Analyse des dispositions du projet de loi C-59, Loi concernant des questions de sécurité nationale, première lecture, portant sur la *Loi sur le Centre de la sécurité des télécommunications* et des dispositions connexes (18 décembre 2017)

Décembre 2017

Rapport préparé par Christopher Parsons, Lex Gill, Tamir Israel, Bill Robinson et Ronald Deibert

Cette page est laissée en blanc intentionnellement.

Le Citizen Lab et la CIPPIC sont des partenaires de recherche qui travaillent en collaboration. Ensemble, les deux groupes participent à des recherches qui portent sur les relations entre les technologies numériques, le droit et les droits de la personne.

Version du document : 1.0.

Le Citizen Lab et la Clinique d'intérêt public et de politique d'Internet du Canada Samuelson-Glushko

Le Citizen Lab est un laboratoire interdisciplinaire établi à l'École Munk des affaires internationales de l'Université de Toronto. Ses activités sont axées sur la recherche, le développement, les politiques stratégiques de haut niveau et l'engagement juridique à l'intersection des technologies de l'information et des communications, des droits de la personne et de la sécurité internationale.

Nous utilisons des méthodes de recherche « mixtes » qui regroupent des méthodes tirées de divers domaines, à savoir la science politique, le droit, la science informatique et les études territoriales. Nos recherches consistent entre autres à enquêter sur l'espionnage numérique de la société civile, à recueillir des renseignements sur le filtrage de l'Internet ainsi que d'autres technologies et pratiques ayant une incidence sur la liberté d'expression en ligne, à analyser la protection de la vie privée, la sécurité et les contrôles de l'information d'applications courantes, et à examiner les mécanismes de transparence et de responsabilité concernant la relation entre les sociétés et les organismes gouvernementaux en ce qui a trait aux données personnelles et à d'autres activités de surveillance.

La **Clinique d'intérêt public et de politique d'Internet du Canada Samuelson-Glushko (CIPPIC)** est une clinique d'aide juridique établie au Centre de recherche en droit, technologie et société de la faculté de droit de l'Université d'Ottawa. Son principal mandat consiste à veiller à ce que l'intérêt public soit pris en compte dans la prise de décisions sur des questions qui se posent à l'intersection du droit et de la technologie. Elle a également le mandat d'offrir une aide juridique aux particuliers et aux organismes sous-représentés sur des questions relatives au droit et à la technologie. Elle a aussi un mandat en matière d'enseignement, qui vise à offrir aux étudiants en droit une formation pratique dans un milieu axé sur le droit et les technologies.

Pour exercer son mandat, la CIPPIC adopte une approche multilatérale dans le cadre de laquelle elle présente des recherches et des arguments objectifs et exhaustifs à des décideurs du domaine de la politique, de la réglementation et du droit. Elle vise à adopter une approche globale pour son analyse, qui intègre les dimensions sociopolitiques, techniques et juridiques d'un problème précis se rapportant aux politiques. Dans le cadre de son mandat, elle livre régulièrement des témoignages d'experts devant des comités parlementaires, et participe à des procédures réglementaires quasi judiciaires, à des interventions stratégiques à tous les échelons du système judiciaire et à des forums nationaux et internationaux sur la gouvernance d'Internet.

Le rapport

Le présent rapport vise à fournir en temps opportun une analyse juridique, à situer le contexte politique et à présenter l'historique des dispositions du projet de loi C-59, Loi concernant des questions de sécurité nationale, première lecture, portant sur la *Loi sur le Centre de la sécurité des télécommunications* et des dispositions connexes (18 décembre 2017). Nous espérons que ce document permettra aux députés, aux journalistes, aux chercheurs, aux avocats et aux défenseurs des intérêts de la société civile à participer de façon plus efficace à l'examen des enjeux. Il s'agit d'une analyse du projet de loi au moment où commencent les débats politiques sur celui-ci au Canada, et il faut l'interpréter en tenant compte de l'évolution rapide du paysage juridique et politique.

Nous sommes reconnaissants des discussions approfondies auxquelles ont participé d'éminents experts canadiens spécialisés dans les politiques, les pratiques et la loi sur la sécurité nationale dans le cadre des ateliers d'été du Citizen Lab en 2017. Nous sommes aussi reconnaissants d'avoir eu la possibilité de participer à des discussions et de recevoir des commentaires sur des aspects de notre analyse du projet de loi dans le cadre de l'atelier sur le renseignement de sécurité et la surveillance en cette ère de mégadonnées, qui a eu lieu à Ottawa à l'automne 2017. Nous sommes également reconnaissants des efforts que déploie Sécurité publique Canada pour examiner avec nous des enjeux relatifs au projet de loi C-59. Enfin, nous sommes heureux d'avoir eu l'occasion de discuter de certains aspects du projet de loi au cours d'une séance d'information sur le projet de loi C-59 qu'ont organisée à l'automne 2017 des membres du Centre de la sécurité des télécommunications, du Service canadien du renseignement de sécurité, de Sécurité publique Canada et des parties externes à ces organismes, et de discuter avec d'autres professionnels de la sécurité nationale.

Nous aimerions également remercier chaleureusement la fondation John D. et Catherine T. MacArthur, la Fondation Ford et Frederick Ghahramani, dont l'aide financière généreuse a permis de préparer le présent rapport. Nous aimerions aussi remercier Kate Robertson pour sa recherche juridique et sa grande contribution au rapport. S'il y a des erreurs ou des omissions, les auteurs en assument l'entière responsabilité.

Si vous avez des questions ou des commentaires, veuillez les faire parvenir à : christopher@christopher-parsons.com; lex@citizenlab.ca; tisrael@cippic.ca.

Les auteurs

Christopher Parsons, Lex Gill, Tamir Israel, Bill Robinson et Ronald Deibert ont effectué la recherche sur laquelle s'appuie l'analyse et ont rédigé celle-ci.

Christopher Parsons est titulaire d'un baccalauréat et d'une maîtrise de l'Université de Guelph, et d'un doctorat de l'Université de Victoria**.** Il est actuellement associé en recherche au Citizen Lab, à l'École Munk des affaires internationales de l'Université de Toronto, et directeur général du projet de transparence des télécommunications du Citizen Lab.

Lex Gill est une chercheuse universitaire au Citizen Lab, à l'École Munk des affaires internationales. Elle est également représentante du Programme de la sécurité nationale à l'Association canadienne des libertés civiles. Lex est récipiendaire de la bourse Google Policy pour la Clinique d'intérêt public et de politique d'Internet du Canada, et a déjà été chercheuse et membre du Berkman Klein Center for Internet & Society à l'Université Harvard. Elle est titulaire d'un diplôme en droit civil et en common law (B.C.L./LL.B.) de la faculté de droit de l'Université McGill.

Tamir Israel est avocat-conseil à l'interne à la Clinique d'intérêt public et de politique d'Internet du Canada (CIPPIC), qui fait partie de la faculté de droit de l'Université d'Ottawa. Il dirige les activités de la CIPPIC portant sur la protection de la vie privée, la neutralité de l'Internet, la surveillance électronique et la réglementation des télécommunications, et mène des activités de recherche et de défense des droits portant sur une variété de sujets se rapportant aux droits numériques. Il donne également des cours magistraux sur la réglementation d'Internet à la faculté des études supérieures et postdoctorales à l'Université d'Ottawa.

Bill Robinson est un chercheur universitaire au Citizen Lab, à l'École Munk des affaires internationales. Il est l'auteur du blogue Lux Ex Umbra, qui est axé sur les activités passées et présentes liées au renseignement électromagnétique au Canada.

Ronald Deibert (membre de l'Ordre de l'Ontario et titulaire d'un doctorat de l'Université de la Colombie-Britannique) est professeur de sciences politiques et directeur du Citizen Lab, de l'École Munk des affaires internationales de l'Université de Toronto. Le Citizen Lab est un laboratoire interdisciplinaire menant des activités axées sur la recherche, le développement, les politiques stratégiques de haut niveau et l'engagement juridique à l'intersection des technologies de l'information et des communications, des droits de la personne et de la sécurité internationale. En 2013, il a été nommé membre de l'Ordre de l'Ontario et a reçu la médaille du jubilé de diamant de la Reine Elizabeth II pour avoir été « l'une des premières personnes à reconnaître les menaces grandissantes pour les droits de communication, l'ouverture et la sécurité à l'échelle mondiale, et à prendre des mesures pour les atténuer. » [TRADUCTION]

Sigles

Adresse IP	Adresse de protocole Internet
BCCLA	British Columbia Civil Liberties Association
CIPPIC	Clinique d'intérêt public et de politique d'Internet du Canada
CSARS	Comité de surveillance des activités de renseignement de sécurité
CST	Centre de la sécurité des télécommunications du Canada
GCHQ	Government Communications Headquarters (Royaume-Uni)
GRC	Gendarmerie royale du Canada
IMEI	Identité internationale d'équipement mobile
IMSI	Identité internationale d'abonnement mobile
LCST	*Loi sur le Centre de la sécurité des télécommunications*
LDN	*Loi sur la défense nationale*
LOSASNR	*Loi sur l'Office de surveillance des activités en matière de sécurité nationale et de renseignement*
LPRPDE	*Loi sur la protection des renseignements personnels et les documents électroniques*
NSA	National Security Agency (États-Unis)
OSASNR	Office de surveillance des activités en matière de sécurité nationale et de renseignement
SCRS	Service canadien du renseignement de sécurité
VPN	Réseau virtuel privé

Table des matières

Résumé des recommandations

Portée du mandat et pouvoirs

Problèmes concernant des termes définis (et non définis)

Ententes

Production de rapports et mesures favorisant la transparence

Aperçu

Le Centre de la sécurité des communications (« le CST ») est l'organisme national responsable du renseignement électromagnétique et de la cybersécurité au Canada. Le présent rapport contribue au débat sur la sécurité nationale qui se déroule actuellement au Canada, car il fournit une analyse de la *Loi sur le Centre de la sécurité des télécommunications* (la « LCST ») proposée, soit un élément important des réformes que propose le gouvernement du Canada dans le projet de loi C-59, Loi concernant des questions de sécurité nationale (le « projet de loi C-59 » ou le « projet de loi[1] »). Dans cette analyse, nous résumons le mandat, les activités, les opérations et les pouvoirs du CST, et nous nous concentrons sur leurs répercussions éventuelles sur les droits de la personne et la sécurité mondiale. Nous formulons également une série de recommandations qui, si elles sont adoptées, garantiront que le cadre du CST soit plus solide sur le plan juridique, protégeront mieux les intérêts mondiaux en matière de sécurité dans un environnement technologique connaissant une évolution rapide et tiendront compte plus efficacement des obligations nationales et internationales du Canada en matière de droits de la personne.

Dans la **section I**, nous donnons un aperçu du mandat actuel du CST et de certaines activités controversées menées dans le cadre de ce mandat. Nous donnons aussi un aperçu très général du projet de loi C-59 et de ses principales répercussions sur le CST.

Dans la **section II**, nous analysons en détail les principaux enjeux liés au CST qui découlent du projet de loi C-59 et nous nous concentrons sur les aspects ayant les répercussions les plus importantes sur les droits de la personne, la transparence politique et la sécurité mondiale. Plus précisément, voici certains enjeux du projet de loi sur lesquels nous mettons l'accent :

- les problèmes de longue date concernant les opérations du CST relatives au renseignement étranger, qui s'appuient sur des interprétations juridiques ambiguës et secrètes qui légitiment les activités de collecte massive de données et de surveillance de masse. Ces activités sont toutes deux visées par les protections prévues dans la *Charte* et doivent respecter les obligations du Canada en matière de droits de la personne;
- l'absence totale de moyens significatifs de surveillance et de contrôle des activités du CST selon les volets du mandat proposés en ce qui a trait aux cyberopérations actives et défensives;
- l'absence de restrictions ou de mesures de protection significatives en ce qui concerne les cyberopérations actives et défensives du CST, qui sont susceptibles de menacer sérieusement les outils de communication sécurisés, la sécurité publique et la sécurité mondiale;
- l'absence de restrictions ou de mesures de protection significatives en ce qui concerne les activités du CST en général. Telle qu'elle est actuellement rédigée, la LCST semble comprendre une lacune qui permet au CST de causer la mort ou des lésions corporelles, ou d'entraver le « cours de la justice ou de la démocratie » en application de ses

[1] Chambre des communes du Canada, Loi concernant des questions de sécurité nationale (projet de loi C-59), 1re session, 42e législature, première lecture, 20 juin 2017.

pouvoirs en matière de renseignement étranger ou de cybersécurité, mais qui lui interdit d'agir de la sorte en application de ses nouveaux pouvoirs relatifs aux cyberopérations;

- le risque que les opérations du CST en matière de cybersécurité et d'assurance pour le gouvernement fédéral menacent l'indépendance des tribunaux ou la séparation des pouvoirs;
- les préoccupations relatives au cadre régissant la façon dont le CST peut acquérir des logiciels malveillants, des logiciels espions et des outils de piratage informatique, ce qui peut légitimer un marché fondé non pas sur le renforcement de la sécurité de l'infrastructure mondiale de l'information, mais bien sur la diminution de cette sécurité et sur l'atteinte à celle-ci;
- les graves enjeux concernant la façon dont le CST apporte une aide technique et opérationnelle à d'autres organismes, dont les organismes canadiens responsables de l'application de la loi, qui peuvent faire en sorte que le CST offre des capacités que des partenaires nationaux ne pourraient pas, légalement ou constitutionnellement, élaborer, utiliser ou posséder, ou qui seraient en soi disproportionnées si elles étaient appliquées dans ces contextes (p. ex. dans des opérations policières);
- les enjeux éventuels concernant la capacité de l'Office de surveillance des activités en matière de sécurité nationale et de renseignement à accéder à des renseignements d'origine étrangère et le risque de détournement de la réglementation par l'entremise de ses politiques d'embauche;
- les graves lacunes, juridiques et pratiques, du rôle du commissaire au renseignement, qui ne règle pas les problèmes constitutionnels concernant le commissaire du CST actuel ou la constitutionnalité des activités du CST en général;
- l'incapacité du commissaire au renseignement à surveiller et à contrôler de façon significative et complète les activités du CST (y compris ses activités les plus problématiques) en raison d'un mandat trop peu inclusif, d'enjeux relatifs à l'indépendance et de pouvoirs insuffisants de nature quasi judiciaire;
- la faiblesse et l'imprécision des mesures de protection de la vie privée des Canadiens et des personnes se trouvant au Canada, et le mépris le plus total des droits de la protection de la vie privée en tant que norme internationale en matière de droits de la personne;
- les exceptions extraordinaires à la règle générale du CST empêchant de « donner un ordre » aux Canadiens et aux personnes se trouvant au Canada accroissent considérablement la capacité du CST à utiliser ses larges pouvoirs à l'échelle nationale;
- l'absence générale de reconnaissance de la nature fortement interreliée et interdépendante de l'infrastructure mondiale de l'information signifie que les mesures de protection ou les pouvoirs du CST, qui ne dépassent pas les frontières du pays, sont insuffisants pour protéger les intérêts du Canada en matière de sécurité;
- les tensions profondes au cœur du mandat du CST, qui exigent à celui-ci, d'une part, de protéger la sécurité et de la défendre contre les menaces, et d'autre part, d'exploiter, de maintenir et de créer simultanément de nouvelles vulnérabilités afin de poursuivre ses

objectifs relatifs au renseignement étranger. Ces tensions sont exacerbées par l'ajout de nouveaux pouvoirs offensifs et par les deux nouveaux volets de son mandat;
- le manque de clarté juridique quant à la question de savoir s'il convient d'informer les fournisseurs et le public des vulnérabilités découvertes par le CST ainsi que la façon et le moment de le faire, et la façon dont le CST tient compte parallèlement de l'intérêt public;
- le manque d'exigence en matière de reddition de comptes ou de surveillance en ce qui concerne les « ententes » avec des homologues du CST à l'étranger. Dans le cadre de ces partenariats, il existe un risque que de l'information soit obtenue par la torture ou par l'entremise d'autres activités qui seraient illégales ou inconstitutionnelles si elles étaient menées par un organisme canadien.

Dans la **section III**, nous résumons les recommandations formulées à l'issue de notre analyse à l'intention des membres de comités et d'autres députés étudiant la LCST proposée. Plus précisément, nous formulons des recommandations afin d'améliorer les systèmes d'examen, de surveillance et de contrôle du CST et de limiter la capacité du CST à participer à des activités qui sont problématiques, abusives, inconstitutionnelles ou contraires aux normes internationales en matière de droits de la personne.

Section I – Contexte

Le Centre de la sécurité des télécommunications

Le CST est l'organisme national responsable du renseignement électromagnétique et de la cybersécurité au Canada. Le CST, qui était initialement la Direction des télécommunications du Conseil national de recherches, a été créé par le décret C.P. 54/3535 du 13 avril 1946 à la suite de la fusion de deux organismes de cryptographie. Il a relevé du Conseil national de recherches jusqu'au 1er avril 1975, date à laquelle il a été intégré au ministère de la Défense nationale et renommé le Centre de la sécurité des communications.

En 2001, la partie V.1 a été ajoutée à la *Loi sur la défense nationale* (LDN), consacrant l'organisme pour la première fois dans une loi publique[2]. Cette petite partie de la LDN comprend encore les principales dispositions législatives régissant les activités du CST, et bien que celui-ci ne fasse plus partie du ministère de la Défense nationale (il est devenu un organisme indépendant en 2011), il demeure sous la responsabilité du ministre de la Défense nationale.

