le Bureau du Conseil privé, la dégradation de cadres de contrôle des armes à l'échelle mondiale, l'élaboration de nouveaux systèmes d'armes par plusieurs états possédant des armes nucléaires, et le ciblage continu du Canada par des acteurs étatiques ou non étatiques en ce qui a trait aux technologies à double usage pour la conception de nouvelles armes sont toutes source de préoccupations[166].

« Biological Weapons Convention Signatories and States-Parties », septembre 2018, https://www.armscontrol.org/factsheets/bwcsig; et Arms Control Association « Chemical Weapons Convention Signatories and States-Parties », juin 2018, https://www.armscontrol.org/factsheets/cwcsig.

[160] Sécurité publique Canada, *Renforcer le cadre canadien de lutte contre la prolifération*, 2018, https://www.securitepublique.gc.ca/cnt/rsrcs/pblctns/2018-strngthnng-cntr-prlfrtn-frmwrk/index-fr.aspx.

[161] Sécurité publique Canada, *Renforcer le cadre canadien de lutte contre la prolifération*, 2018, https://www.securitepublique.gc.ca/cnt/rsrcs/pblctns/2018-strngthnng-cntr-prlfrtn-frmwrk/index-fr.aspx

[162] GRC, *Tiered Project Activity Report*, 27 novembre 2020.

[163] SCRS, réponse par courriel au Secrétariat du CPSNR, 10 décembre 2020.

[164] Selon le Bureau des affaires de désarmement des Nations Unies, les seuls cas où des armes nucléaires ont été employées sont les bombardements d'Hiroshima et de Nagasaki par les États-Unis en 1945. Actuellement, neuf états possèdent des armes nucléaires, et cinq d'entre eux (la Chine, la France, le Royaume-Uni, les États-Unis et la Russie) possédaient des armes nucléaires au moment où le Traité sur la non-prolifération des armes nucléaires est entré en vigueur. La République populaire démocratique de la Corée (Corée du Nord), l'Inde, Israël et le Pakistan se sont procurés des armes nucléaires après l'entrée en vigueur du Traité, et ne sont pas partie au Traité. Bureau des affaires de désarmement des Nations Unies, « Armes de destruction massive », sans date, https://www.un.org/disarmament/fr/amd/armas-nucleares/; « World Nuclear Forces », *SIPRI Yearbook 2020*, 2020, https://www.sipri.org/yearbook/2020/10; et Tariq Rauf, « Is Past Prologue? Examining NPT Review Conference Commitments », UN Institute on Disarmament Research, sans date, https://unidir.org/publication/past-prologue-examining-npt-review-conference-commitments.

[165] Bureau des affaires de désarmement des Nations Unies, *Assurer notre avenir commun : un programme de désarmement*, 2018, https://front.un-arm.org/documents/SGDA_fr_web.pdf.

[166] BCP, *National Security Environment in a Less Multilateral World*, le 17 octobre 2019.

Armes nucléaires

102. Dans un article du Bulletin of the Atomic Scientists datant de janvier 2020, il est indiqué que [traduction] « le monde entier marche les yeux fermés vers un paysage nucléaire nouvellement instable[167]. » Deux tendances importantes dans le domaine des armes nucléaires ont fait surface au cours des cinq dernières années : l'affaiblissement du régime de désarmement nucléaire et la détérioration du milieu de la sécurité nucléaire.

103. Le régime de désarmement nucléaire s'affaiblit pour plusieurs raisons. Premièrement, des ententes bilatérales en matière de contrôle des armes à long terme entre les deux plus grandes puissances nucléaires, les États-Unis et la Russie, sont en jeu. Les États-Unis se sont retirés du Traité sur les forces nucléaires à portée intermédiaire en 2019 après avoir prétendu que la Russie avait enfreint le Traité. La seule entente bilatérale en matière de contrôle des armes toujours en vigueur entre les deux pays, l'accord New Strategic Arms Reduction (New START Treaty), vient à expiration en 2021, et son renouvellement est incertain[168]. Deuxièmement, les négociations au sujet du désarmement avec la Corée du Nord ont atteint un point mort, et le retrait unilatéral des États-Unis du Plan d'action global commun (PAGC), une entente multilatérale visant à limiter la capacité de l'Iran à développer des armes nucléaires, a incité l'Iran à reprendre certaines activités auparavant restreintes de son programme nucléaire[169]. Enfin, il y a peu de progrès en matière de désarmement nucléaire par les états possédant une arme nucléaire. Le nombre d'ogives nucléaires dans le monde a diminué, mais les états possédant une arme nucléaire continuent de moderniser leurs systèmes d'armes, et ils ont de mauvais antécédents en ce qui a trait au respect des engagements en matière de désarmement qu'ils ont pris lors de conférences d'examen du Traité sur la non-prolifération des armes nucléaires[170]. Cette faible cadence a entraîné une frustration de plus en plus marquée chez les états qui ne possèdent pas d'armes nucléaires et un fossé de plus en plus grand entre les deux groupes, ce qui compromet possiblement le régime mondial de désarmement dans son ensemble[171].