La LDN énonce le mandat du CST, qui comporte trois volets, généralement appelés les mandats A, B et C (LDN (1985), par. 273.64(1)).

- **Mandat A :** « [A]cquérir et utiliser l'information provenant de l'infrastructure mondiale d'information dans le but de fournir des renseignements étrangers [...] »

[2] *Loi sur la défense nationale,* L.R.C. 1985, ch. N-5.

- **Mandat B : «** [F]ournir des avis, des conseils et des services pour aider à protéger les renseignements électroniques et les infrastructures d'information importantes pour le gouvernement du Canada. »
- **Mandat C :** « [F]ournir une assistance technique et opérationnelle aux organismes fédéraux chargés de l'application de la loi et de la sécurité, dans l'exercice des fonctions que la loi leur confère. »

Les activités dans les volets du mandat concernant le renseignement étranger (volet A) et la cybersécurité (volet B) ne peuvent viser des Canadiens ou des personnes se trouvant au Canada. Autrement dit, le CST est un organisme se préoccupant principalement d'acteurs étrangers et de menaces étrangères (LDN, 1985, al. 273.64(2)a)).

Le CST mène des activités dans ce qu'on appelle l'« infrastructure mondiale d'information », qui, selon la définition donnée dans la loi actuellement en vigueur, s'entend notamment « des émissions électromagnétiques, des systèmes de communication, des systèmes et réseaux des techniques de l'information ainsi que des données et des renseignements techniques qu'ils transportent, qui s'y trouvent ou qui les concernent » (LDN, art. 273.61). La définition proposée dans la nouvelle LCST ajoute également à la définition de l'infrastructure mondiale de l'information « tout équipement produisant de telles émissions [électromagnétiques], les systèmes de communication [...] ainsi que les données et les renseignements techniques qu'ils transportent, qui s'y trouvent ou qui les concernent » (LCST, art. 2). Concrètement, cela signifie que le champ d'activité du CST comprend absolument tout, de l'Internet aux communications mobiles en passant par la radio, les satellites, tous les types de systèmes informatiques imaginables, les micro-ondes, les signaux thermiques, etc.

Le CST mène généralement ses activités dans le secret presque complet; presque tous les éléments de ses programmes, de ses opérations et de ses activités ne peuvent pas faire l'objet d'un débat ou d'un examen public significatif. Par conséquent, la population a commencé à prendre conscience de l'organisme de façon généralisée à la fin de 2013, des suites des révélations d'Edward Snowden. Bien qu'en 2017 seulement 3 % des répondants au sondage aient été en mesure de dire que le CST était l'organisme canadien responsable du renseignement électromagnétique étranger et de la cybersécurité[3], de nombreux Canadiens connaissent sans doute les controverses que ces documents ont soulevées en ce qui concerne les droits juridiques et les droits de la personne.

Avant d'expliquer en détail comment la LCST proposée (et le projet de loi C-59 en général) peut finir par modifier, limiter ou élargir le cadre juridique régissant le fonctionnement du CST, il est utile de donner quelques exemples des connaissances actuelles sur les activités de celui-ci. Nous donnons ci-dessous cinq exemples d'activités autorisées dans le cadre du mandat actuel du CST à trois volets, comme l'ont révélé les documents originaux publiés par Edward Snowden. Ensemble, ces exemples illustrent la portée actuelle des activités de collecte de données du CST à l'échelle nationale qui sont connues, la mesure dans laquelle les opérations de surveillance du CST dépendent de la contribution de ses partenaires étrangers, la mesure dans laquelle le Canada échange ses données de surveillance

[3] La Presse canadienne, « Just 3% Of Canadians Can Name The Communications Security Establishment: Survey », *Huffpost*, 2017, http://www.huffingtonpost.ca/2017/11/08/just-3-of-canadians-can-name-the-communications-security-establishment-survey_a_23270492/.

de masse avec ses meilleurs alliés dans le secteur du renseignement, la façon dont le CST cible les appareils de personnes innocentes et les façons dont les programmes du CST peuvent tirer profit de divers volets du mandat simultanément.

- **Collecte et utilisation de métadonnées nationales :** Un document original a révélé que le CST utilisait les métadonnées des communications canadiennes – comme des adresses de protocole Internet (IP), des témoins, des adresses de courriel ou des données de routage semblables – pour effectuer des expériences visant à concevoir des techniques permettant de suivre des personnes ciblées localisées à des adresses IP non identifiées. À partir d'identificateurs numériques détectés dans un grand aéroport canadien, le CST a utilisé d'autres données liées à l'aéroport ainsi que des données liées à des universités canadiennes, à des cafés, à des bibliothèques et à des entreprises, pour suivre les appareils mobiles de personnes pendant que celles-ci se déplaçaient dans le pays. Ces documents ont révélé la mesure dans laquelle le CST a régulièrement accès aux données canadiennes nationales ainsi qu'une des façons dont ses analystes utilisent ces données. Malgré le fait que ces activités comportaient des renseignements très révélateurs sur la vie privée et l'emplacement de personnes, ni le CST ni son organisme de surveillance ne considéraient que l'utilisation ou la collecte de ces métadonnées constituaient une violation des attentes raisonnables des Canadiens en matière de protection de la vie privée ou une violation de la disposition selon laquelle le CST ne peut « viser » des Canadiens[4].

- **Collecte de données par des partenaires étrangers :** Bien que le CST ne puisse soi-disant cibler délibérément des Canadiens ou des personnes se trouvant au Canada, des rapports ont révélé comment ses partenaires étrangers (comme la National Security Agency (NSA)) ont délibérément ciblé des parties de l'infrastructure mondiale de l'information se trouvant au Canada. Lorsque la NSA a cherché à établir une représentation graphique des réseaux virtuels privés (VPN) d'entreprises partout dans le monde, y compris les banques canadiennes, les recherches et les documents ont été transmis au CST. Même lorsque le CST n'a pas l'autorisation de recueillir de renseignements sur des organisations canadiennes, des Canadiens ou des personnes se trouvant au Canada, ses organismes partenaires peuvent recueillir ces renseignements, puis les lui transmettre afin qu'il les utilise, les analyse ou les transmette à son tour[5].

- **Échange de données avec des entités étrangères :** Des documents originaux ont montré à quel point les opérations de renseignement canadiennes dépendaient de données recueillies, et peut-être fournies, par des alliés afin d'effectuer une opération de surveillance de masse. Après avoir travaillé avec une « source spéciale » [TRADUCTION]

[4] Voir Centre de la sécurité des télécommunications, *IP Profiling Analytics & Mission Impacts*, gouvernement du Canada, 2012, https://christopher-parsons.com/writings/cse-summaries/#ip-profiling.

[5] Voir Colin Freeze et Christine Dobby, « NSA trying to map Rogers, RBC communications traffic, leak shows », *Globe and Mail*, 2015, https://www.theglobeandmail.com/news/national/nsa-trying-to-map-rogers-rbc-communications-traffic-leak-shows/article23491118/.

pour surveiller de façon exhaustive le téléchargement et le téléversement de documents dans des sites Web permettant de téléverser des fichiers gratuitement, le CST a conçu des analyses complètes du mode de vie des personnes utilisant ce genre de services. Ces analyses comportaient l'établissement de liens entre les identificateurs numériques se rapportant à l'activité du fichier et d'autres comportements de ces personnes en ligne, comme la navigation sur le Web ou la consultation de Facebook. Individuellement, le CST n'aurait pas pu effectuer ce type d'opération de surveillance ou d'analyse du mode de vie. Pour y parvenir, il devait absolument consulter des bases de données étrangères comprenant des données de surveillance de masse recueillies par les meilleurs alliés du Canada en ce qui a trait au renseignement étranger, y compris la NSA et le Government Communications Headquarters (GCHQ)[6].

- **Exploitation des appareils de personnes non ciblées :** Le CST utilise un système automatisé pour trouver des appareils pouvant être exploités par la suite. Ces appareils ne sont pas nécessairement utilisés par des personnes représentant une menace pour le Canada. Il utilise plutôt ces appareils afin de simplement dissimuler ses opérations, ce qui l'aide à faire en sorte qu'il soit impossible d'établir un lien entre ses activités et les systèmes qu'il héberge (les activités semblent plutôt être effectuées à partir d'appareils indépendants désignés et exploités par le CST). Ce subterfuge fait en sorte que les propriétaires non concernés d'appareils exploités « participent » à leur insu et involontairement aux activités du CST. Ce type d'activité peut avoir des répercussions négatives sur les droits et les intérêts de personnes sans méfiance si les adversaires du CST tentent de compromettre ou de gêner autrement les personnes qui possèdent ou contrôlent les appareils exploités – que ce soit en les traitant comme des dommages collatéraux ou en les tenant responsables d'une quelconque manière des activités du CST[7].

- **L'exploitation de divers mandats pour les opérations :** Les opérations de renseignement étranger et de cyberdéfense comportent le déploiement d'au moins 200 capteurs partout dans le monde. Ces capteurs, qui fonctionnent exclusivement dans les réseaux du gouvernement du Canada, sont autorisés selon le volet du mandat axé sur la cybersécurité (B). Cependant, nombre de ces systèmes sont également autorisés selon les volets du mandat concernant le renseignement étranger (A) ou l'assistance (C). Ce cadre signifie que le réseau peut activement empêcher ou modifier le trafic de données, ou en effectuer la surveillance et le suivi de façon exhaustive. Le fait qu'aucun mandat ne dresse les limites de cette opération révèle que les mandats et les interventions connexes du CST ne devraient pas nécessairement être interprétés

[6] Voir Centre de la sécurité des télécommunications, *LEVITATION and the FFU Hypothesis*, gouvernement du Canada, après 2012, https://christopher-parsons.com/writings/cse-summaries/#levitation-and.
[7] Voir Centre de la sécurité des télécommunications, *LANDMARK*, gouvernement du Canada, s.d., https://christopher-parsons.com/writings/cse-summaries/#landmark-associated.

isolément. Il serait plutôt plus exact de considérer que ces efforts sont interreliés et complémentaires[8].

Les renseignements sur le CST qui ont été révélés dans les documents publiés par Edward Snowden ont surpris tant le public que les experts, qui n'avaient pas réalisé à quel point le cadre juridique actuel du CST permettait un comportement si intrusif. Toutefois, il est essentiel de comprendre que les activités décrites précédemment, et les activités menées par le CST en général, ne sont pas toutes nécessairement légales ou constitutionnelles. En particulier, la British Columbia Civil Liberties Association (BCCLA) mène actuellement une contestation constitutionnelle de taille en ce qui concerne les activités de surveillance de masse du CST. Elle fait valoir que la prétendue capacité de l'organisme à intercepter sans mandat les communications privées des Canadiens et à recueillir massivement des métadonnées canadiennes viole le droit à la protection contre les fouilles, les perquisitions ou les saisies abusives garanti par l'article 8 de la *Charte canadienne des droits et libertés*[9].

En outre, le public a un aperçu relativement limité des activités du CST à la différence de certains des plus proches alliés du Canada. Cela signifie qu'il est impossible pour le public de bien comprendre comment la LCST proposée modifierait ou limiterait les activités que mène actuellement le CST ou en élargirait la portée. Il est également impossible de comprendre la mesure dans laquelle la LCST proposée pourrait servir à intégrer dans le droit public des aspects des activités actuelles du CST qui sont problématiques sur le plan constitutionnel. En l'absence de renseignements bien détaillés sur la portée et la nature des activités actuelles du CST, il est extrêmement difficile d'évaluer leur légalité actuelle ou future, leurs répercussions sur les droits garantis par la *Charte* et les droits internationaux de la personne, ainsi que leur lien par rapport aux intérêts nationaux du Canada.

Cependant, en l'absence d'une plus grande transparence de la part du CST – et compte tenu de certaines différences relatives au mandat, au contexte juridique et à l'ampleur des activités –, il est raisonnable pour les observateurs de déduire que le CST mène des activités semblables à celles de ses meilleurs alliés dans le secteur du renseignement, y compris la NSA et le GCHQ. Dans bien des cas, les activités de ces autres organismes sont considérées comme extrêmement controversées et pourraient être inconstitutionnelles si elles étaient menées par le gouvernement du Canada. Les parlementaires doivent mieux comprendre les types d'activités que mène actuellement le CST et les projets d'avenir de celui-ci afin de comprendre entièrement les répercussions de la loi proposée actuellement : malgré la possibilité que le ministre ne soit pas disposé à répondre avec précision aux questions concernant les activités du CST, il est néanmoins impératif que le public et les parlementaires comprennent mieux les types d'activités qui sont actuellement autorisées et qui pourraient être autorisées ou le seraient en application de la LCST proposée.

---

[8] Voir Centre de la sécurité des télécommunications, *IP Profiling Analytics & Mission Impacts*, gouvernement du Canada, 2012, https://christopher-parsons.com/writings/cse-summaries/#ip-profiling; Centre de la sécurité des télécommunications, *CSEC Cyber Threat Capabilities: SIGINT and ITS: an end-to-end approach*, gouvernement du Canada, 2009 ou 2010, https://christopher-parsons.com/writings/cse-summaries/#cse-cyber-threat-capabilities.

[9] *British Columbia Civil Liberties Association c. Canada (procureur général)*, Déclaration T-2210- 14, Cour fédérale, par. 32, https://bccla.org/wp-content/uploads/2014/12/20141027-CSEC-Statement-of-Claim.pdf.

Précisions sur le projet de loi C-59, Loi concernant des questions de sécurité nationale

Le gouvernement fédéral a proposé le projet de loi C-59 en juin 2017 et a ainsi articulé les réformes comme une réaction à la *Loi antiterroriste (2015)* du gouvernement précédent qui a suscité la controverse (auparavant le projet de loi C-51). Le projet de loi C-59 offre des solutions partielles à certains problèmes constitutionnels du projet de loi C-51 et répond à certaines préoccupations que le public a soulevées dans le cadre de la consultation sur la sécurité nationale menée à la fin de 2016[10]. Le projet de loi C-59 porte sur un vaste éventail de questions dans le domaine du droit de la sécurité nationale, de la communication d'information à la liste d'interdiction de vol en passant par le terrorisme en droit pénal. Certaines de ces réformes étaient facilement prévisibles des suites de la consultation de 2016, d'autres offrent une réponse partielle aux enquêtes et aux commissions gouvernementales sur la sécurité nationale[11] et d'autres cherchent à légitimer le comportement du gouvernement en fonction de jugements que la Cour fédérale a rendus récemment[12].

Pourtant, de nombreuses modifications proposées dans le projet de loi C-59, y compris des réformes radicales visant les cadres régissant le mandat et les autorisations du CST, n'ont pas fait l'objet de consultations publiques ni de débats considérables. Bien des dispositions du projet de loi C-59 étaient prévisibles – que ce soit à partir de décisions des tribunaux, de lois antérieures, de commissions d'enquête ou de consultations publiques –, mais les réformes des dispositions législatives régissant le CST étaient en grande partie inattendues. À l'exception de deux recommandations que le Comité permanent de la sécurité publique et nationale a formulées dans la feuille de route pour la sécurité nationale du Canada en mai 2017, peu d'indices laissaient penser que le CST ferait l'objet d'une réforme importante.

> Recommandation 40
> Que le Centre de la sécurité des télécommunications, lorsqu'il répond aux demandes d'un autre organisme de sécurité nationale concernant l'interception des communications privées ainsi que la collecte et la conservation des métadonnées, limite ses activités au mandat de l'organisme à l'origine de la demande.
>
> Recommandation 41
> Que les stratégies de cybersécurité reposent sur une approche pangouvernementale, telle que celle adoptée au Royaume-Uni par le Government Communications Headquarters (GCHQ).
>
> Feuille de route du Comité permanent de la sécurité publique et nationale, p. 46[13]

[10] Sécurité publique Canada, *Consultation sur la sécurité nationale*, gouvernement du Canada, 2016, https://www.canada.ca/fr/services/defense/securitenationale/consultation-securite-nationale.html.

[11] Voir l'honorable Dennis R. O'Connor, *Commission d'enquête sur les actions des responsables canadiens relativement à Maher Arar*, 2006, http://epe.lac-bac.gc.ca/100/206/301/pco-bcp/commissions/maher_arar/07-09-13/www.ararcommission.ca/fr/index.htm; l'honorable Frank Iacobucci, c.r., *Enquête interne sur les actions des responsables canadiens relativement à Abdullah Almalki, Ahmad Abou-Elmaati et Muayyed Nureddin*, 2008, http://epe.lac-bac.gc.ca/100/206/301/pco-bcp/commissions/internal_inquiry/2010-03-09/www.iacobucciinquiry.ca/pdfs/documents/final-report-copy-fr.pdf; l'honorable John C. Major, *Vol 182 d'Air India : Une tragédie canadienne*, 2010, http://epe.lac-bac.gc.ca/100/206/301/pco-bcp/commissions/air_india/2010-07-23/www.majorcomm.ca/fr/reports/finalreport/index.asp.

[12] Voir X (Re), 2013 FC 1275, X (Re), [2017] 2 RCF 396, 2016 CF 1105.

[13] Comité permanent de la sécurité publique et nationale, *Protéger les Canadiens et leurs droits : une nouvelle feuille de route pour la sécurité nationale au Canada*, 2017, 1re session, 42e législature,

La partie 3 édicte la *Loi sur le Centre de la sécurité des télécommunications* (LCST), modifie la *Loi sur la défense nationale* (la loi habilitante actuelle du CST) et apporte des modifications corrélatives à d'autres lois. Notamment, la LCST :

- apporterait des modifications importantes au mandat du CST et pourrait élargir considérablement les pouvoirs de celui-ci;
- dresserait une liste d'exceptions plus longue et explicitement plus permissive à la règle générale interdisant au CST de mener des activités « visant » des Canadiens, des personnes se trouvant au Canada et, dans certains cas, l'infrastructure au Canada, dans l'exercice de certains mandats;
- créerait un nouveau cadre régissant l'autorisation des activités du CST sous l'autorité du ministre désigné et du commissaire au renseignement nouvellement créé;
- créerait un cadre permettant au CST de communiquer de l'information à des catégories de personnes et à des personnes désignées;
- prévoirait que le CST a le pouvoir de conclure des « ententes » avec des entités étrangères et internationales aux fins de communication de l'information à ces entités ou de coopération avec elles.

En outre, le projet de loi C-59 édicte et modifie d'autres lois ayant des répercussions sur le CST, dont la *Loi sur l'Office de surveillance des activités en matière de sécurité nationale et de renseignement* (LOSASNR) et la *Loi sur le commissaire au renseignement*.

L'Office de surveillance des activités en matière de sécurité nationale et de renseignement (OSASNR) proposé aurait pour mandat d'examiner les activités exercées par le CST et le Service canadien du renseignement de sécurité (SCRS), les activités d'autres ministères liées à la sécurité nationale ou au renseignement, ainsi que d'autres questions dont il est saisi par un ministre. Il aurait également le pouvoir de faire enquête sur les plaintes et de formuler des conclusions et des recommandations (*Loi sur l'Office de surveillance des activités en matière de sécurité nationale et de renseignement*, art. 8).

La *Loi sur le commissaire au renseignement* abolirait le poste de commissaire du Centre de la sécurité des télécommunications et créerait le bureau du commissaire au renseignement. Le commissaire au renseignement proposé aurait un rôle indépendant et quasi judiciaire de surveillance du CST et du SCRS, et aurait le pouvoir d'approuver certaines de ces autorisations, modifications aux autorisations et déterminations demandées au titre des lois respectives de ces organismes.

Section II – Analyse de la LCST

i. Mandat

La LCST proposée élargirait le mandat actuel du CST, qui passerait de trois à cinq volets (LCST, par. 16(1)). Cette modification ajouterait deux « nouveaux » volets au mandat du CST, outre le renseignement étranger, la cybersécurité et l'assistance :

---

https://www.noscommunes.ca/Content/Committee/421/SECU/Reports/RP8874869/securp09/securp09-f.pdf, p. 46.

- les cyberopérations défensives (LCST, art. 19);
- les cyberopérations actives (LCST, art. 20).

Cependant, la LCST modifie la structure et la portée de tous les volets du mandat du CST, sans se limiter à ces deux « nouveaux » volets. De même, au lieu de concevoir que le volet du mandat relatif aux « cyberopérations défensives » (art. 18) est tout à fait nouveau, il serait plus juste de considérer qu'il s'agit à la fois de l'élargissement du mandat B (cybersécurité) actuellement prévu dans la LDN et de la division de celui-ci en deux catégories distinctes dans la LCST, à savoir la cybersécurité et l'assurance de l'information (art. 18), et les cyberopérations défensives (art. 19), respectivement.

En général, et en ce qui concerne le mandat relatif aux « cyberopérations actives », il demeure difficile de savoir dans quelle mesure le mandat à cinq volets de la LCST faciliterait la réalisation d'activités d'une nature et d'un type que n'exerce pas déjà le CST. Compte tenu du caractère secret des activités du CST, il est difficile d'établir si par ces changements, le législateur a l'intention soit d'accorder de nouveaux pouvoirs au CST, soit d'apporter une clarté juridique et de prévoir un cadre d'autorisation explicite en droit public régissant les activités que le CST mène déjà ou a menées par le passé.

Le tableau 1 illustre comment le projet de loi C-59 modifierait le mandat actuel du CST et constitue une référence permettant de comprendre les cinq volets du mandat proposé dans la LCST.

Loi sur la défense nationale	***LCST***
Mandat A (al. 273.64 (1)a)) Le mandat du Centre de la sécurité des télécommunications est le suivant : a) acquérir et utiliser l'information provenant de l'infrastructure mondiale d'information dans le but de fournir des renseignements étrangers, en conformité avec les priorités du gouvernement du Canada en matière de renseignement;	**Renseignement étranger (art. 17)** En ce qui a trait au volet de son mandat touchant le renseignement étranger, le Centre acquiert, secrètement ou d'une autre manière, de l'information à partir de l'infrastructure mondiale de l'information ou par son entremise, notamment en engageant des entités étrangères situées à l'extérieur du Canada ou en interagissant avec celles-ci ou en utilisant tout autre moyen d'acquérir de l'information, et utilise, analyse et diffuse l'information dans le but de fournir des renseignements étrangers, en conformité avec les priorités du gouvernement fédéral en matière de renseignement.

Mandat B (al. 273.64 (1)b)) Le mandat du Centre de la sécurité des télécommunications est le suivant : **…** b) fournir des avis, des conseils et des services pour aider à protéger les renseignements électroniques et les infrastructures d'information importantes pour le gouvernement du Canada;	**Cybersécurité et assurance de l'information (art. 18)** En ce qui a trait au volet de son mandat touchant la cybersécurité et l'assurance de l'information, le Centre : a) fournit des avis, des conseils et des services afin d'aider à protéger : (i) l'information électronique et les infrastructures de l'information des institutions fédérales, (ii) l'information électronique et les infrastructures de l'information d'importance pour le gouvernement fédéral désignées comme telles en vertu du paragraphe 22(1); b) acquiert, utilise et analyse de l'information provenant de l'infrastructure mondiale de l'information ou d'autres sources afin de fournir de tels avis, conseils et services.
	Cyberopérations défensives (art. 19) En ce qui a trait au volet de son mandat touchant les cyberopérations défensives, le Centre mène des activités dans l'infrastructure mondiale de l'information ou par l'entremise de celle-ci afin d'aider à protéger : a) l'information électronique et les infrastructures de l'information des institutions fédérales; b) l'information électronique et les infrastructures de l'information d'importance pour le gouvernement fédéral désignées comme telles en vertu du paragraphe 22(1).
S.O.	**Cyberopérations actives (art. 20)** En ce qui a trait au volet de son mandat touchant les cyberopérations actives, le Centre mène des activités dans l'infrastructure mondiale de l'information ou par l'entremise de celle-ci afin de réduire, d'interrompre, d'influencer ou de contrecarrer, selon le cas, les capacités, les intentions ou les activités de tout étranger ou État, organisme ou groupe terroriste étrangers, dans la mesure où ces capacités, ces intentions ou ces activités se rapportent aux affaires internationales, à la défense ou à la sécurité, ou afin d'intervenir dans le déroulement de telles intentions ou activités.

Mandat C (al. 273.64 (1)c))	**Assistance technique et opérationnelle (art. 21)**
Le mandat du Centre de la sécurité des télécommunications est le suivant : … c) fournir une assistance technique et opérationnelle aux organismes fédéraux chargés de l'application de la loi et de la sécurité, dans l'exercice des fonctions que la loi leur confère.	En ce qui a trait au volet de son mandat touchant l'assistance technique et opérationnelle, le Centre fournit une assistance technique et opérationnelle aux organismes fédéraux chargés de l'application de la loi et de la sécurité, aux Forces canadiennes et au ministère de la Défense nationale.

Dans le reste de la présente section, nous décrivons les types d'activités se rapportant à chaque volet du mandat, la façon dont ces activités seraient autorisées aux termes de la LCST proposée, le risque de violation des droits garantis par la *Charte* et des droits de la personne en général, et les répercussions sur la sécurité mondiale.

Renseignement étranger

Loi sur la défense nationale	***LCST***
Mandat A (al. 273.64 (1)a)) Le mandat du Centre de la sécurité des télécommunications est le suivant : a) acquérir et utiliser l'information provenant de l'infrastructure mondiale d'information dans le but de fournir des renseignements étrangers, en conformité avec les priorités du gouvernement du Canada en matière de renseignement;	**Renseignement étranger (art. 17)** En ce qui a trait au volet de son mandat touchant le renseignement étranger, le Centre acquiert, secrètement ou d'une autre manière, de l'information à partir de l'infrastructure mondiale de l'information ou par son entremise, notamment en engageant des entités étrangères situées à l'extérieur du Canada ou en interagissant avec celles-ci ou en utilisant tout autre moyen d'acquérir de l'information, et utilise, analyse et diffuse l'information dans le but de fournir des renseignements étrangers, en conformité avec les priorités du gouvernement fédéral en matière de renseignement.

Le CST a le mandat d'acquérir et d'utiliser l'information provenant de l'infrastructure mondiale de l'information dans le but de fournir des renseignements étrangers (LDN, al. 273.64 (1)a), LCST, art. 17). Dans le cadre de ce mandat, il mène des activités de surveillance ciblée et de surveillance de masse dans l'objectif d'obtenir des renseignements sur des étrangers, des États étrangers, des organisations étrangères ou des groupes terroristes étrangers et qui portent sur les affaires internationales, la défense ou la sécurité (LDN, art. 273.61, LCST, art. 2). Les modifications que la LCST propose d'apporter

au volet du mandat touchant le renseignement étranger sont plus explicites que les dispositions de la LDN. Elles prévoient que le CST peut acquérir l'information secrètement et avec l'aide d'entités étrangères, et qu'il est possible non seulement d'acquérir de l'information et de l'utiliser, mais aussi de l'analyser et de la diffuser (LCST, art. 17).

Cette nouvelle version proposée du mandat du CST touchant le renseignement étranger a une portée qui permettrait au CST d'avoir recours à des agents humains pour installer des dispositifs d'écoute électronique ou exercer d'autres activités à l'appui des opérations de renseignement électromagnétique à l'étranger[14]. Le SCRS peut effectuer de telles activités pour le CST au Canada, mais la portée du mandat du SCRS en matière de renseignement étranger est vague, et on a laissé entendre qu'une aide étrangère concernant le renseignement humain pourrait être bénéfique pour le CST[15]. Dans certains cas, cela pourrait permettre au CST de mener des opérations plus ciblées et proportionnées (p. ex. en créant des moyens d'accéder à un ordinateur en particulier et non à un réseau en entier), mais cela pourrait aussi créer une variété de nouveaux moyens d'adopter des comportements disproportionnés et problématiques (p. ex. en ciblant un nœud autrement inaccessible dans l'infrastructure mondiale de l'information afin de créer un accès généralisé). Le gouvernement devrait énoncer clairement ses intentions à cet égard : s'il envisage la possibilité d'ajouter un volet de renseignement humain aux opérations du CST, il devrait informer le Parlement et les Canadiens de cette modification importante à la nature du CST, et dans le cas contraire, il devrait le déclarer de façon explicite.

La LDN actuellement en vigueur permet au CST d'intercepter incidemment des communications privées lorsqu'il exerce des activités conformément à une autorisation ministérielle de renseignement étranger, ce qui lui permet de contrevenir à la partie VI du *Code criminel* (LDN, art. 273.65 et 273.61; une communication privée est définie à l'article 183 du *Code criminel*). En revanche, aux termes de la LCST proposée, le CST peut demander une autorisation relative au renseignement étranger pour les activités connexes qui contreviendraient à toute loi canadienne, y compris à la *Charte* (LCST, par. 23(1)). Sous le régime de cette loi, le ministre peut autoriser le CST à mener beaucoup plus d'activités qui seraient autrement illégales que ne le permet actuellement la LDN. Parallèlement, le CST n'est pas tenu d'obtenir une autorisation ministérielle (et les protections qu'elle comprend) s'il estime que ses activités ne contreviennent à aucune loi canadienne.

Aux termes de la LCST, le ministre peut délivrer des autorisations de renseignement étranger si le chef du CST lui en fait la demande par écrit et expose dans cette demande les faits qui permettent au ministre de conclure qu'il y a des motifs raisonnables de croire que l'autorisation est nécessaire et que

---

[14] Bill Robinson, « CSE and Bill C-59 overview », *Lux Ex Umbra*, 2017, https://luxexumbra.blogspot.ca/2017/08/cse-and-bill-c-59-overview.html.

[15] En 2007, Bob Brûlé, ancien chef adjoint du CST, opérations SIGINT, s'est exprimé en ces termes devant le Comité sénatorial permanent de la Sécurité nationale et de la défense : « [L]es organismes comme le CST ont désespérément besoin d'un service de renseignement étranger pour connaître du succès à l'avenir. D'un point de vue purement égoïste, je dirai que ce que le gouvernement peut décider pour faire progresser le dossier sera utile à un organisme dont le travail est technique comme le CST. » Voir Comité sénatorial permanent de la sécurité nationale et de la défense, *Délibérations du Comité sénatorial permanent de la sécurité nationale et de la défense*, Sénat du Canada, fascicule 17, 11 juin 2007, https://sencanada.ca/fr/Content/Sen/committee/391/defe/17eva-f.

les conditions énoncées au paragraphe 35(2) de la LCST sont remplies (art. 34). Plus précisément, le ministre peut délivrer une autorisation uniquement s'il a des motifs raisonnables de croire :

- que l'activité en cause est « raisonnable et proportionnelle » dans les circonstances (LCST, par. 35(1));
- que l'information à acquérir au titre de l'autorisation ne peut raisonnablement être acquise d'une autre manière (al. 35(2)a)) et que dans le cas où l'autorisation vise l'acquisition d'informations non sélectionnées, celles-ci ne peuvent raisonnablement être acquises d'une autre manière (al. 35(2)b));
- que l'information à acquérir au titre de l'autorisation ne sera pas conservée plus longtemps que ce qui est raisonnablement nécessaire (al. 35(2)a));
- que les mesures visées à l'article 25 permettront d'assurer que l'information acquise au titre de l'autorisation qui est identifiée comme se rapportant à un Canadien ou à une personne se trouvant au Canada sera utilisée, analysée ou conservée uniquement si elle est essentielle aux affaires internationales, à la défense ou à la sécurité (al. 35(2)c)).

En outre, la LCST permet également au CST de communiquer de l'information qui pourrait être utilisée pour identifier un Canadien à des personnes désignées comme des destinataires appropriés si l'information est jugée essentielle aux affaires internationales, à la défense, à la sécurité ou à la cybersécurité (art. 44 et 46). Seule l'information qui a été « utilisée, analysée ou conservée » au titre d'une autorisation de renseignement étranger peut être communiquée en application de cet article, ce qui offre une certaine mesure de protection contre le glissement de données d'un mandat à un autre. Cependant, l'article 44 est problématique dans la mesure où il élargit les objectifs déjà vastes et imprécis du « renseignement étranger » afin d'y inclure la « cybersécurité », soit un terme qui n'est pas défini dans la LCST en général et précisément en ce qui a trait au mandat du CST touchant le renseignement étranger. Il est difficile de savoir pourquoi il est nécessaire d'ajouter ce terme ambigu dans cet article. Dans la mesure où le CST peut effectuer des activités relatives à la cybersécurité conformément à son mandat touchant le renseignement étranger, ces préoccupations s'appliqueront déjà aux objectifs du renseignement étranger se rapportant « aux affaires internationales, à la défense ou à la sécurité ».

Recommandation 41.

Modifier l'article 44 afin d'éliminer le terme « cybersécurité », qui n'est pas défini dans la LCST et qui n'est pas mentionné autrement en ce qui a trait aux activités du CST touchant le renseignement étranger.

L'article 44 constitue une exception aux limites imposées par l'article 23 (qui interdit au CST de mener des activités touchant le renseignement étranger qui visent des Canadiens) et à l'article 25 (qui exige que des mesures soient en place pour protéger la vie privée des Canadiens dans les communications faites par le CST aux termes de son mandat touchant le renseignement étranger). En pratique, il semble que le CST pourra incidemment communiquer des données canadiennes anonymisées de masse sous réserve de restrictions minimes conformément à son mandat touchant le renseignement étranger, mais il pourra seulement lier ces données anonymisées à des Canadiens sous le régime de

l'article 44. Cela est particulièrement préoccupant compte tenu de la grande variété d'entités que le ministre peut désigner comme des destinataires légitimes de communications aux termes de l'article 44 (LCST, art. 47). En fait, l'article 47 ne semble imposer aucune restriction quant aux personnes ou aux catégories de personnes pouvant être désignées comme des destinataires de communications aux termes de l'article 44, y compris des entités étrangères et des organismes du secteur privé. Bien que l'article 55 de la LCST prévoie un cadre supplémentaire régissant l'échange d'information avec des entités étrangères (sous réserve de l'approbation du ministre des Affaires étrangères), l'article 55 est facultatif, c'est-à-dire qu'il n'est pas nécessaire de le respecter pour échanger de l'information avec des entités étrangères désignées aux termes de l'article 44.