---

[167] John Mecklin, « Closer than ever: it is 100 seconds to midnight », *Bulletin of the Atomic Scientists*, 23 janvier 2020, https://thebulletin.org/doomsday-clock/current-time.

[168] John Mecklin, « Can the nuclear non-proliferation regime be saved when arms control is collapsing? », *Bulletin of the Atomic Scientists*, 24 février 2020, https://thebulletin.org/premium/2020-03/can-the-nuclear-nonproliferation-regime-be-saved-when-arms-control-is-collapsing/.

[169] MDN/FAC, *** 16 novembre 2020; Tongfi Kim, « The North Korean nuclear weapons programme and strategic stability in East Asia », *Reassessing CBRN Threats in a Changing Global Environment*, eds. Fei Su et Ian Anthony, SIPRI, juin 2019, https://www.sipri.org/sites/default/files/2019-06/1906_cbrn_threats_su_anthony_0.pdf; et John Mecklin, « Closer than ever: it is 100 seconds to midnight », *Bulletin of the Atomic Scientists*, le 23 janvier 2020, https://thebulletin.org/doomsday-clock/current-time.

[170] Tariq Rauf, « Is Past Prologue? Examining NPT Review Conference Commitments », UN Institute on Disarmament Research, sans date, https://unidir.org/publication/past-prologue-examining-npt-review-conference-commitments; Bureau des affaires de désarmement des Nations Unies, *Assurer notre avenir commun : un programme de désarmement*, 2018, https://front.un-arm.org/documents/SGDA_fr_web.pdf.; et Cheryl Rofer, « Low-Yield Nukes are a Danger, Not a Deterrent », *Foreign Policy*, 11 février 2020, https://foreignpolicy.com/2020/02/11/deterrence-nuclear-war-low-yield-nukes-danger-not-deterrent/.

[171] En juillet 2017, l'Assemblée générale des Nations Unies a adopté le Traité sur l'interdiction des armes nucléaires. Les états possédant des armes nucléaires ont défendu que ce Traité met en cause le Traité sur la non-prolifération des armes nucléaires. Dr. Tytti Erasto et Dr. Tarja Cronberg, « Opposing Trends: the Renewed Salience of Nuclear Weapons and Nuclear Abolitionism », *SIPRI*, septembre 2018, https://www.sipri.org/publications/2018/sipri-insights-peace-and-security/opposing-trends-renewed-salience-nuclear-weapons-and-nuclear-abolitionism.

104. Les organisations faisant partie de l'appareil de la sécurité et du renseignement ont attiré l'attention sur la modernisation continue des systèmes de missiles. Selon le ministère de la Défense nationale et les Forces armées canadiennes (MDN/FAC), la Chine demeure au premier rang de la mise à l'essai et de la conception de missiles balistiques, tandis que la Corée du Nord, l'Iran et la Russie ont gardé un rythme stable pour la mise à l'essai de missiles durant la même période[172].