La LCST prévoit également un cadre explicite en ce qui a trait à l'acquisition d'information « non sélectionnée », qui est définie dans la loi proposée comme « l'information acquise, pour des raisons techniques ou opérationnelles, sans avoir recours à des termes ou des critères pour identifier l'information ayant un intérêt en matière de renseignement étranger » (LCST, art. 2). Autrement dit, l'information « non sélectionnée » est obtenue grâce à des activités qui sont explicitement des formes de surveillance de masse non ciblée, qui constituent selon de nombreuses personnes une violation des obligations internationales en matière de droits de la personne et une violation des droits relatifs à la vie privée des Canadiens touchés accessoirement aux termes de la *Charte*[16].

Une autorisation relative au renseignement étranger permet au CST de mener une activité qui serait autrement illégale « malgré toute autre loi fédérale ou loi d'un État étranger » dans la réalisation de son mandat, sous réserve des conditions de délivrance d'une autorisation prévues au paragraphe 35(2) de la LCST et des modalités de l'autorisation. La grande variété d'activités pouvant être autorisées dans le cadre de ce volet du nouveau mandat est décrite à l'article 27 de la LCST proposée. L'alinéa 27(2)e) crée également une catégorie résiduelle, qui permet au CST de « mener toute autre activité qui est raisonnable dans les circonstances et est raisonnablement nécessaire pour faciliter l'exécution des activités ou catégories d'activités visées par l'autorisation ».

Les autorisations de renseignement étranger sont valides uniquement si le commissaire au renseignement les a approuvées par écrit (LCST, art. 29). Les autorisations demeurent valides pour une période maximale d'un an après l'obtention de l'approbation du commissaire et le ministre peut les prolonger d'au plus un an. Bien que la décision de prolonger la période de validité d'une autorisation ne soit pas assujettie à l'examen du commissaire au renseignement, une nouvelle autorisation doit être délivrée par la suite (LCST, art. 37). Il s'agit d'une amélioration par rapport au système actuellement prévu dans la LDN, qui permet au chef du CST de demander au ministre de renouveler les autorisations chaque année indéfiniment, tant que la durée de chaque période de renouvellement ne dépasse pas un an (LDN, par. 273.68(1)). La LCST ajoute également une mesure de protection, qui exige au chef du CST d'aviser le ministre si des faits exposés dans la demande d'autorisation initiale changent considérablement, et qui exige au ministre d'aviser le commissaire à l'information et l'OSASNR de ces

[16] Rapport du Haut-Commissariat des Nations Unies aux droits de l'homme, *Le droit à la vie privée à l'ère du numérique*, 30 juin 2014, A/HRC/27/37, http://undocs.org/fr/A/HRC/27/37; Tamir Israel, « Foreign Intelligence in an Inter-Networked World: Time for a Re-Evaluation », 2015, dans Michael Geist, dir., *Law, Privacy and Surveillance in Canada in the Post-Snowden Era*, Ottawa, Presses de l'Université d'Ottawa, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2960283.

changements (LCST, art. 38). Le commissaire au renseignement peut alors examiner de nouveau l'autorisation et il peut l'abroger ou exiger qu'elle fasse l'objet de modifications. Il s'agit d'ajouts importants, car les paramètres factuels, techniques et opérationnels régissant le fonctionnement du CST évoluent rapidement, tout comme les capacités techniques du CST.

Interprétations juridiques ambiguës et seuils bas

En grande partie, les activités du CST touchant le renseignement étranger ont un fondement juridique très ambigu et il est extrêmement rare que des tribunaux interprètent ce fondement compte tenu du secret entourant de façon inhérente les opérations du CST. Les protections garanties par la *Charte* dans ce contexte sont tout aussi ambiguës, ne serait-ce que parce qu'elles n'ont jamais fait l'objet d'un examen rigoureux devant un tribunal. Par exemple, l'obtention de l'accès à une partie de l'infrastructure mondiale de l'information déclenche-t-elle l'application du droit canadien même si cet accès est obtenu à partir d'un point d'entrée situé à l'étranger? Les activités sous-jacentes peuvent être intrusives, mais la façon dont le droit canadien s'applique demeure ambiguë. De même, l'article 342.1 et le paragraphe 430(1.1) du *Code criminel* énoncent les principales interdictions limitant l'intrusion dans les réseaux ou les appareils informatiques.

Cependant, aucune de ces interdictions ne s'applique si les activités en question sont menées avec « apparence de droit[17] ». L'« apparence de droit » est un concept juridique désignant les situations où une personne agit en croyant honnêtement qu'elle a légalement le droit de le faire[18]. Le CST peut honnêtement croire que son mandat, dans le cadre duquel il « acquiert, secrètement ou d'une autre manière, de l'information à partir de l'infrastructure mondiale de l'information ou par son entremise [...] dans le but de fournir des renseignements étrangers », permet de mener des activités avec « apparence de droit » qu'il est autrement interdit de mener aux termes des articles 342.1 et 430 du *Code criminel*. La Cour fédérale a récemment tiré une conclusion semblable en ce qui concerne le SCRS. Elle a conclu que l'article 12 de la *Loi sur le Service canadien du renseignement de sécurité* permet au SCRS d'agir avec « apparence de droit » pour brouiller des transmissions de téléphones cellulaires de façon qui seraient autrement interdites par l'article 430 du *Code criminel*, même en l'absence de toute autre autorisation judiciaire, comme un mandat[19]. Le CST peut également faire valoir que son mandat lui donne une « apparence de droit » suffisante pour mener de telles activités même en l'absence d'autorisation. Par conséquent, il est difficile de savoir dans quelles circonstances le CST doit obtenir une autorisation pour effectuer des activités comportant l'intrusion dans un réseau. En bref, le fait qu'il

---

[17] Voir le par. 429(2), « Nul ne peut être déclaré coupable d'une infraction visée aux articles 430 à 446 s'il prouve qu'il a agi avec une justification ou une excuse légale et avec apparence de droit », et le par. 342.1(1), « Est coupable d'un acte criminel [...] quiconque, frauduleusement et sans apparence de droit [...] ».

[18] *R c. Bahr*, 2006 ABPC 360, par. 24-26.

[19] *X (Re)*, 2017 CF 1047, par. 101-106, plus particulièrement les par. 103, 105 et 106 (« J'ajoute simplement au passage que, dans leurs observations orales, les amici ont reconnu que, si je statue que l'article 12 suffit à autoriser la collecte de l'IMSI et de l'IMEI au moyen de la technologie relative aux ESB, cette activité pourrait être visée par une défense fondée sur l'article 429 du *Code criminel*. ») L'article 12 de la *Loi sur le Service canadien du renseignement de sécurité*, L.R.C. 1985, ch. C-23, définit les fonctions du SCRS : « Le Service recueille, au moyen d'enquêtes ou autrement, dans la mesure strictement nécessaire, et analyse et conserve les informations et renseignements sur les activités dont il existe des motifs raisonnables de soupçonner qu'elles constituent des menaces envers la sécurité du Canada; il en fait rapport au gouvernement du Canada et le conseille à cet égard. »

est nécessaire qu'une loi canadienne soit violée pour exiger l'obtention d'une autorisation ministérielle signifie que certaines activités problématiques du CST pourraient contourner entièrement le processus d'autorisation ainsi que les obligations connexes relatives à la proportionnalité et à la nécessité.

Recommandation 16.

Modifier les paragraphes 23(3) et 23(4) pour veiller à ce que les activités menées dans la réalisation des volets du mandat du CST concernant le renseignement étranger et la cybersécurité ainsi que l'assurance de l'information puissent toucher incidemment un Canadien ou une personne se trouvant au Canada ou s'y rapporter uniquement si elles sont menées conformément à une autorisation prévue aux paragraphes 27(1), 28(1), 28(2) et 41(1).

Recommandation 17.

Modifier le seuil obligeant le CST à obtenir une autorisation (« les activités menées par le Centre […] ne doivent pas contrevenir aux autres lois fédérales, à moins d'être menées au titre d'une autorisation ») (LCST, par. 23(3) et 23(4)) afin d'ajouter que le CST ne doit pas contrevenir aux lois provinciales et à la common law.

Les interprétations juridiques ambiguës peuvent aussi avoir une incidence sur les évaluations de la proportionnalité qui sont prévues dans le processus d'autorisation aux termes du projet de loi C-59. En particulier, des termes juridiques, comme « interception », « acquisition » et « collecte », qui ont une importance fondamentale dans les activités de surveillance de l'infrastructure mondiale de l'information menées par le CST, font depuis longtemps l'objet d'un désaccord entre le CST et de nombreux commissaires du CST[20]. Plus précisément, de nombreux organismes étrangers du renseignement font valoir que le renseignement est « acquis », « intercepté » ou « analysé » uniquement lorsque l'organisme en question le recueille en permanence. Cela permet à ces organismes de ne pas tenir compte des répercussions des données relatives au trafic sur le réseau et d'autres données sur la vie privée lorsque ces données font l'objet d'analyses et de recherches à distance[21]. Par exemple, le commissaire du CST, qui doit évaluer les activités du CST en fonction des interprétations juridiques de celui-ci, évalue la portée des activités d'interception du CST en ce qui a trait aux communications privées « interceptées et conservées » sans tenir compte de toutes les communications privées qui ont fait l'objet d'une recherche en temps réel afin d'obtenir les communications « conservées[22] ». D'importants volumes de trafic ayant fait l'objet d'une recherche

[20] Commissaire du Centre de la sécurité des télécommunications, Rapport annuel 2007-2008, mai 2008, https://www.ocsec-bccst.gc.ca/a85/ann-rpt-2007-2008_f.pdf, p. 4, « Ma seconde recommandation principale est de définir les termes *intercepter* et *interception*, ou d'établir un renvoi à la définition du terme *intercepter* qui se trouve dans le *Code criminel*. À l'heure actuelle, ces termes ne sont pas définis dans la *Loi sur la défense nationale*. Or, ils ont tous les deux une signification juridique et opérationnelle pour le CSTC. En l'absence de définitions qui soient comprises et appliquées uniformément, il m'est difficile d'interpréter les pouvoirs conférés au CSTC et d'examiner la façon dont ils ont été appliqués. »

[21] Privacy and Civil Liberties Oversight Board, *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act*, 2 juillet 2014, p. 7; Open Rights Group, « GCHQ and Mass Surveillance », *OpenRightsGroup.org*, 11 mars 2015, p. 6-8, https://www.openrightsgroup.org/ourwork/reports/gchq-andmass-surveillance.

[22] Tamir Israel, « Foreign Intelligence in an Inter-Networked World: Time for a Re-Evaluation », 2015, dans Michael Geist,

peuvent ainsi être mis de côté, même lorsque ces recherches peuvent avoir d'importants effets paralysants[23]. Cela se traduit finalement par une analyse de la proportionnalité très biaisée qui amoindrit les véritables répercussions des activités de filtrage de réseau menées par le CST.

Recommandation 37.

Modifier la LCST afin de préciser que les termes « intercepter », « analyse », « interception » et « acquisition » ont le même sens que dans la partie VI du *Code criminel*.

Recommandation 38.

Définir les termes « acquérir », « utiliser », « analyser » et « recueillir » dans la LCST afin, d'une part, d'énoncer explicitement en quoi consiste une « acquisition » et une « collecte », et d'autre part, d'établir clairement la distinction entre l'analyse et l'utilisation d'information déjà recueillie et l'analyse et l'utilisation d'information que le CST n'a pas encore recueillie.

Collecte massive de données et surveillance de masse

Le CST effectue actuellement ce qu'on appelle souvent la « collecte massive » de données (ou la surveillance de masse) au moyen de différentes techniques. Certains types de surveillance de masse comportent l'utilisation de mots clés, de termes ou d'autres types de « sélecteurs » qui servent à filtrer un trafic intense sur un réseau et à intercepter les flux de trafic qui comportent une occurrence d'un sélecteur donné. Les sélecteurs peuvent être des adresses de courriel ou des adresses IP, des mots

---

dir., *Law, Privacy and Surveillance in Canada in the Post-Snowden Era*, Ottawa, Presses de l'Université d'Ottawa, p. 79, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2960283.

[23] *R. c. Taylor*, [1990] 3 RCS 892, par. 76-77, « [...] le par. 13(1) a pour conséquence d'interdire des communications privées, ce qui est une intrusion grave et profonde dans la vie privée des personnes. [...] Je conviens qu'ordinairement les conversations téléphoniques sont censées être privées; il est certainement raisonnable d'espérer que des tiers n'intercepteront pas ces communications.[...] On ne devrait pas écarter inconsidérément le lien entre l'al. 2b) et le droit à la vie privée et je conviens que les justifications d'une restriction de la liberté d'expression sont moins faciles à établir quand l'activité d'expression n'est pas destinée au public, essentiellement parce que le mal qui peut découler de la dissémination d'un message est limité quand la communication est privée, mais aussi peut-être parce que les libertés de conscience, de pensée et de croyance sont mises en cause de façon particulière dans un cadre privé. »; *Bennett c. Lenovo,* 2017 ONSC 1082, par. 27 (« Le risque d'accès non autorisé à de l'information privée est en soi préoccupant, même si cette information n'est pas extraite ou volée. Par exemple, si un propriétaire perce un trou lui permettant de voir dans la salle de bains d'une locataire, celle-ci estimera sans doute qu'il y a eu atteinte à sa vie privée, même si le trou n'était pas utilisé à un moment donné. » [TRADUCTION]; Assemblée générale des Nations Unies, *Rapport du Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression*, A/HRC/29/32, 22 mai 2015 (« Les systèmes de surveillance [...] peuvent compromettre le droit de se faire une opinion puisque, selon toute probabilité, la crainte de voir ses activités en ligne, comme les recherches effectuées et les pages Web consultées, divulguées contre son gré dissuade d'accéder aux informations. »; Jon Penney, « Chilling Effects: Online Surveillance and Wikipedia Use », *Berkeley Technology Law Journal*, vol. 31, n° 1, 2016, p. 117; Human Rights Watch & American Civil Liberties Union, *With Liberty to Monitor All: How Large-Scale US Surveillance is Harming Journalism, Law & American Democracy*, juillet 2014, Human Rights Watch; Cindy Cohn, « Protecting the Fourth Amendment in the Information Age: A Response to Robert Litt », *Yale Law Journal*, vol. 126, 2016, p. 107; Elizabeth Stoycheff, « Under Surveillance: Examining Facebook's Spiral of Silence Effects in the Wake of NSA Internet Monitoring », *Journalism & Mass Communication Quarterly*, vol. 93, n° 2, 2016, p. 296; PEN America, « Global Chilling: The Impact of Mass Surveillance on International Writers », *Pen.org*, 5 janvier 2015.

clés, comme « bombe », ou des critères plus recherchés, comme « message en provenance du Brésil écrit en caractères chinois simplifiés ». La forme de surveillance de masse la plus envahissante est peut-être le mécanisme par lequel les organismes, comme le CST, recueillent toutes les données du trafic sur un réseau sans utiliser de sélecteur ou de critère de ciblage. Bien que le CST ait toujours été en mesure de mener de telles activités, la LCST proposée – contrairement à la LDN – prévoit explicitement que le CST peut mener de telles activités et précise qu'il est possible de délivrer une autorisation pour la collecte d'information non sélectionnée dans la réalisation du volet du mandat du CST touchant le renseignement étranger (al. 27(2)b)).

La LCST exige au CST de prouver de façon indépendante qu'il est nécessaire d'obtenir une autorisation ministérielle pour acquérir de l'information non sélectionnée dans les circonstances — c'est-à-dire qu'il doit démontrer pourquoi les méthodes de collecte habituelles sont insuffisantes — avant d'utiliser de telles méthodes pour acquérir de l'information (al. 35(2)b)). Cependant, le fait que le CST serait encore en mesure d'acquérir de l'information « non sélectionnée » aux termes de la LCST proposée soulève d'importantes questions quant au cadre d'autorisation dans son ensemble, et jette un doute sérieux sur la question de savoir si le libellé, qui semble pouvoir limiter les activités de renseignement étranger du CST (voir les art. 27 et 35), aura un effet significatif. En effet, la LCST prévoit qu'une activité « raisonnable et proportionnelle » comprend non seulement la collecte massive de données fondée sur un « sélecteur », mais aussi les formes de surveillance de masse non sélectionnée les plus extrêmes et complètes. En revanche, nombreux sont ceux qui ont fait valoir que la surveillance de masse est par nature disproportionnée compte tenu de l'importance des intérêts relatifs à la vie privée en jeu[24]. Dans la LCST proposée, la prétendue « proportionnalité » des activités de surveillance de masse de l'information non sélectionnée menées par le CST a été établie dans la loi dès le début. Si de telles activités sont énumérées expressément dans la LCST, le commissaire au renseignement et les tribunaux doivent avoir la latitude nécessaire pour établir légalement qu'elles sont par nature disproportionnées.

Recommandation 5.

Modifier la *Loi sur le commissaire au renseignement* et la LCST pour veiller à ce que le commissaire au renseignement ait la capacité de soumettre les autorisations approuvées à des conditions; ait l'obligation de statuer sur la légalité, la constitutionnalité, la nécessité raisonnable et la proportionnalité de toute activité menée par le CST; et ait le pouvoir de prendre des décrets pour empêcher le CST de mener toute activité qui est illégale, inconstitutionnelle ou disproportionnée ou qui n'est pas raisonnablement nécessaire.

[24] Rapport du Haut-Commissariat des Nations Unies aux droits de l'homme, *Le droit à la vie privée à l'ère du numérique*, 30 juin 2014, A/HRC/27/37, http://undocs.org/fr/A/HRC/27/37; Article 19 et Electronic Frontiers Foundation, *Necessary & Proportionate: International Principles on the Application of Human Rights to Communications Surveillance: Background and Supporting International Legal Analysis*, mai 2014, https://cippic.ca/uploads/IPAHRCS-legal_analysis.pdf.

Contestation constitutionnelle en cours

La British Columbia Civil Liberties Association (BCCLA) mène actuellement une contestation constitutionnelle en ce qui concerne les activités de surveillance du CST. Cette contestation remet en question le cadre d'autorisation ministérielle actuel (LDN (1985), art. 273.65 et 273.68), qui permet au CST d'intercepter et de recueillir des communications privées et des métadonnées sans avoir obtenu une autorisation judiciaire au préalable, sans respecter la norme des « motifs raisonnables et probables » (ou toute norme reconnue) ou sans appliquer d'autres mesures de protection de base, qui peuvent limiter la conservation d'information ou interdire de la communiquer à des entités étrangères. Dans sa contestation, la BCCLA fait aussi valoir que ces activités portent atteinte au droit à la liberté de pensée, de croyance, d'opinion et d'expression garanti par l'alinéa 2b) de la *Charte*[25]. La disposition du projet de loi C-59 proposant d'ajouter un commissaire au renseignement chargé d'approuver et d'examiner les autorisations ministérielles – bien qu'il s'agisse d'une amélioration marginale – ne fournira sans doute pas le contrôle indépendant exigé par l'article 8 de la *Charte* et ne répond pas à toutes les préoccupations constitutionnelles soulevées par la BCCLA.

Inclusion d'activités problématiques relatives au renseignement étranger

Comme il a été mentionné précédemment, le paragraphe 27(2) de la LCST proposée prévoit une variété d'activités que le CST peut mener pour réaliser son mandat touchant le renseignement étranger. Bien qu'aucune de ces activités ne constitue un ajout aux outils à la disposition du CST, leur codification explicite entraîne au moins deux conséquences. Premièrement, elle accroît la transparence, car elle énonce une liste indicative précise des activités que le CST peut mener pour réaliser son mandat touchant le renseignement étranger. Deuxièmement, le fait de codifier certaines activités au paragraphe 27(2) réduit la portée des restrictions normatives essentielles que la LCST impose au CST, comme la nécessité que le ministre autorise uniquement les activités « raisonnable[s] et proportionnelle[s] » et les activités « raisonnablement nécessaire[s] ». Cependant, ces dispositions sont en quelque sorte annulées par l'alinéa 27(2)e) proposé, soit une disposition fourre-tout qui permet au CST de mener « toute autre activité qui est raisonnable dans les circonstances ».

Voici des activités pouvant s'avérer problématiques qui peuvent facilement être considérées comme « proportionnelles » en raison de l'inclusion d'une liste d'activités au paragraphe 27(2) :

- l'utilisation de logiciels malveillants pour cibler des routeurs précis sur Internet ou les appareils électroniques de personnes en particulier afin d'avoir accès à une partie de l'infrastructure mondiale de l'information;
- la collecte non sélective et non ciblée d'énormes volumes de données canadiennes et non canadiennes à partir d'appareils numériques et de réseaux;
- la diminution de l'efficacité ou le fait de coopter l'utilité d'un logiciel antivirus afin de préserver le caractère secret d'une activité du CST;

[25] *British Columbia Civil Liberties Association c. Canada (procureur général)*, Déclaration T-2210- 14, Cour fédérale, par. 32, https://bccla.org/wp-content/uploads/2014/12/20141027-CSEC-Statement-of-Claim.pdf.

- le fait de compromettre des serveurs de mise à niveau des systèmes offrant des correctifs de sécurité afin soit d'installer un maliciel dans des systèmes ciblés, soit d'empêcher à des systèmes de corriger des vulnérabilités qu'exploite le CST;
- l'affaiblissement des protocoles de chiffrement approuvés à l'échelle mondiale pour qu'il soit possible d'avoir accès à de l'information censée être protégée par ces protocoles[26].

Portée excessive du « renseignement étranger »

Dans la LDN et dans la LCST proposée, le « renseignement étranger » est défini comme des « renseignements sur les moyens, les intentions ou les activités d'un étranger, d'un État étranger, d'une organisation étrangère ou d'un groupe terroriste étranger et qui portent sur les affaires internationales, la défense ou la sécurité ». D'entrée de jeu, la portée de cette définition est excessive, particulièrement parce qu'elle englobe les intentions de tout étranger se rapportant aux affaires internationales. Par le passé, les organismes du renseignement étranger étaient investis de vastes pouvoirs, mais ceux-ci étaient axés sur les États étrangers et leurs agents. À la fin des années 1990 et au début des années 2000, la NSA et ses partenaires en matière de renseignement ont revu l'orientation de leurs programmes de surveillance afin d'englober les intentions de tout étranger sans se limiter simplement à ceux ayant un lien avec les agents de l'État[27]. La mondialisation et la montée d'Internet ont internationalisé de nombreuses questions politiques au sujet desquelles les décisions étaient surtout prises à l'échelle nationale[28]. Les débats politiques se déroulent de plus en plus souvent sur la scène internationale; les politiques nationales sont négociées dans des accords commerciaux et les politiques nationales se rapportant à Internet sont élaborées au cours d'événements de gouvernance internationaux[29]. Le fait de permettre au CST d'utiliser ses redoutables pouvoirs sur la base des intentions de personnes (et non d'États, d'agents d'État ou de groupes terroristes) se rapportant aux affaires internationales favorise la surveillance des personnes en fonction de leurs opinions politiques légitimes, ce qui entraîne un effet paralysant sur l'expression des opinions divergentes partout dans le monde[30]. Une telle portée peut également menacer le caractère adéquat

---

[26] Voir par exemple James Ball, Julian Borger et Glenn Greenwald, « Revealed: how US and UK spy agencies defeat internet privacy and security »,*The Guardian*, 2013, https://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security; Jeff Larson, « Revealed: The NSA's Secret Campaign to Crack, Undermine Internet Security », *ProPublica*, 2013, https://www.propublica.org/article/the-nsas-secret-campaign-to-crack-undermine-internet-encryption.

[27] Tamir Israel, « Foreign Intelligence in an Inter-Networked World: Time for a Re-Evaluation », 2015, dans Michael Geist, dir., *Law, Privacy and Surveillance in Canada in the Post-Snowden Era*, Ottawa, Presses de l'Université d'Ottawa, p. 81-83, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2960283.

[28] Tamir Israel, « Foreign Intelligence in an Inter-Networked World: Time for a Re-Evaluation », 2015, dans Michael Geist, dir., *Law, Privacy and Surveillance in Canada in the Post-Snowden Era*, Ottawa, Presses de l'Université d'Ottawa, p. 81-83, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2960283.

[29] Tamir Israel, « Foreign Intelligence in an Inter-Networked World: Time for a Re-Evaluation », 2015, dans Michael Geist, dir., *Law, Privacy and Surveillance in Canada in the Post-Snowden Era*, Ottawa, Presses de l'Université d'Ottawa, p. 81-83, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2960283.

[30] Jonathan W. Penney, « Internet Surveillance, Regulation, and Chilling Effects Online: A Comparative Case Study », *Internet Policy Review*, vol. 6, n° 2, 2017; Jonathan W. Penney, « Chilling Effects: Online Surveillance and Wikipedia Use », *Berkeley Technology Law Journal*, vol. 31, n° 1, 2016, p. 117; Elizabeth Stoycheff, « Under Surveillance: Examining Facebook's Spiral of Silence Effects in the Wake of NSA Internet Monitoring », *Journalism & Mass Communication Quarterly*, vol. 93, n° 2, 2016; Christopher Parsons, « Transparency in Surveillance: Role of various intermediaries in facilitating state surveillance

de la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE), soit la loi fédérale canadienne régissant la protection des données commerciales. Sous le régime du cadre de protection des données de l'Union européenne, il est établi si diverses lois étrangères en matière de protection de la vie privée sont adéquates, auquel cas les entreprises régies par ces lois peuvent recevoir des renseignements personnels en provenance de résidents de l'Union européenne. Le caractère illimité du mandat du CST touchant le renseignement étranger, qui permet de cibler des personnes en fonction de leurs motivations politiques, peut pousser les tribunaux européens à établir que la LPRPDE n'est plus adéquate[31].

Recommandation 15.

Redéfinir le « renseignement étranger » afin qu'il englobe l'information et le renseignement sur les moyens, les intentions ou les activités de groupes terroristes étrangers, d'États étrangers et de leurs agents se rapportant aux affaires internationales, à la défense ou à la sécurité, mais limite l'inclusion d'information ou de renseignement sur les moyens, les intentions ou les activités d'étrangers aux situations présentant une menace pour la sécurité du Canada, selon la définition donnée dans la *Loi sur le Service canadien du renseignement de sécurité*.

Cybersécurité et assurance de l'information

Loi sur la défense nationale	***LCST***
Mandat (al. 273.64 (1)b)) Le mandat du Centre de la sécurité des télécommunications est le suivant : [...] b) fournir des avis, des conseils et des services pour aider à protéger les renseignements électroniques et les	**Cybersécurité et assurance de l'information (art. 18)** En ce qui a trait au volet de son mandat touchant la cybersécurité et l'assurance de l'information, le Centre : a) fournit des avis, des conseils et des services afin d'aider à protéger : (i) l'information électronique et les infrastructures de l'information des institutions fédérales,

transparency », *Centre for Law and Democracy*, http://responsible-tech.org/wp-content/uploads/2016/06/Parsons.pdf; Suné von Solms et Renier van Heerden, « The Consequences of Edward Snowden NSA Related Information Disclosures », *ICCWS 2015 - The Proceedings of the 10th International Conference on Cyber Warfare and Security*, Skukuza, Afrique du Sud, 2015; Bruce Schneier, *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World*, New York, W.W. Norton & Company, 2015; Christopher Parsons, « The Governance of Telecommunications Surveillance: How Opaque and Unaccountable Practices and Policies Threaten Canadians », *Citizen Lab*, *2015,* http://www.telecomtransparency.org/wp-content/uploads/2015/05/Governance-of-Telecommunications-Surveillance-Final.pdf.

[31] *Schrems c. Data Protection Commissioner*, affaire C-362/14, 6 octobre 2015, CJUE, grande chambre; Parlement européen, Commission des libertés civiles, de la justice et des affaires intérieures, *Rapport sur le programme de surveillance de la NSA*, 21 février 2014, 2013/2188(INI), http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+REPORT+A7-2014-0139+0+DOC+PDF+V0//FR, en général et en particulier les paragraphes AQ et QR; Ryan Chiavetta, « Could Canada lose its adequacy standing? », *IAPP*, 2017, https://iapp.org/news/a/could-canada-lose-its-adequacy-standing/.

infrastructures d'information importantes pour le gouvernement du Canada;	(ii) l'information électronique et les infrastructures de l'information d'importance pour le gouvernement fédéral désignées comme telles en vertu du paragraphe 22(1); b) acquiert, utilise et analyse de l'information provenant de l'infrastructure mondiale de l'information ou d'autres sources afin de fournir de tels avis, conseils et services.

Le deuxième volet du mandat du CST consiste à mener des activités relatives à la cybersécurité et à l'assurance de l'information. Aux termes de l'article 18 de la LCST, le CST fournit des avis, des conseils et des services afin d'aider à protéger l'information électronique et les infrastructures de l'information du gouvernement du Canada ainsi que l'information électronique et les infrastructures de l'information d'importance pour le gouvernement du Canada explicitement désignées comme telles (al. 18a)). Les activités menées dans la réalisation de ce volet du mandat comportent aussi l'acquisition, l'utilisation et l'analyse de l'information provenant de l'infrastructure mondiale de l'information ou d'autres sources afin de fournir les avis, conseils et services susmentionnés (al. 18b)).

Bien que l'alinéa 18a) de la LCST proposée reprenne en grande partie le mandat actuel du CST touchant la cybersécurité en ce qui concerne l'information contrôlée, les systèmes informatiques et les réseaux internes du gouvernement du Canada, l'alinéa 18b) proposé créera un cadre qui permettra au ministre de désigner de l'information électronique et des infrastructures de l'information privées comme étant « importantes » pour le gouvernement du Canada aux termes du paragraphe 22(1). Notamment, le paragraphe 22(1) est ouvert et accorde ainsi au ministre le pouvoir discrétionnaire en apparence illimité de désigner toute information électronique, infrastructure de l'information ou catégorie d'information électronique ou d'infrastructure de l'information comme « importante » et de faire en sorte qu'elle entre dans la portée du mandat du CST touchant la cybersécurité et l'assurance de l'information (nous désignerons l'information ou l'infrastructure désignée comme « importante » aux termes du paragraphe 22(1) de la façon suivante, selon le cas : « information ou infrastructure non gouvernementale essentielle »).

Comme c'est le cas pour le volet du mandat du CST touchant le renseignement étranger, la LCST oblige le CST à obtenir une autorisation ministérielle lorsqu'il mène des activités entrant dans le volet de son mandat touchant la cybersécurité et l'assurance de l'information uniquement si ces activités contreviennent autrement à une loi canadienne (LCST, par. 23(4)). Aux termes de la LDN actuellement en vigueur, le ministre peut seulement autoriser le CST à contrevenir à une loi canadienne (l'interception de communications privées sur un réseau de télécommunications). Cependant, la LCST élargira la portée des autorisations ministérielles, qui permettront d'accéder à une infrastructure et d'acquérir « de l'information qui provient ou passe par cette infrastructure, qui y est destinée ou y est stockée » (LCST, par. 28(1) et 28(2)). Bien que cette disposition élargisse la portée des activités que le CST peut être autorisé à mener en contravention à une loi canadienne (y compris la *Charte*), elle n'exige pas au CST d'obtenir une autorisation ministérielle (et de respecter les mesures de protection connexes) sauf si celui-ci estime qu'il est possible que ses activités contreviennent à une loi

canadienne. Par conséquent, cette situation soulève des préoccupations semblables à celles soulevées par le mécanisme de la LCST applicable au volet de son mandat touchant le renseignement étranger[32].

Recommandation 16.

Modifier les paragraphes 23(3) et 23(4) pour veiller à ce que les activités menées dans la réalisation des volets du mandat du CST concernant le renseignement étranger et la cybersécurité ainsi que l'assurance de l'information puissent toucher incidemment un Canadien ou une personne se trouvant au Canada ou s'y rapporter uniquement si elles sont menées conformément à une autorisation prévue aux paragraphes 27(1), 28(1), 28(2) et 41(1).

Recommandation 17.

Modifier le seuil obligeant le CST à obtenir une autorisation (« les activités menées par le Centre […] ne doivent pas contrevenir aux autres lois fédérales, à moins d'être menées au titre d'une autorisation ») (LCST, par. 23(3) et 23(4)) afin d'ajouter que le CST ne doit pas contrevenir aux lois provinciales et à la common law.

Les autorisations ministérielles délivrées dans le cadre du volet du mandat touchant la cybersécurité habilitent le CST, malgré toute autre loi fédérale, à :

> « [...] accéder à une infrastructure de l'information d'une institution fédérale ou à acquérir de l'information qui provient ou passe par cette infrastructure, qui y est destinée ou y est stockée afin d'aider à protéger, dans les cas visés à l'alinéa 184(2)e) du *Code criminel*, cette infrastructure contre tout méfait, toute utilisation non autorisée ou toute perturbation de leur fonctionnement » (LCST, par. 28(1)).

Autrement dit, le CST pourrait intercepter des communications privées selon les conditions énoncées à l'alinéa du *Code criminel* cité dans la LCST. Notamment, il pourrait intercepter des communications privées si leur interception était raisonnablement nécessaire pour la gestion de la qualité du service de l'ordinateur ou pour la protection de l'ordinateur contre un acte qui constituerait une infraction aux paragraphes 342.1(1) (utilisation non autorisée d'un ordinateur) ou 430(1.1) (méfait à l'égard de données informatiques) du *Code criminel*. Le CST aurait aussi le droit d'intercepter uniquement les communications passant par le système informatique en particulier (le gouvernement si l'activité est menée aux termes du paragraphe 28(1) ou le secteur privé si l'activité est menée aux termes du paragraphe 28(2)) visé par l'interruption, conformément à l'alinéa 184(2)e), qui exempte une telle activité de l'interdiction générale d'intercepter des communications privées qui est prévue dans le *Code criminel*.

Par exemple, si une banque canadienne désignée faisait l'objet d'une attaque quelconque, le CST pourrait intercepter les données privées sur les réseaux internes de la banque afin de les analyser et d'établir la nature de la menace après avoir reçu une demande d'assistance écrite de la part de la banque. Cependant, le CST ne pourrait pas utiliser ses ressources en matière de renseignement étranger ou d'autres ressources pour intercepter des communications privées d'une autre provenance sur Internet dans l'objectif d'analyser ou d'atténuer l'attaque en question dans la réalisation de ce

[32] Pour avoir un aperçu de ces préoccupations, voir l'analyse fournie sous le sous-titre « Renseignement étranger ».

volet de son mandat[33]. Cela semble corriger un problème concernant le régime de cybersécurité actuel du CST, qui permet seulement au CST d'intercepter des communications privées dans les circonstances prévues à l'alinéa 184(2)c) du *Code criminel*, c.-à-d. sur un réseau d'un fournisseur de services de télécommunications (LDN, par. 273.65(3)). Comme l'a souligné le commissaire du CST, il est rare que le CST intercepte des communications privées dans la réalisation du volet de son mandat touchant la cybersécurité dans de telles conditions, ce qui suppose qu'à l'heure actuelle, ses activités à cet égard sont principalement menées en violation de la partie VI du *Code criminel*[34]. Si le motif non précisé sur lequel s'appuie la conclusion du commissaire du CST se présente parce que le CST intercepte à l'heure actuelle principalement des communications privées sur les réseaux du gouvernement du Canada, la modification proposée dans la LCST répondra à la préoccupation du commissaire du CST.