105. La menace envers le Canada liée à l'utilisation d'armes nucléaires provient seulement de la Russie et de la Chine, qui envisageraient probablement de frapper des cibles canadiennes dans un conflit nucléaire avec les États-Unis. Le MDN/FAC estime que même si les deux pays poursuivent la modernisation de leur arsenal nucléaire, leurs principaux objectifs stratégiques demeurent d'empêcher une attaque nucléaire ou une attaque traditionnelle de grande importance[173]. Les capacités nucléaires et de missiles de la Corée du Nord ont augmenté depuis 2018 et le pays ne cesse de développer ses capacités de frapper les États-Unis. Même si les activités nucléaires de l'Iran suscitent des préoccupations, [*** La phrase suivante a été revue pour supprimer l'information préjudiciable ou privilégiée. Elle décrit une évaluation du MDN/FAC. ***][174]

106. La possibilité que des groupes terroristes acquièrent des armes nucléaires ne préoccupe pas l'appareil de la sécurité et du renseignement. Le SCRS estime que, [*** Deux phrases ont été revues pour supprimer l'information préjudiciable ou privilégiée. Elles décrivent une évaluation du SCRS. ***][175] ***[176] Dans un contexte de sécurité nucléaire et radiologique, l'Agence internationale de l'énergie atomique a enregistré plus de 450 incidents de contrebande ou de possession non autorisée de matériel nucléaire (pas des armes) et plus de 700 incidents impliquant le vol ou la perte de matériel nucléaire depuis les années 1990[177]. L'indice de sécurité des matières nucléaires de 2020 de l'Initiative contre la menace nucléaire indique que les progrès en matière de sécurité nucléaire à l'échelle mondiale ont [traduction] « considérablement ralenti » depuis 2018 et que les lacunes qui persistent en matière de sécurité rendent le matériel ou les installations nucléaires vulnérables face à la menace et au sabotage[178]. Des experts ont également soulevé des préoccupations en ce qui a trait au risque que des cyberattaques soient dirigées contre des installations nucléaires[179]. Cependant, dans le contexte canadien, la Commission canadienne de sûreté nucléaire indique que toutes les installations nucléaires

---

[172] MDN/FAC, ***, 6 février 2020.
[173] MDN/FAC, 2020 Strategic Threat Overview, exposé devant le Secrétariat du CPSNR, 13 octobre 2020; et MDN/FAC, *Global: Strike Threats Against North America*, 15 juillet 2018.
[174] MDN/FAC, *Global: Strike Threats Against North America*, 15 juillet 2018; et MDN/FAC, « Excerpt from *** 16 novembre 2020
[175] SRCS, *Évaluation conjointe de la menace avec le Group scientifique, technique et du renseignement (STIG) 2018,*** 2018.
[176] SCRS, *Évaluation conjointe de la menace avec le Group scientifique, technique et du renseignement (STIG) 2018,*** 2018.
[177] Affaires mondiales Canada, « Le Canada et la non-prolifération, le contrôle des armes et le désarmement », 2017, https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/peace_security-paix_securite/weapons_mass_destruction-armes_destruction_massive.aspx?lang=fra.
[178] Nuclear Threat Initiative, « Losing Focus in a Disordered World », *2020 Nuclear Security Index*, juillet 2020, https://www.nti.org/analysis/reports/2020-nti-nuclear-security-index/.
[179] "Nuclear Threat Initiative, « Losing Focus in a Disordered World », 2020 Nuclear Security Index, juillet 2020, https://www.nti.org/analysis/reports/2020-nti-nuclear-security-index/.

exerçant des activités au Canada respectent des règles strictes en matière de cybersécurité et font régulièrement l'objet d'examens et d'inspections visant à assurer leur conformité continue[180].

Armes chimiques

107. Un autre risque touche l'affaiblissement des normes relatives à l'utilisation d'armes chimiques. Au cours de la dernière décennie, on s'est servi d'armes chimiques à répétition dans le cadre de conflits et d'assassinats ciblés. Durant la guerre civile en Syrie, l'équipe de mission d'enquête conjointe de l'Organisation pour l'interdiction des armes chimiques et des Nations Unies a découvert que des armes chimiques avaient été utilisées à maintes reprises par des acteurs étatiques ou non étatiques depuis 2013[181]. Le MDN/FAC estime que le régime syrien a employé à de nombreuses reprises des armes chimiques depuis l'ouverture d'hostilités et que Daech a utilisé des substances chimiques *** en Syrie, ***[182] L'utilisation d'armes chimiques dans le cadre d'assassinats ciblés au cours des trois dernières années, malgré l'imposition de sanctions et de condamnations internationales, compromet également les normes interdisant l'utilisation de ces armes[183]. En février 2017, le gouvernement de la Corée du Nord a ordonné l'assassinat de Kim Jong-nam, le frère du dirigeant de la Corée du Nord, Kim Jong-un, au moyen de l'agent neurotoxique VX en Malaisie[184]. En mars 2018, des agents de renseignement russe ont empoisonné l'ancien espion russe Sergeï Skripal et sa fille Ioulia au moyen d'un agent neurotoxique à Salisbury, au Royaume-Uni[185]. En août 2020, des agents de renseignement russes ont empoisonné le chef de l'opposition russe Alexei Navalny avec un agent neurotoxique de la même catégorie en Russie[186].

108. La prolifération d'armes chimiques constitue une autre préoccupation. Selon l'Initiative contre la menace nucléaire, les armes chimiques représentent [traduction] « l'arme de destruction massive dont l'utilisation et la prolifération sont les plus importantes[187]. » Certaines substances servant à la conception d'armes chimiques ont des utilisations légitimes et sont hautement réglementées. Cependant, les avancées technologiques de la dernière décennie, y compris les technologies et les chaînes d'approvisionnement qui peuvent faciliter la livraison de matériel et d'armes chimiques,

---

[180] Eric Lemoine, « CNSC Cyber Security program for NPPS: The Present and the Future », Commission canadienne de sûreté nucléaire, mars 2020.
[181] Arms Control Association, « Timeline of Syrian Chemical Weapons Activity, 2012-2020 », mars 2020, https://www.armscontrol.org/factsheets/Timeline-of-Syrian-Chemical-Weapons-Activity; et Sadik Toprak, « Trends in recent CBRN incidents », *Reassessing CBRN Threats in a Changing Global Environment*, eds. Fei Su et Ian Anthony, SIPRI, juin 2019, https://www.sipri.org/sites/default/files/2019-06/1906_cbrn_threats_su_anthony_0.pdf.
[182] MDN/FAC, *Syria: Chemical Weapon Attack* *** 16 avril 2018.
[183] Sadik Toprak, « Trends in recent CBRN incidents », *Reassessing CBRN Threats in a Changing Global Environment*, eds. Fei Su et Ian Anthony, SIPRI, juin 2019, https://www.sipri.org/sites/default/files/2019-06/1906_cbrn_threats_su_anthony_0.pdf.
[184] Hannah Ellis Peterson et Benjamin Haas, « How North Korea got away with the assassination of Kim Jong-nam », *The Guardian*, 1er avril 2019, https://theguardian.com/world/2019/apr/01/how-north-korea-got-away-with-the-assassination-of0kim-jong-nam.
[185] BBC News, « Russian spy poisoning: what we know so far », *BBC*, 8 octobre 2018, https://www.bbc.com/news/uk-44315636.
[186] Dan Sabbagh et Luke Harding, « Kremlin meant to kill Navalny, western security agencies believe », *The Guardian*, 16 novembre 2020, https://www.theguardian.com/world/2020/nov/16/kremlin-alaexei-navalny-western-security-agencies-novichok.
[187] Nuclear Threat Initiative, « The Chemical Threat », 30 décembre 2015, https://www.nti.org/learn/chemical/.

pourraient nuire aux futurs efforts de lutte contre la prolifération[188]. Le SCRS laisse entendre que de récents incidents liés à l'utilisation d'armes chimiques ont permis de sensibiliser et d'informer le public concernant ces armes, et pourraient donc changer le contexte de la menace en matière d'armes chimiques[189]. Des chercheurs ont mentionné que des groupes terroristes comme al-Qaïda ont cherché à obtenir des armes chimiques, et l'équipe de mission d'enquête conjointe de l'OIAC et des Nations Unies a découvert des situations où le groupe Daech s'est servi d'armes chimiques en Syrie[190]. Le SCRS estime [*** Deux phrases ont été revues pour supprimer l'information préjudiciable ou privilégiée. Elles décrivent une évaluation du SCRS des risques associés aux groupes terroristes et la prolifération. ***][191] ***[192]