Comme il est mentionné ci-dessus, le paragraphe 22(1) de la LCST accorde au ministre le vaste pouvoir discrétionnaire de désigner de l'information électronique ou des infrastructures de l'information non gouvernementales comme essentielles, de façon à les inclure dans la portée du volet du CST touchant la cybersécurité. Il s'agit d'un écart exceptionnel par rapport au cadre juridique actuel du CST, car cela permet explicitement au CST de mener des activités sur de l'infrastructure et des systèmes canadiens privés, ce qui est susceptible de toucher de nombreux acteurs du secteur privé. Bien qu'il soit difficile d'avancer des hypothèses sur toute la gamme d'informations et d'infrastructures qui finiront par être désignées comme essentielles, cette désignation est au moins susceptible de s'appliquer aux entités de divers secteurs, comme le secteur bancaire, la défense, l'énergie, les télécommunications et le transport. En application d'une autorisation ministérielle de cybersécurité, le CST peut accéder à une infrastructure non gouvernementale essentielle – y compris à toute information qui provient ou passe par cette infrastructure – et interagir avec celle-ci de la même manière que s'il s'agissait d'information et d'une infrastructure du gouvernement fédéral (LCST, par. 28(2)). Cependant, le ministre doit avoir reçu une demande écrite de la part du propriétaire ou de l'opérateur de l'infrastructure de l'information avant de délivrer au CST une autorisation de cybersécurité se rapportant à une infrastructure non gouvernementale essentielle lui permettant de « mener l'activité en cause » (par. 34(3)) (l'exigence de formuler une demande écrite demeure en vigueur même dans le cas des autorisations en cas d'urgence : par. 41(4)).

---

[33] Il importe de souligner que le CST a mené d'autres opérations défensives aux termes de la LDN dans la réalisation des trois volets de son mandat pour recueillir de l'information dans le but de détecter des activités malveillantes ciblant des systèmes du gouvernement du Canada ou une infrastructure de l'information désignée comme étant d'importance par le gouvernement du Canada, et de se défendre contre celles-ci. Voir Centre de la sécurité des télécommunications, *CSEC Cyber Threat Capabilities : SIGINT and ITS: an end-to-end approach*, gouvernement du Canada, 2009 ou 2010, https://christopher-parsons.com/writings/cse-summaries/#cse-cyber-threat-capabilities.

[34] Bureau du commissaire du Centre de la sécurité des télécommunications, *Points saillants des examens et des rapports présentés au ministre en 2014-2015*, gouvernement du Canada, 2015, https://www.ocsec-bccst.gc.ca/s21/s20/d274/eng/highlights-reviews-reports-submitted, « Étant donné que le CST agit rarement dans les cas prévus à l'alinéa 184(2)c) du *Code criminel*, on peut faire valoir qu'une autorisation ministérielle applicable à la sécurité des TI émise sous le régime du paragraphe 273.65(3) de la *Loi sur la défense nationale* ne viserait pas les principales activités de cyberdéfense du CST. En conséquence, si une communication privée était interceptée pendant une activité du CST qui n'est pas prévue "dans les cas visés à l'alinéa 184(2)c) du *Code criminel*", le Centre pourrait tomber sous le coup de l'application de la partie VI du *Code criminel*. Je suis d'avis que le paragraphe 273.65(3) de la *Loi sur la défense nationale* ne reflète pas avec exactitude les activités du CST puisque le Centre entreprend des activités qui ne font pas partie des "cas visés à l'alinéa 184(2)c) du *Code criminel*". »

Recommandation 20.

Ajouter dans la LCST les critères qu'applique le ministre pour désigner comme « étant importantes pour le gouvernement fédéral » de l'information électronique, des infrastructures de l'information ou des catégories d'information électronique ou d'infrastructures de l'information aux termes du paragraphe 22(1) de la LCST.

Recommandation 21.

Modifier le paragraphe 22(1) de la LCST pour veiller à ce que les critères qui y sont établis garantissent que l'information électronique et les infrastructures de l'information désignées sont uniquement celles d'une « importance essentielle ».

La méthode de présentation d'une demande d'autorisation est autrement semblable dans ce volet du mandat et dans celui touchant le renseignement étranger. Ainsi, le chef du CST doit présenter une demande écrite exposant les faits qui permettent au ministre de conclure qu'il y a des motifs raisonnables de croire que l'autorisation est nécessaire et que les conditions énoncées au paragraphe 35(3) de la LCST sont remplies (par. 34(3)). Comme dans le contexte du renseignement étranger, l'autorisation du ministre est assujettie à l'approbation du commissaire au renseignement (art. 29), peut être prolongée pour une période d'au plus un an sans être assujettie à l'examen du commissaire et est régie par le même cadre en ce qui a trait à l'examen, à l'abrogation et à la modification si des faits sur lesquels s'appuie l'autorisation changent considérablement (art. 38-40). Dans le cas des autorisations concernant une infrastructure non gouvernementale essentielle, la demande d'autorisation doit comprendre la demande écrite du propriétaire de l'infrastructure décrit précédemment (par. 41(4)).

La LCST impose des limites en ce qui a trait à la collecte, à l'utilisation et à la conservation de toute information acquise conformément à une autorisation de cybersécurité et d'assurance de l'information. Une telle autorisation permet d'acquérir uniquement l'information nécessaire pour découvrir, isoler, prévenir ou atténuer des dommages à l'information ou à l'infrastructure non gouvernementale essentielle. En outre, Le CST ne peut conserver cette information plus longtemps que ce qui est raisonnablement nécessaire (al. 35(3)a) et 35(3)c)) et l'information identifiée comme se rapportant à un Canadien ou à une personne se trouvant au Canada sera utilisée, analysée ou conservée uniquement si elle est essentielle (al. 35(3)d)). En réalité, cela assouplit les mesures de protection de la vie privée des personnes non canadiennes prévues dans le cadre actuel de la LDN, qui interdit au CST d'acquérir, d'utiliser ou de conserver des renseignements non essentiels, sans se limiter uniquement aux renseignements concernant des Canadiens (LDN, al. 273.65(4)d)).

Enfin, l'article 45 de la LCST proposée accorde légalement au CST le pouvoir de communiquer de l'information aux personnes désignées si la communication est nécessaire pour protéger de l'information électronique et des infrastructures de l'information des institutions fédérales ou de l'information électronique et des infrastructures de l'information non gouvernementales essentielles. L'article 45 s'applique uniquement à l'information « acquise, utilisée ou analysée » au cours d'activités menées dans le cadre du volet du mandat du CST touchant la cybersécurité, ce qui limite la capacité du CST à communiquer à des fins de cybersécurité toute donnée canadienne qu'il est susceptible

d'acquérir dans le cadre des volets touchant le renseignement étranger ou l'assistance. Cependant, cet article ne limite pas la capacité du CST à communiquer de l'information à laquelle il a eu accès dans le cadre d'un autre volet de son mandat (par exemple, s'il a accédé à un réseau canadien dans le cadre du volet de son mandat touchant le renseignement étranger, mais n'a pas acquis ou analysé l'information transmise dans ce réseau[35]). En ce qui a trait à la surveillance et au contrôle, le ministre et le commissaire au renseignement doivent approuver les mesures de protection de la vie privée des Canadiens lorsque de l'information est communiquée aux termes de l'article 45.

L'article 45 est problématique, car il utilise la norme permissive du « nécessaire »; le CST a le plein pouvoir d'établir s'il respecte cette norme au cas par cas sans demander l'avis du ministre ou du commissaire au renseignement. Cette norme est plus permissive que celle du caractère « essentiel », qui s'applique généralement lorsqu'il est directement question de données privées de Canadiens. Bien que l'article 45 ne permette pas au CST de mener des activités de communication visant des Canadiens (les articles 23 et 25 continuent de s'appliquer), il permet au CST d'inclure dans l'information communiquée des communications privées interceptées (par. 45(2)). Compte tenu du fait que dans ce contexte, les communications privées se rapportent généralement à des échanges ayant au moins un lien avec des Canadiens[36], il s'ensuit que le CST communiquera des données canadiennes au moins dans certains contextes, même s'il le fait incidemment dans un ensemble de données volumineux. Cette situation est particulièrement problématique compte tenu de la capacité illimitée du ministre à désigner des personnes ou des catégories de personnes auxquelles il communiquera de l'information aux termes de l'article 45. L'article 46 prévoit que le ministre peut désigner des personnes ou des catégories de personnes, y compris des personnes du secteur privé et des gouvernements étrangers, à qui il communiquera de façon légitime de l'information aux termes de l'article 45. Ce contexte de cybersécurité favorise de façon importante la communication d'information privée de nature délicate (acquise ou interceptée pendant l'évaluation des risques de sécurité de systèmes internes) à un large éventail de parties du secteur privé et du secteur public.

Risques d'achat de logiciels malveillants à des fins défensives

Dans le cadre de ce volet de son mandat, le CST pourrait entre autres se procurer des logiciels malveillants auprès de fournisseurs dans l'objectif d'élaborer des techniques défensives servant à protéger les systèmes appartenant au gouvernement du Canada ou à des personnes désignées comme étant importantes par le gouvernement du Canada. Ces activités peuvent sembler servir les intérêts du Canada en matière de sécurité, mais en pratique, elles doivent être limitées soigneusement et être assujetties à des mesures de protection réfléchies, car elles ont nécessairement pour effet de soutenir une industrie entière dont les activités visent non pas à renforcer et à promouvoir la sécurité de

---

[35] Centre de la sécurité des télécommunications, *CSEC Cyber Threat Capabilities : SIGINT and ITS: an end-to-end approach*, gouvernement du Canada, 2009 ou 2010, https://christopher-parsons.com/writings/cse-summaries/#cse-cyber-threat-capabilities.

[36] Craig Forcese, « Putting the Law to Work for CSE: Bill C-59 and Reforming the Foreign Intelligence Collection and Cybersecurity Process », *Ottawa Faculty of Law Working Paper No. 2017-43*, 2017, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3045507; Tamir Israel, « Foreign Intelligence in an Inter-Networked World: Time for a Re-Evaluation », 2015, dans Michael Geist, dir., *Law, Privacy and Surveillance in Canada in the Post-Snowden Era*, Ottawa, Presses de l'Université d'Ottawa, p. 79, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2960283.

l'infrastructure mondiale de l'information, mais bien à la miner et à la compromettre. Les recherches du Citizen Lab démontrent constamment que les entreprises actives dans ce domaine ne sont soumises à aucune réglementation stricte, ne sont généralement pas tenues responsables des répercussions des outils qu'elles conçoivent sur les droits de la personne et ne prennent pas les mesures nécessaires pour veiller à ce que ces outils ne se retrouvent pas entre de mauvaises mains, ce qui arrive invariablement[37].

Indépendance du pouvoir exécutif

Comme il a été mentionné précédemment dans la présente section, le CST aurait l'autorisation d'intercepter des communications privées dans une infrastructure contrôlée par le gouvernement ou dans une infrastructure non gouvernementale essentielle si leur interception est raisonnablement nécessaire pour la gestion de la qualité du service de l'ordinateur ou pour la protection de l'ordinateur contre un acte qui constituerait une infraction aux paragraphes 342.1(1) (utilisation non autorisée d'un ordinateur) ou 430(1.1) (méfait à l'égard de données informatiques) du *Code criminel*. L'interception

[37] Voir les exemples suivants : Bill Marczak, Geoffrey Alexander, Sarah McKune, John Scott-Railton et Ron Deibert, « Champing At The Cyberbit: Ethiopian Dissidents Targeted with New Commercial Spyware », *Citizen Lab,* 2017, https://citizenlab.ca/2017/12/champing-cyberbit-ethiopian-dissidents-targeted-commercial-spyware/; John Scott-Railton, Bill Marczak, Bahr Abdul Razzak, Masashi Crete-Nishihata et Ron Deibert, « Reckless V: Director of Mexican Anti-Corruption Group Targeted with NSO Group's Spyware », *Citizen Lab*, 2017, https://citizenlab.ca/2017/08/nso-spyware-mexico-corruption/; John Scott-Railton, Bill Marczak, Bahr Abdul Razzak, Masashi Crete-Nishihata et Ron Deibert, « Reckless IV: Lawyers for Murdered Mexican women's Families Targeted with NSO Spyware », *Citizen Lab*, 2017, https://citizenlab.ca/2017/08/lawyers-murdered-women-nso-group/; John Scott-Railton, Bill Marczak, Bahr Abdul Razzak, Masashi Crete-Nishihata et Ron Deibert, « Reckless III: Investigation Into Mexican Mass Disappearance Targeted with NSO Spyware », *Citizen Lab*, 2017, https://citizenlab.ca/2017/07/mexico-disappearances-nso/; John Scott-Railton, Bill Marczak, Bahr Abdul Razzak, Masashi Crete-Nishihata et Ron Deibert, « Reckless Exploit: Mexican Journalists, Lawyers, and a Child Targeted with NSO Spyware », *Citizen Lab*, 2017, https://citizenlab.ca/2017/06/reckless-exploit-mexico-nso/; John Scott-Railton, Bill Marczak, Bahr Abdul Razzak, Masashi Crete-Nishihata et Ron Deibert, « Reckless Redux: Senior Mexican Legislators and Politicians Targeted with NSO Spyware », *Citizen Lab*, 2017, https://citizenlab.ca/2017/06/more-mexican-nso-targets/; Bill Marczak et John Scott-Railton, « The Million Dollar Dissident: NSO Group's iPhone Zero-Days used against a UAE Human Rights Defender », *Citizen Lab*, 2016, https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/; John Scott-Railton, Morgan Marquis-Boire, Claudio Guarnieri et Mario Marschalek, « Packrat: Seven Years of a South American Threat Actor », *Citizen Lab*, 2015, https://citizenlab.ca/2015/12/packrat-report/; Bill Marczak, John Scott-Railton, Adam Senft, Irene Poetranto et Sarah McKune, « Pay No Attention to The Server Behind The Proxy: Mapping FinFisher's Continuing Proliferation », *Citizen Lab*, 2015, https://citizenlab.ca/2015/10/mapping-finfishers-continuing-proliferation/; Bill Marczak, John Scott-Railton et Sarah McKune, « Hacking Team Reloaded? US-Based Ethiopian Journalists Again Targeted with Spyware », *Citizen Lab*, 2015, https://citizenlab.ca/2015/03/hacking-team-reloaded-us-based-ethiopian-journalists-targeted-spyware/; John Scott-Railton et Seth Hardy, « Malware Attack Targeting Syrian ISIS Critics », *Citizen Lab*, 2014, https://citizenlab.ca/2014/12/malware-attack-targeting-syrian-isis-critics/; Morgan Marquis-Boire, « Schrodinger's Cat Video and the Death of Clear-Text », *Citizen Lab*, 2014, https://citizenlab.ca/2014/08/cat-video-and-the-death-of-clear-text/; Morgan Marquis-Boire, John Scott-Railton, Claudio Guarnieri et Katie Kleemola, « Police Story: Hacking Team's Government Surveillance Malware », *Citizen Lab*, 2014, https://citizenlab.ca/2014/06/backdoor-hacking-teams-tradecraft-android-implant/; Bill Marczak, Claudio Guarnieri, Marquis-Boire et John Scott-Railton, « Hacking Team and the Targeting of Ethiopian Journalists », *Citizen Lab*, 2014, https://citizenlab.ca/2014/02/hacking-team-targeting-ethiopian-journalists/; Morgan Marquis-Boire et John Scott-Railton, « Quantum Of Surveillance: Familiar Actors and Possible False Flags in Syrian Malware Campaigns », *Citizen Lab*, 2013, https://citizenlab.ca/2013/12/syrian-malware-campaigns/; Morgan Marquis-Boire, Bill Marczak, Caludo Guarnieri et John Scott-Railton, « For Their Eyes Only: The Commercialization of Digital Spying », *Citizen Lab*, 2014, https://citizenlab.ca/2013/04/for-their-eyes-only-2/.

de telles communications n'est pas exempte de controverse. Comme l'a souligné la Bibliothèque du Parlement, la portée des activités du CST proposées en matière de surveillance des communications gouvernementales « pourrait avoir des implications en ce qui concerne la séparation constitutionnelle des pouvoirs. Les cours fédérales et la Cour suprême du Canada ont menacé de lancer une contestation constitutionnelle au vu des efforts déployés par le gouvernement pour les forcer à utiliser les services de technologie de l'information offerts par Services partagés Canada, ce qui comprend la surveillance de la cybersécurité par le CST, au motif que cela compromettrait leur indépendance[38] ».

Recommandation 22.

Modifier la LCST afin de permettre à toute institution fédérale, au sens de l'article 2, de présenter une demande écrite au ministre afin de cesser de recevoir des conseils en matière de cybersécurité, des services de surveillance et d'autres services fournis par le CST, y compris, mais sans s'y limiter, toute activité du CST qui pourrait autrement être autorisée aux termes de l'article 28.