Armes biologiques

109. Des préoccupations semblables ont été soulevées quant à la prolifération d'armes biologiques et à la capacité des pays d'intervenir face à une attaque biologique de grande envergure[193]. En mars 2020, le secrétaire général des Nations Unies a donné un avertissement par rapport au fait que les [traduction] « avancées scientifiques réduisent les barrières techniques qui auparavant limitaient le potentiel des armes biologiques[194]. » Cette préoccupation a été confirmée dans le Bulletin of the Atomic Scientists : [traduction] « les technologies en matière de biologie synthétique et de génie génétique sont maintenant moins coûteuses et plus faciles à obtenir, et elles se répandent rapidement[195]. » Même si ces technologies ont des utilisations légitimes, elles peuvent aussi servir à l'utilisation d'armes biologiques. La Convention sur les armes biologiques n'a aucun mécanisme de vérification officiel à sa disposition. Même si aucun pays n'affirme posséder un programme de guerre biologique, le MDN/FAC est d'avis que des pays spécifiques maintiennent de tels programmes ***[196] Le secrétaire général des Nations Unies a souligné l'importance de renforcer la capacité des états d'intervenir en cas d'attaque biologique s'il n'est pas possible de la prévenir[197]. Les défis auxquels plusieurs pays font face pour

---

[188] Elena Dinu, « Reassessing CBRN terrorism threats », *Reassessing CBRN Threats in a Changing Global Environment*, eds. Fei Su et Ian Anthony, SIPRI, juin 2019, https://www.sipri.org/sites/default/files/2019-06/1906_cbrn_threats_su_anthony_0.pdf.
[189] SCRS, *Évaluation conjointe de la menace avec le Group scientifique, technique et du renseignement (STIG) 2018, ***** 2018.
[190] Elena Dinu, « Reassessing CBRN terrorism threats », *Reassessing CBRN Threats in a Changing Global Environment*, eds. Fei Su et Ian Anthony, SIPRI, juin 2019, https://www.sipri.org/sites/default/files/2019-06/1906_cbrn_threats_su_anthony_0.pdf.
[191] SCRS, *Évaluation conjointe de la menace avec le Group scientifique, technique et du renseignement (STIG) 2018, ***** 2018.
[192] SCRS, *Évaluation conjointe de la menace avec le Group scientifique, technique et du renseignement (STIG) 2018, ***** 2018.
[193] Depuis l'entrée en vigueur de la Convention sur les armes biologiques en 1975, les seules attaques connues ayant été perpétrées à l'aide d'armes biologiques l'ont été par des acteurs non étatiques. John P. Caves, Jr. et W. Seth Carus, « The Future of Weapons of Mass Destruction: Their Nature and Role in 2030 », *National Defence University Centre for the Study of Weapons of Mass Destruction*, article occasionnel n° 10, juin 2014, https://ndupress.ndu.edu/Portals/68/Documents/occasional/cswmd/CSWMD_OccationalPaper-10.pdf.
[194] Secrétaire général des Nations Unies, *Secretary-General's message on the forty-fifth anniversary of the entry into force of the Biological Weapons Convention*, le 26 mars 2020, https://www.un.org/sg/en/content/sg/statement/2020-03-26/secretary-generals-message-the-forty-fifth-anniversary-of-the-entry-force-of-the-biological-weapons-convention.
[195] John Mecklin, « Closer than ever: it is 100 seconds to midnight », *Bulletin of the Atomic Scientists*, 23 janvier 2020, https://thebulletin.org/doomsday-clock/current-time.
[196] MDN/FAC, *** 6 juin 2013; Bureau des affaires de désarmement des Nations Unies, *Securing our Common Future: An Agenda for Disarmament*, 2018, https://www.un.org/disarmament/publications/more/securing-our-common-future/.
[197] Bureau des affaires de désarmement des Nations Unies, *Assurer notre avenir commun : un programme de désarmement*, 2018, https://front.un-arm.org/documents/SGDA_fr_web.pdf/.

prendre des mesures à l'égard de la pandémie mondiale de COVID-19 donnent à penser que leur capacité d'intervenir en cas d'attaque biologique de grande envergure est limitée.

Technologies à double usage

110. Selon le SCRS, le Canada demeure une cible pour l'approvisionnement illégal et clandestin ainsi que le transfert de technologie ***[198] [*** Le paragraphe a été revu pour supprimer de l'information préjudiciable ou privilégiée. Il décrit des évaluations du SCRS des méthodes et des objectifs d'un état ainsi que des préoccupations découlant des nouvelles technologies. ***][199] ***[200] ***[201]

Pandémie de COVID-19

111. La pandémie de COVID-19 n'a pas eu de répercussions importantes sur la menace que représentent les armes de destruction massive. Par contre, la pandémie de COVID-19 a révélé des faiblesses notables des secteurs de la santé et des systèmes d'intervention.

Principales conclusions

112. Le contexte de la sécurité entourant les armes de destruction massive n'a connu aucune amélioration depuis 2018. Le régime de contrôle des armes nucléaires a subi des revers importants au cours des deux dernières années. L'utilisation de ces armes par des acteurs étatiques ou non étatiques dans le cadre de conflits et d'assassinats ciblés a compromis les normes internationales à long terme contre l'utilisation d'armes chimiques. Les armes biologiques sont rarement utilisées, mais le régime de vérification est faible, et les défis découlant de la pandémie de COVID-19 laissent croire que la capacité des états d'intervenir est limitée. L'accessibilité au matériel chimique et biologique ainsi que la prolifération des technologies à double usage préoccupent particulièrement le Canada.

---

[198] SCRS, *Rapport annuel au ministre sur les activités opérationnelles 2018-2019*, 19 décembre 2019.
[199] SCRS, *** 2020.
[200] SCRS, *** 2019.
[201] SCRS, *** 2019.

Conclusion

113. Cette année a été difficile pour tous les Canadiens. Quant au Comité, étant donné le changement des membres à la suite des élections de 2019, il a à peine pu commencer ses travaux avant que des mesures visant à limiter la propagation de la COVID-19 ne soient prises. Ces mesures ont forcé le Comité à adapter son plan de travail et à trouver des moyens de réaliser ses activités tout en respectant les exigences en matière de santé et de sécurité. Le Comité reconnait l'aide du Service canadien du renseignement de sécurité pour lui avoir fourni un moyen sécuritaire de tenir des réunions, et ainsi de remplir son mandat. Le Comité reconnait également les efforts des organisations de la sécurité et du renseignement d'avoir fourni des documents en réponse aux demandes du Comité même si elles étaient également aux prises avec leurs propres défis liés à la pandémie.

114. Pour le Comité, ces efforts renforcent l'importance d'assurer la responsabilisation, même dans les situations les plus difficiles. Comme le démontre l'aperçu des menaces pour la sécurité nationale du Comité, les risques envers la sécurité du Canada continuent d'évoluer, même pendant une crise mondiale. Les menaces terroristes ont grandement changé; des états ont mené des attaques opportunistes en vue de compromettre nos politiques et de voler des recherches exigeantes ainsi que des données exclusives; et les groupes du crime organisé ont exploité les points faibles des lois et de l'application de la loi pour se prêter au blanchiment d'argent et au trafic de drogues de plus en plus mortelles. Les organisations canadiennes de la sécurité et du renseignement n'ont pas relâché leurs efforts et ont continué de cerner et d'atténuer les menaces, et d'adapter leurs propres activités à de nouvelles réalités.

115. Les organisations chargées d'examiner les activités et le cadre de la sécurité et du renseignement du Canada doivent faire de même. Le Comité est conscient des pressions auxquelles les organisations de la sécurité et du renseignement font face pour assumer leurs responsabilités opérationnelles. En réponse, il a adapté ses propres demandes aux ministères en prolongeant les délais et en réduisant le nombre de demandes d'exposés. Néanmoins, le Comité et son homologue, l'Office de surveillance des activités en matière de sécurité nationale et de renseignement, continuent d'assumer leurs rôles conférés par la loi. Au cours de la prochaine année, le Comité prévoit fournir deux examens au premier ministre : le cadre du gouvernement visant à protéger ses systèmes et ses réseaux contre les cyberattaques ainsi que les activités d'Affaires mondiales Canada liées à la sécurité nationale et au renseignement, qui étudieront les questions importantes de la responsabilisation, de la gouvernance et de l'efficacité. Ces examens reflètent l'idée du Comité que les activités de la sécurité et du renseignement ainsi que leur examen sont essentiels pour protéger la sécurité, les droits et les libertés des Canadiens, et que leur reprise doit avoir lieu au moyen d'une étroite coopération.

Annexe A : Aperçu et principales conclusions

Terrorisme

Aperçu

116. Dans son Rapport annuel 2018, le Comité a souligné que l'appareil de la sécurité nationale et du renseignement a défini le terrorisme comme étant la principale menace pour la sécurité nationale. Le gouvernement a également déclaré que des personnes ou des groupes inspirés par l'idéologie salafiste-jihadiste représentent la plus grande menace terroriste pour le Canada. Toutefois, plusieurs tendances et événements ont changé cette évaluation. On compte notamment la libération du territoire sous le joug de Daech en Irak et en Syrie, la détention subséquente des voyageurs extrémistes canadiens (aussi connus sous le nom de combattants étrangers) en Syrie, des attaques contre des Canadiens par des individus et des organisations extrémistes, et la montée de l'extrémisme violent à caractère idéologique.