Recommandation 23.

Pour qu'une autorisation soit délivrée aux termes du paragraphe 28(1), exiger que l'institution fédérale en question demande par écrit l'autorisation de mener l'activité, de la même façon que le prévoit le paragraphe 34(3) pour les autorisations délivrées aux termes du paragraphe 28(2).

Questions concernant les exigences actuelles fondées sur le « nécessaire » et le caractère « essentiel »

Il est difficile de savoir si la collecte, l'utilisation et la conservation doivent respecter les seuils relatifs au nécessaire ou au caractère essentiel pour atténuer un risque de dommage précis et déterminé, ou si on envisage une portée plus généralisée. De même, les dispositions proposées n'exigent pas au ministre de délivrer des autorisations en fonction d'une menace en particulier, c'est-à-dire que le ministre peut délivrer des autorisations générales pour protéger dans l'ensemble l'infrastructure non gouvernementale essentielle. Si c'est le cas, l'ampleur éventuelle de la nouvelle capacité du CST à surveiller l'infrastructure nationale est profondément troublante. Si une société de communications, comme Bell ou TELUS, demandait l'aide du CST et qu'une autorisation de cybersécurité était approuvée par la suite, le CST pourrait légalement intercepter toute communication privée effectuée sur ce réseau, car il ne serait pas tenu d'intercepter uniquement les communications ayant trait aux dommages pour lesquels son aide a été demandée. En outre, il est difficile de savoir si les limites concernant la conservation et l'utilisation de données canadiennes (sauf si elles sont essentielles ou raisonnablement nécessaires pour découvrir, isoler, prévenir ou atténuer des dommages à des infrastructures électroniques) interdiraient aussi l'analyse de l'information conservée à des fins de renseignement étranger, de renseignement criminel ou autre, lorsque ces fins secondaires pourraient contribuer aux activités du CST se rapportant à la cybersécurité et à l'assurance de l'information.

[38] Tanya Dupuis, Chloé Forget, Holly Porteous et Dominique Valiquet, Projet de loi C-59 : Loi concernant des questions de sécurité nationale, publication n° 32-1-C59-F, Bibliothèque du Parlement, 2017, p. 10.

Cyberopérations défensives et actives

LCST
Cyberopérations défensives (art. 19) En ce qui a trait au volet de son mandat touchant les cyberopérations défensives, le Centre mène des activités dans l'infrastructure mondiale de l'information ou par l'entremise de celle-ci afin d'aider à protéger : a) l'information électronique et les infrastructures de l'information des institutions fédérales; b) l'information électronique et les infrastructures de l'information d'importance pour le gouvernement fédéral désignées comme telles en vertu du paragraphe 22(1).
Cyberopérations actives (art. 20) En ce qui a trait au volet de son mandat touchant les cyberopérations actives, le Centre mène des activités dans l'infrastructure mondiale de l'information ou par l'entremise de celle-ci afin de réduire, d'interrompre, d'influencer ou de contrecarrer, selon le cas, les capacités, les intentions ou les activités de tout étranger ou État, organisme ou groupe terroriste étrangers, dans la mesure où ces capacités, ces intentions ou ces activités se rapportent aux affaires internationales, à la défense ou à la sécurité, ou afin d'intervenir dans le déroulement de telles intentions ou activités.

La LCST proposée ajoute deux « nouveaux » volets au mandat du CST, à savoir les « cyberopérations défensives » et les « cyberopérations actives ». Nous les analysons conjointement dans la présente section, car les types d'activités pouvant être autorisées et le cadre d'autorisation pour chacune d'entre elles sont en grande partie semblables (cependant, chaque volet a un objectif différent et le ministre des Affaires étrangères doit consentir aux cyberopérations actives, tandis qu'il doit seulement être consulté en ce qui concerne les cyberopérations défensives).

Le volet du mandat concernant les « cyberopérations défensives » permettrait au CST de mener des activités « afin d'aider à protéger » l'information électronique et les infrastructures de l'information des institutions fédérales ainsi que l'information électronique et les infrastructures de l'information d'importance pour le gouvernement fédéral désignées comme telles en vertu du paragraphe 22(1) (LCST, art. 19) (ci-après « information ou infrastructure non gouvernementale essentielle »). Le volet de son mandat touchant les cyberopérations actives permettrait au Centre de mener des activités « afin de réduire, d'interrompre, d'influencer ou de contrecarrer, selon le cas, les capacités, les intentions ou les activités de tout étranger ou État, organisme ou groupe terroriste étrangers, dans la mesure où ces capacités, ces intentions ou ces activités se rapportent aux affaires internationales, à la défense ou à la sécurité, ou afin d'intervenir dans le déroulement de telles intentions ou activités » (art. 20). Bien que les objectifs diffèrent, dans les deux cas, les volets proposés du mandat du CST prévoient un rôle plus « actif » que celui prévu par le passé dans une loi. Les types d'activités qui pourraient être autorisées dans les deux volets du mandat seraient les mêmes. Ils peuvent comprendre (LCST, art. 32) :

a) accéder à des portions de l'infrastructure mondiale de l'information;
b) installer, maintenir, copier, distribuer, rechercher, modifier, interrompre, supprimer ou intercepter quoi que ce soit dans l'infrastructure mondiale de l'information ou par son entremise;
c) prendre toute mesure qui est raisonnablement nécessaire pour assurer la nature secrète de l'activité;
d) mener toute autre activité qui est raisonnable dans les circonstances et est raisonnablement nécessaire pour faciliter l'exécution des activités ou des catégories d'activités visées par l'autorisation.

Le libellé de l'article 32 de la LCST proposé est extraordinairement permissif. En plus d'établir le fondement juridique permettant d'autoriser toutes sortes de piratage dirigé par l'État, cet article comporte deux catégories résiduelles d'activités qui permettent de délivrer une autorisation aux termes de laquelle le CST peut « prendre toute mesure qui est raisonnablement nécessaire pour assurer la nature secrète de l'activité » et mener toute autre activité « qui est raisonnable dans les circonstances et est raisonnablement nécessaire pour faciliter l'exécution des activités ou des catégories d'activités visées par l'autorisation » (LCST, al. 32c) et 32d)).

Le cadre d'autorisation des cyberopérations actives et défensives comporte des différences importantes comparativement à celui des activités se rapportant au renseignement étranger et à la cybersécurité. Dans le cas des cyberopérations, le chef du CST présente une demande écrite (par. 34(1)) exposant les faits qui permettent au ministre de conclure qu'il y a des motifs raisonnables de croire que l'autorisation est nécessaire et que les conditions de sa délivrance, énoncées au paragraphe 35(4), sont remplies (par. 34(2)). À la différence des activités se rapportant au renseignement étranger ou à la cybersécurité, l'autorisation entre en vigueur sans que le ministre ait à demander l'approbation du commissaire au renseignement[39]. Les activités menées dans le cadre du volet du mandat touchant les cyberopérations défensives peuvent plutôt être autorisées uniquement par le ministre, qui doit seulement consulter le ministre des Affaires étrangères (art. 30). En revanche, lorsqu'il est question d'activités menées dans le cadre du volet du mandat concernant les cyberopérations actives, le ministre ne peut délivrer l'autorisation de cyberopérations actives que si le ministre des Affaires étrangères demande ou consent qu'elle soit délivrée (par. 31(2)). Il est difficile de savoir à quoi ressembleront concrètement ces demandes ou le processus de transmission d'un avis au ministre des Affaires étrangères, particulièrement en raison de la possibilité que ces activités puissent être approuvées pour chaque catégorie.

Problèmes fondamentaux concernant les activités interdites à l'article 33

Les seules limites explicites des activités pouvant être autorisées sous le régime permissif établi à l'article 32 sont énoncées au paragraphe 33(1), qui prévoit que le CST ne peut :

[39] Cela contraste avec les autorisations de renseignement étranger ou les autorisations de cybersécurité, qui doivent être approuvées par le commissaire au renseignement avant d'entrer en vigueur.

a) causer, intentionnellement ou par négligence criminelle, des lésions corporelles à une personne physique ou la mort de celle-ci;
b) tenter intentionnellement de quelque manière d'entraver, de détourner ou de contrecarrer le cours de la justice ou de la démocratie.

Cette disposition comporte trois problèmes fondamentaux. Le premier problème réside dans le fait que ces limites explicites concernant les « interdictions » s'appliquent uniquement aux autorisations délivrées dans le cadre des volets du mandat touchant les cyberopérations actives et défensives. Autrement dit, ni l'acte de causer des lésions corporelles ou la mort (al. 33(1)a)) ni l'acte de tenter d'entraver le cours de la justice ou de la démocratie (al. 33(1)b)) sont des activités expressément interdites dans le cas des autorisations de renseignement étranger ou de cybersécurité. Partant de la supposition qu'il s'agit d'une erreur de rédaction, il est essentiel que les législateurs indiquent explicitement si le CST peut avoir l'autorisation de causer des lésions corporelles ou la mort, ou encore d'entraver « le cours de la justice ou de la démocratie » dans les autres volets de son mandat, comme au cours d'activités se rapportant au renseignement étranger.

Recommandation 31.
Modifier l'article 33 de la LCST afin qu'il s'applique à tous les volets du mandat et à toutes les activités du CST (sous réserve de l'exclusion éventuelle d'activités menées dans le cadre du volet du mandat touchant l'assistance).

Le deuxième problème réside dans le fait que le libellé de cette limite est d'une imprécision inacceptable. Bien que l'expression « lésions corporelles » ait le même sens que dans le *Code criminel* (par. 33(2)), il est possible que les questions juridiques concernant la causalité et l'utilisation des normes du droit criminel soient moins simples dans le contexte des capacités uniques du CST. Pire encore, ni le terme « justice » ni le terme « démocratie » ne sont définis dans la LCST, ce qui ouvre la porte à des interprétations superficielles ou créatives de ces termes qui compromettront leur capacité à offrir une protection significative. Les dispositions actuelles suscitent plus de questions qu'elles ne donnent de réponses. Par exemple, le gouvernement souhaite-t-il se réserver la possibilité d'intervenir dans les processus électoraux ou les processus de gouvernance d'États étrangers que le Canada ne considère pas comme des « démocraties », ou encore dans les tribunaux dont le fonctionnement ne correspond pas à la façon dont le CST interprète le concept nébuleux de « justice »?

Recommandation 33.
Modifier l'alinéa 33(1)b) de la façon suivante : « [...] tenter intentionnellement de quelque manière d'entraver, de détourner ou de contrecarrer le cours de la justice ou de la démocratie, notamment en tentant intentionnellement d'entraver, de détourner ou de contrecarrer le cours de toute procédure judiciaire ou de tout processus électoral, directement ou indirectement. »

Le troisième problème réside dans le fait que cette courte liste d'interdictions est beaucoup trop courte, qu'elle s'applique en fin de compte uniquement à ces deux volets du mandat ou aux activités du CST en général. Telle qu'elle est actuellement rédigée, la LCST permet au CST de mener un large éventail d'activités non mentionnées et profondément problématiques qui sont susceptibles de porter atteinte aux droits et aux libertés garantis par la *Charte* ou, de façon plus générale, aux obligations internationales du Canada en matière de droits de la personne. De la diffusion massive de fausse information à l'usurpation d'identité en passant par la fuite de documents étrangers dans l'objectif d'influencer des résultats politiques ou juridiques, les attaques à grande échelle par déni de service et les interventions dans le réseau de distribution d'électricité, les types d'activités envisagées à l'article 32 ne sont limitées que par l'imagination. En ce qui concerne les pouvoirs de « réduire les menaces » du SCRS, le projet de loi C-59 ajouterait une longue liste de formes de comportements qu'il serait interdit aux agents du SCRS d'adopter au cours d'activités régies par un mandat (par. 21.1(1.1) de la *Loi sur le Service canadien du renseignement de sécurité* proposée). Les types de limites imposées au SCRS au paragraphe 20(18) devraient au moins être ajoutés à l'article 33 de la LCST proposée.

***Loi sur le Service canadien du renseignement de sécurité* proposée (par. 20.1(18))**	***LCST***
Même avec une autorisation judiciaire préalable... 20.1(18) Le présent article n'a pas pour effet de justifier une personne : a) de causer, volontairement ou par négligence criminelle, des lésions corporelles à un individu ou la mort de celui-ci; b) de tenter volontairement, de quelque manière, d'entraver, de détourner ou de contrecarrer le cours de la justice; c) de porter atteinte à l'intégrité sexuelle d'un individu; d) de soumettre un individu à la torture ou à d'autres peines ou traitements cruels, inhumains ou dégradants, au sens de la Convention contre la torture; e) de détenir un individu; f) de causer la perte de biens ou des dommages importants à ceux-ci si cela porterait atteinte à la sécurité d'un individu.	Même avec une double autorisation ministérielle... 33(1) Dans le cadre de toute activité menée au titre d'une autorisation délivrée en vertu des paragraphes 30(1) ou 31(1), le Centre ne peut : a) causer, intentionnellement ou par négligence criminelle, des lésions corporelles à une personne physique ou la mort de celle-ci; b) tenter intentionnellement de quelque manière d'entraver, de détourner ou de contrecarrer le cours de la justice ou de la démocratie. **Définition de *lésions corporelles*** (2) Au paragraphe (1), *lésions corporelles* s'entend au sens de l'article 2 du *Code criminel*.

Recommandation 32.

Ajouter les alinéas suivants au paragraphe 33(1) de la LCST :

[…]

c) porter atteinte à l'intégrité sexuelle d'un individu;

d) soumettre un individu à la torture ou à d'autres peines ou traitements cruels, inhumains ou dégradants, au sens de la Convention contre la torture;

e) détenir un individu;

f) causer la perte de biens ou des dommages importants à ceux-ci si cela porterait atteinte à la sécurité d'un individu;

g) mener des activités qui sont susceptibles de compromettre la sécurité de technologies de communications, de réseaux et de services accessibles au public, y compris en affaiblissant ou en entravant les normes et les protocoles de sécurité.

Seuil bas autorisant la réalisation des activités décrites à l'article 32

En outre, le seuil autorisant la réalisation des types d'activités décrites à l'article 32 est bas, particulièrement dans le contexte des cyberopérations actives, dans le cadre desquelles le CST peut, sans fondement ou motif évident, avoir l'autorisation d'entraver « les capacités, les intentions ou les activités de tout étranger ou État, organisme ou groupe terroriste étrangers, dans la mesure où ces capacités, ces intentions ou ces activités se rapportent aux affaires internationales, à la défense ou à la sécurité » (art. 20). Cet article ne précise pas le sens que peut revêtir l'expression « se rapportent » dans ce contexte, et n'exige pas que les éléments visés par l'intervention du CST constituent une quelconque menace significative pour les intérêts du Canada en matière de sécurité. En revanche, dans d'autres lois portant sur la sécurité nationale, des expressions servent à établir le seuil à atteindre pour déclencher des activités invasives, comme « menaces envers la sécurité du Canada » (*Loi sur le Service canadien du renseignement de sécurité*, art. 2) ou « activité portant atteinte à la sécurité du Canada » (*Loi sur la communication d'information ayant trait à la sécurité du Canada*, art. 2). En fait, la nature étendue de ces deux volets du mandat proposé du CST touchant les cyberopérations et les activités correspondantes énoncées à l'article 32 empêchent toute personne de bien comprendre la nature, le type, la portée, l'objectif, les conditions de déclenchement ou les limites des activités éventuelles envisagées par la LCST d'une manière qui soulève finalement des questions relatives à la primauté du droit.

Les activités autorisées dans le cadre du volet du mandat proposé du CST touchant les cyberopérations actives ou défensives peuvent être au moins aussi invasives et problématiques que les activités du SCRS visant à « réduire les menaces », et porter autant atteinte aux droits que celles-ci. En outre (compte tenu de la nature de l'écosystème numérique), ces activités sont par nature plus susceptibles de causer des dommages collatéraux à l'infrastructure et à des parties non ciblées. Il n'a pas été prouvé que ces pouvoirs sont nécessaires ni qu'ils procureront de nets avantages pour la sécurité des Canadiens. Il convient de souligner que même si ces nouveaux volets du mandat du CST ne finissent pas par être adoptés, le CST peut tout de même participer à des activités visant à « réduire les menaces » aux côtés du SCRS dans le cadre du volet de son mandat en matière d'assistance (LCST,

art. 21, par. 26(1*), Loi sur le Service canadien du renseignement de sécurité* proposée, par. 24.1(1)). Si le Parlement est déterminé à conserver les capacités de perturbation des volets du mandat touchant les cyberopérations, il est nécessaire d'intégrer un cadre analogue au régime encadrant le mandat du SCRS prévu dans le projet de loi C-59, ou, au moins, un cadre plus solide régissant la surveillance indépendante en temps réel —ainsi qu'une liste plus détaillée des activités interdites et une liste plus limitée des activités permises. Enfin, nous tenons à souligner que l'aval législatif du piratage dirigé par le gouvernement du Canada entraîne de graves conséquences internationales sur le plan normatif et est susceptible de légitimer cette pratique et d'inciter d'autres États, y compris ceux ayant un bilan problématique sur le plan du respect des droits de la personne, à faire de même.

Recommandation 36.

Exiger au Parlement de mener une étude portant, d'une part, sur la division du travail et la répartition des rôles entre le CST et les Forces canadiennes en ce qui a trait aux cyberopérations, et d'autre part, sur la division du travail et la répartition des rôles entre le CST et le SCRS en ce qui a trait aux activités se rapportant au renseignement étranger.