Principales conclusions

117. Les individus ou les groupes inspirés par l'idéologie salafiste-jihadiste, comme celle de Daech et d'al-Qaïda, représentaient la menace terroriste la plus importante de 2018. Même si Daech et al-Qaïda ont été relativement affaiblis au cours des deux dernières années, ils constituent encore une menace pour le Canada et les intérêts canadiens au pays et à l'étranger. En même temps, le SCRS a découvert d'importantes activités liées à l'extrémisme violent à caractère idéologique au cours des deux dernières années (notamment les groupes d'extrême droite), comme en témoignent l'activité en ligne et les attaques. L'augmentation importante des activités extrémistes violentes à caractère idéologique en 2020 donne à penser que le contexte de la menace terroriste amorce un virage. La principale menace physique au Canada demeure les attentats peu sophistiqués contre les lieux publics non protégés. Ces tendances sont à l'image des tendances discernées chez les plus proches alliés du Canada.

Espionnage et ingérence étrangère

Aperçu

118. En 2018, le Comité a défini que l'espionnage et l'ingérence étrangère étaient des menaces grandissantes pour lesquelles il faudra probablement prendre des mesures non négligeables au cours des années à venir. L'espionnage et l'ingérence étrangère menace la souveraineté, la prospérité et les intérêts nationaux du Canada. Ces menaces visent les collectivités, les gouvernements, les entreprises, les universités et la technologie. En 2019, le Comité a examiné la réponse du gouvernement à l'ingérence étrangère et a constaté que les activités d'ingérence étrangère représentent un risque considérable pour la sécurité nationale et, principalement, parce qu'elles portent atteinte aux institutions fondamentales du Canada et fragilisent les droits et libertés des Canadiens. En 2020, le SCRS a déclaré que les acteurs des états hostiles posaient le danger le plus important pour la sécurité nationale du Canada. Des reportages dans les médias, des discours de dirigeants et des informations sur

des dossiers criminels montrent tous que la menace continue d'évoluer non seulement au Canada, mais également chez ses alliés.

Principales conclusions

119. La menace de l'espionnage et de l'ingérence étrangère est substantielle et continue de s'accroître. Plusieurs états se livrent à de telles activités au Canada, mais le renseignement indique que la Chine et la Russie sont toujours les principales coupables. Même si les effets de l'espionnage et de l'ingérence étrangère ne sont pas aussi rapidement manifestes que ceux du terrorisme, ils représentent les menaces à long terme les plus lourdes de conséquences pour la souveraineté et la prospérité du Canada. La pandémie, quant à elle, a incité de nouveau les états étrangers à se livrer à de l'espionnage contre le secteur de la santé du Canada et des organisations canadiennes qui travaillent dans le domaine de la science et de la technologie.

Cybermenaces

Aperçu

120. Dans son survol de 2018, le Comité indiquait que les cyberactivités malveillantes constituaient un risque considérable pour la sécurité nationale et il attirait précisément l'attention sur la menace que font planer la Chine et la Russie sur les réseaux gouvernementaux. Les cybermenaces se font sentir un peu partout; elles touchent les systèmes gouvernementaux, les fournisseurs d'infrastructures essentielles, le secteur privé, ainsi que les Canadiens. Les acteurs de cybermenaces varient de cybercriminels peu sophistiqués à des acteurs étatiques très capables. Leurs motivations sont aussi diversifiées, comme le vol de renseignements personnels dans un dessein de fraude ou de propriétés intellectuelles et d'informations d'entreprise confidentielles dans un but d'espionnage industriel, ou encore l'interruption de services essentiels. En 2020, les cybermenaces figurent encore parmi les préoccupations en matière de sécurité nationale du Canada, et la Russie et la Chine sont toujours les acteurs étatiques les plus perfectionnés qui prennent pour cible les systèmes du gouvernement du Canada. Au cours de la dernière année, les acteurs de cybermenaces ont également pris avantage de la crise sanitaire mondiale causée par la pandémie de COVID-19 pour faire avancer leurs objectifs. Des acteurs malveillants étatiques et non étatiques ont pris pour cible le secteur de la santé et les services gouvernementaux et ont mené des campagnes de désinformation en ligne pour manipuler l'opinion publique et saper la confiance de la population dans le fonctionnement des systèmes de santé publique clés.

Principales conclusions

121. Les cybermenaces présentent un risque grave et croissant pour la sécurité nationale du Canada. Des acteurs étatiques, surtout la Chine et la Russie, continuent de prendre pour cible les réseaux gouvernementaux, les institutions publiques et les entreprises privées aux fins de cyberespionnage. Ces acteurs continuent de renforcer leurs moyens pour cibler les infrastructures essentielles, mener des campagnes d'ingérence en ligne et surveiller les dissidents à l'étranger. La pandémie a fait

manifestement ressortir ces menaces, en particulier les menaces qui planent sur le secteur de la santé du Canada. Le Comité présentera son examen des cybermoyens de défense du gouvernement au premier ministre en 2021.

Crime organisé d'envergure

Aperçu

122. Dans son Rapport annuel 2018, le Comité a indiqué que les répercussions du crime organisé sont énormes et insidieuses. Les groupes du crime organisé mènent des activités criminelles traditionnelles, comme le trafic illégal de drogue, d'armes et de marchandises illicites; la traite de personnes; et les crimes financiers, comme la fraude, les activités de jeu illégales et la manipulation des marchés. Les activités illégales des groupes du crime organisé d'envergure continuent d'engendrer des coûts élevés pour la société et de présenter des risques importants pour le Canada. Au cours des deux dernières décennies, ces activités sont devenues de plus en plus complexes et recherchées. Toutefois, la nature de la menace n'a pas changé de façon marquée depuis 2018.

Principales conclusions

123. Le crime organisé d'envergure présente toujours une menace importante pour la sécurité nationale. On estime que les produits de la criminalité se chiffrent dans les milliards de dollars, ce qui représente une importante perte de revenus pour les gouvernements et pourrait être la source d'autres activités criminelles. Au-delà de ces coûts se trouvent les ramifications sociétales et financières du crime organisé : il sape la primauté du droit, menace la sécurité publique et mine nos institutions financières, légales, politiques et sociales.

Armes de destruction massive

Aperçu

124. Dans son Rapport annuel 2018, le Comité a indiqué que les armes de destruction massive et la prolifération de matériel et de technologies à double usage constituent une menace pour la sécurité nationale. Ces armes peuvent causer des accidents de masse aveugles ainsi que des dommages économiques et environnementaux à long terme. La menace envers le Canada que posent ces armes et leur prolifération est demeurée la même au cours des deux dernières années. Toutefois, certaines tendances, décrites plus loin, pourraient influencer cette évaluation. Voici les grandes lignes de ces tendances : le régime mondial de désarmement nucléaire s'est affaibli depuis 2018, et l'utilisation continue d'armes chimiques par des acteurs étatiques ou non étatiques a porté atteinte aux normes internationales; et les avancées technologiques ont facilité l'accès au matériel à double usage ainsi que la conception et la livraison d'armes chimiques et biologiques. De plus, le Canada demeure une cible d'approvisionnement illicite et clandestin de technologies à double usage par plusieurs acteurs étatiques. En outre, la pandémie de COVID-19 a permis de découvrir d'importantes vulnérabilités en ce qui a trait aux économies de l'état, aux secteurs de la santé et aux systèmes d'intervention.

Principales conclusions

125. Le contexte de la sécurité entourant les armes de destruction massive n'a connu aucune amélioration depuis 2018. Le régime de contrôle des armes nucléaires a subi des revers importants au cours des deux dernières années. L'utilisation de ces armes par des acteurs étatiques ou non étatiques dans le cadre de conflits et d'assassinats ciblés a compromis les normes internationales à long terme contre l'utilisation d'armes chimiques. Les armes biologiques sont rarement utilisées, mais le régime de vérification est faible, et les défis découlant de la pandémie de COVID-19 laissent croire que la capacité des états d'intervenir est limitée. L'accessibilité au matériel chimique et biologique ainsi que la prolifération des technologies à double usage préoccupent particulièrement le Canada.