Assistance technique et opérationnelle

Loi sur la défense nationale	***LCST***
Mandat (al. 273.64 (1)c)) Le mandat du Centre de la sécurité des télécommunications est le suivant : **…** c) fournir une assistance technique et opérationnelle aux organismes fédéraux chargés de l'application de la loi et de la sécurité, dans l'exercice des fonctions que la loi leur confère.	**Assistance technique et opérationnelle (art. 21)** En ce qui a trait au volet de son mandat touchant l'assistance technique et opérationnelle, le Centre fournit une assistance technique et opérationnelle aux organismes fédéraux chargés de l'application de la loi et de la sécurité, aux Forces canadiennes et au ministère de la Défense nationale.

Aux termes de la LCST, en ce qui a trait au volet du mandat du CST touchant l'assistance technique et opérationnelle, le CST devrait utiliser son expertise, ses ressources et ses capacités en matière de surveillance du CST pour fournir une assistance aux organismes fédéraux chargés de l'application de la loi et de la sécurité (art. 21). La LCST proposée énonce désormais explicitement que le CST est en mesure de soutenir les activités des Forces canadiennes et du ministère de la Défense nationale (art. 21). Lorsqu'il s'appuie sur ce volet de son mandat, le CST mène des activités sous l'autorité de l'organisme ou du ministère auquel il fournit une assistance et est assujetti aux mêmes limites que cet organisme ou ce ministère (par. 26(1)). Le personnel du CST qui mène des activités dans la réalisation de ce volet du mandat du CST bénéficie des mêmes exemptions, protections et immunités qui

s'appliqueraient s'il était employé par l'organisme auquel le CST fournit une assistance. La LCST conserve en grande partie la capacité actuelle du CST à fournir une assistance à d'autres organismes sans ajouter d'autres limites ou mesures de protection. Cette situation est problématique, car le CST mène des activités de surveillance qui seraient inconstitutionnelles si elles étaient menées par un autre organisme canadien, comme la GRC. Malgré cela, le volet du mandat du CST touchant l'assistance technique et opérationnelle met les capacités du CST en matière de surveillance à la disposition de l'organisme auquel il fournit une assistance.

Lorsqu'il mène des activités dans la réalisation du volet de son mandat touchant l'assistance technique et opérationnelle, le CST n'est pas tenu de respecter l'exigence minimale d'avoir obtenu une autorisation ministérielle comme c'est le cas dans la réalisation d'autres volets de son mandat contrevenant à la loi, et il n'est pas non plus tenu d'obtenir l'approbation du commissaire au renseignement. Les activités menées dans la réalisation du volet du mandat du CST touchant l'assistance technique et opérationnelle peuvent viser des Canadiens ou des personnes se trouvant au Canada ainsi que des parties de l'infrastructure mondiale de l'information au Canada, dans la mesure où l'organisme à qui le CST fournit de l'assistance a l'autorisation de mener ces activités. Selon un document stratégique interne récent du CST, celui-ci peut fournir de l'assistance dans la réalisation de ce volet de son mandat après avoir reçu une demande écrite de l'organisme en question, bien qu'il puisse « effectuer des travaux préliminaires en prévision de la réception d'une demande d'assistance écrite[40] ». Cependant, cette exigence n'est formulée ni dans la loi actuellement en vigueur ni dans la LCST proposée.

Les motifs justifiant l'imposition de restrictions minimales sur ce que le CST peut faire lorsqu'il fournit une assistance à d'autres organismes s'appuient sur le fait que les organismes obtenant de l'assistance doivent être dûment autorisés à mener l'activité en question et le CST dépend simplement de l'autorisation de ces organismes. Cependant, pour fournir une assistance, le CST utilise son réseau actuel de surveillance et de perturbation ainsi que les capacités de ces partenaires du Groupe des cinq. Par exemple, en 2013, la Cour fédérale a conclu que le SCRS l'avait induit en erreur en ce qui concerne la mesure dans laquelle il s'appuyait sur des organismes partenaires du Groupe des cinq lorsqu'il demandait l'assistance du CST pour intercepter les communications de Canadiens à l'étranger[41]. La Cour fédérale a conclu que ces activités ont porté atteinte aux droits internationaux de la personne et qu'il était interdit de les mener sans une autorisation légale explicite[42]. En réponse à cette décision, le gouvernement du Canada a modifié la *Loi sur le Service canadien du renseignement de sécurité* afin de créer un mécanisme régissant l'autorisation des activités du SCRS à l'étranger[43]. Cependant, lorsqu'il fournit une assistance à d'autres organismes, comme la GRC, le CST doit sans doute encore se limiter à utiliser ses propres ressources.

---

[40] Centre de la sécurité des télécommunications, *OPS-4 : Policy on Assistance to Law Enforcement and Security Agencies under Part (c) of CSE's Mandate*, gouvernement du Canada, 2016, version caviardée publiée aux termes de la *Loi sur l'accès à l'information*, https://christopher-parsons.com/wp-content/uploads/2017/12/A-2016-00101c.P.9703-Ter_001.pdf, [TRADUCTION].

[41] *X (Re)*, 2013 CF 1275.

[42] *X (Re)*, 2013 CF 1275.

[43] Voir par exemple la *Loi sur le Service canadien du renseignement de sécurité*, L.R.C. 1985, ch. C-23, par. 21(3.1).

Le recours à un vaste réseau de surveillance change à la fois la nature et la portée de l'activité menée après l'obtention d'une autorisation légale, qui devient ainsi beaucoup plus intrusive. Il n'existe cependant aucun mécanisme tenant compte de ce niveau d'intrusion accru. En développant ses capacités en matière de surveillance, le CST peut utiliser un large éventail de pratiques, dont les suivantes : créer des points de transit de données importants et y accéder; compromettre des entrepôts de données de sociétés tierces du secteur de l'Internet, comme des réseaux de médias sociaux ou des fournisseurs de messageries électroniques; trouver ou créer des vulnérabilités sur le plan de la sécurité; adopter des protocoles de chiffrement défectueux; diminuer ou coopter l'efficacité d'un logiciel antivirus; élaborer un réseau de capteurs mondial pouvant analyser le trafic mondial de données en temps réel et mener des interventions s'appuyant sur ce trafic, au cas par cas; recueillir des ensembles de données de masse qui sont publiquement en vente; acquérir ou utiliser des logiciels malveillants ou des exploits conçus pour compromettre la sécurité de l'infrastructure de l'information; mener des opérations axées sur les effets qui sont conçues pour perturber ou bouleverser psychologiquement une personne afin d'accéder à un réseau de communications ou à une base de données; compromettre des processus de mise à jour de logiciels ou intervenir dans ceux-ci afin de fournir une mesure de l'accès à ceux dépendant de l'équipement ou du logiciel ciblé. Un grand nombre de ces activités et capacités dépassent la portée des activités que peuvent légalement mener les organismes obtenant de l'assistance. Pourtant, ces organismes peuvent récolter le fruit empoisonné provenant de l'infrastructure opérationnelle du CST.

En plus de réaliser ses propres activités, le CST utilise les sources de données qu'ont recueillies ses organismes partenaires ainsi que les techniques opérationnelles qu'ils appliquent, et peut mener des activités ou des opérations dépassant la portée de celles qu'il a l'autorisation de mener. Par exemple, les alliés du CST peuvent mener des cyberopérations actives qui, si elles étaient menées par le CST, nécessiteraient le consentement du ministre des Affaires étrangères. De même, les services du renseignement étranger peuvent mener, au nom du CST, des opérations autres que celles qui ont, ou auraient, reçu l'approbation du commissaire au renseignement, ce qui permet au CST de mener, au nom d'organismes nationaux, des activités autres que celles que le CST a légalement l'autorisation de mener.

Recommandation 29.
Préciser que les données et les capacités acquises dans la réalisation des volets du mandat du CST touchant le renseignement étranger ainsi que la cybersécurité et l'assurance de l'information ne peuvent être utilisées, analysées ou communiquées au cours d'activités menées dans la réalisation du volet du mandat du CST touchant l'assistance technique et opérationnelle.

Recommandation 30.
Empêcher le CST de donner accès à l'information ou aux capacités de ses partenaires internationaux lorsqu'il fournit une assistance technique ou opérationnelle à des organismes nationaux chargés de l'application de la loi et à d'autres organismes — autrement dit, dans la réalisation du volet de son mandat touchant l'assistance, le CST devrait fournir uniquement une expertise « interne ».

ii. Examen, surveillance et contrôle indépendant

L'une des réformes les plus importantes du projet de loi C-59 portant sur le CST est l'ajout d'un cadre d'examen intégré et de contrôle externe, à savoir l'Office de surveillance des activités en matière de sécurité nationale et de renseignement (OSASNR) et le commissaire au renseignement, respectivement. Les organismes nouvellement constitués règlent de nombreux problèmes de longue date concernant le cadre de sécurité nationale du Canada, mais plusieurs lacunes sont susceptibles d'empêcher ces nouveaux mécanismes d'atteindre concrètement leur plein potentiel. En particulier, le commissaire au renseignement est loin d'offrir le niveau de contrôle externe qui serait suffisamment efficace pour veiller à ce que les opérations du CST soient proportionnelles, et ne respecte pas les exigences constitutionnelles minimales applicables à un tel contrôle.

Examen

Le projet de loi C-59 remplace le Comité de surveillance des activités de renseignement de sécurité (CSARS) – qui a actuellement la tâche d'examiner les activités du SCRS – par l'OSASNR. L'OSASNR se voit aussi attribuer les fonctions du commissaire au renseignement actuel, qui est responsable de procéder à des examens concernant les activités du CST, de faire des enquêtes et de répondre aux plaintes, et qui a diverses obligations en matière de production de rapports, dont celle de produire un rapport sur la mesure dans laquelle le CST respecte la loi (LDN, art. 273.63).

Les lacunes actuelles du cadre d'examen de la sécurité nationale du Canada sont bien documentées et étroitement liées à la nature très cloisonnée de l'examen effectué en ce moment[44]. L'examen du CSARS porte uniquement sur les activités du SCRS, le commissaire au renseignement peut examiner uniquement les activités du CST et divers autres organismes dont le mandat comporte un volet axé sur la sécurité nationale n'ont accès à aucun examen adéquat[45]. En revanche, les enquêtes modernes portant sur la sécurité nationale misent souvent sur la participation de divers organismes de façon très intégrée. En particulier, dans la réalisation du volet de son mandat touchant l'« assistance », le CST peut mettre à profit des ressources et des capacités importantes afin de soutenir d'autres organismes dans leurs efforts. Malgré ces relations étroites, le commissaire du CST peut actuellement examiner uniquement les activités des organismes à qui il fournit une assistance, ce qui limite grandement sa capacité à évaluer toutes répercussions ou toute la portée des activités en question. À l'inverse, les entités ayant la responsabilité d'examiner les organismes obtenant une assistance (comme le SCRS) ne peuvent pas évaluer les activités du CST se rapportant à leur propre mandat, ce qui crée des angles morts lorsque plusieurs organismes travaillent en collaboration. En revanche, l'OSASNR serait un organisme intégré ayant la compétence nécessaire pour examiner les activités exercées par le SCRS et

[44] Craig Forcese et Kent Roach, « The roses and the thorns of Canada's new national security bill », *Macleans*, 2017, http://www.macleans.ca/politics/ottawa/the-roses-and-thorns-of-canadas-new-national-security-bill/; Bill Robinson, « Bill C-59 : New dogs for new tricks », *Lux Ex Umbra*, 2017, https://luxexumbra.blogspot.ca/2017/07/bill-c-59-new-dogs-for-new-tricks.html; Michael Geist, « Five Eyes Wide Open: How Bill C-59 Mixes Oversight with Expansive Cyber-Security Powers », *Michael Geist* (blogue), 2017, http://www.michaelgeist.ca/2017/06/billc59/; Chuck Strahl, *Le Comité sénatorial permanent de la sécurité nationale et de la défense – Témoignages*, Parlement du Canada, 2013, https://sencanada.ca/fr/Content/Sen/committee/412/secd/51109-f.

[45] Christopher Parsons, « The Governance of Telecommunications Surveillance: How Opaque and Unaccountable Practices and Policies Threaten Canadians », *Citizen Lab*, 2015, http://www.telecomtransparency.org/wp-content/uploads/2015/05/Governance-of-Telecommunications-Surveillance-Final.pdf.

le CST, ainsi que les activités d'autres ministères se rapportant à la sécurité nationale ou au renseignement dans la mesure où ces activités sont liées à la sécurité nationale ou au renseignement (*Loi sur l'Office de surveillance des activités en matière de sécurité nationale et de renseignement*, art. 8).

L'organisme nouvellement créé pourrait suivre les répercussions des activités relatives à la sécurité nationale et au renseignement dans différents organismes et pourrait examiner les activités du CST de façon plus complète. En ce moment, le rôle du commissaire du CST consiste en grande partie à examiner les activités du CST pour veiller à ce qu'elles soient conformes à la loi (LDN, par. 273.63(2)). Cependant, ce type d'examen est limité, car aux termes de la LDN, les opérations du CST sont régies par un cadre juridique vague et très permissif et sont assujetties à des autorisations ministérielles larges qui procurent une grande latitude opérationnelle au CST. Même lorsque le CST exerce cette latitude de façon très disproportionnée, il peut sembler agir dans les limites légales, ce qui fait en sorte que le commissaire du CST a très peu d'outils pour procéder à un examen significatif de ces pratiques. Pire encore, le commissaire du CST ne peut pas imposer sa propre interprétation de la loi habilitante du CST, c'est-à-dire que l'analyse des activités du CST effectuée par le commissaire respecte en grande partie les propres interprétations et théories juridiques du CST[46]. En revanche, l'OSASNR a le mandat d'évaluer non seulement si le CST respecte la loi, mais aussi le caractère raisonnable et la nécessité de l'exercice par le CST de ses pouvoirs (LOSASNR, par. 33(2)). Ce mandat accorde à l'OSASNR une base de référence plus solide en fonction de laquelle elle peut évaluer les activités du CST.

Accessibilité de l'information en provenance de l'étranger pour l'OSASNR

L'un des problèmes éventuels de ce cadre d'examen réside dans l'incapacité de l'OSASNR à examiner les échanges du CST avec des organismes étrangers. Bien qu'en théorie l'OSASNR soit censé avoir accès « aux informations qui relèvent de tout ministère ou qui sont en la possession de tout ministère » dans le cadre de ses examens, il peut y avoir certaines lacunes lorsque des organismes du renseignement canadiens travaillent conjointement avec des alliés étrangers et qu'il est impossible de dire que des informations relèvent d'eux ou sont en leur possession, ou lorsqu'ils ne peuvent communiquer ces informations en raison de principes relatifs au droit de regard de la source (LOSASNR, art. 9). Plus précisément, on craint que l'OSASNR ne puisse accéder à de l'information en provenance de l'étranger si l'information communiquée fait l'objet de mises en garde indiquant le « droit de regard de la source ». La préoccupation concerne la possibilité que le CST considère que l'information et le renseignement d'une tierce partie obtenus de cette façon ne « relèvent » pas de lui ou ne soient pas

[46] Commissaire du Centre de la sécurité des télécommunications, *Rapport annuel 2005-2006*, avril 2006, https://www.ocsec-bccst.gc.ca/a87/ann-rpt-2005-2006_f.pdf, p. 10 et 19 – Antonio Lamer, ancien juge en chef du Canada : « Pour établir la légalité des activités exercées par le CST en vertu d'autorisations ministérielles, je tiens compte de l'interprétation que le ministère de la Justice donne des dispositions applicables de la loi. [...] Mon seul regret serait peut-être de devoir quitter mon poste avant qu'aient pu se régler les problèmes d'interprétation juridique qui compromettent la bonne marche des activités de ce bureau depuis décembre 2001. » Commissaire du Centre de la sécurité des télécommunications, *Rapport annuel* 2006-2007, mai 2007, http://publications.gc.ca/collections/collection_2007/nd-dn/D95-2007F.pdf, p. 2-3. Tamir Israel, « Foreign Intelligence in an Inter-Networked World: Time for a Re-Evaluation », 2015, dans Michael Geist, dir., *Law, Privacy and Surveillance in Canada in the Post-Snowden Era*, Ottawa, Presses de l'Université d'Ottawa, p. 72-76https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2960283.

en sa « possession », ce qui empêcherait l'OSASNR d'y accéder[47]. Comme il arrive très souvent que le CST travaille conjointement avec des organismes étrangers, cette interprétation pourrait limiter considérablement la capacité de l'OSASNR à évaluer toutes les répercussions des activités du CST.

Recommandation 1.

Modifier l'article 9 de la *Loi sur l'Office de surveillance des activités en matière de sécurité nationale et de renseignement* afin de préciser que l'OSASNR a le droit d'avoir accès aux informations qui relèvent de tout ministère ou qui sont en la possession de tout ministère, y compris à des documents en provenance de gouvernements étrangers, de leurs organismes du renseignement respectifs et d'organismes internationaux, malgré toute limite imposée par ces organismes étrangers ou par le « droit de regard de la source ».

Anciens employés d'un organisme de renseignement au sein de l'OSASNR

La LOSASNR prévoit également un secrétariat qui apportera son appui à l'office de surveillance. Dans son résumé législatif du projet de loi C-59, la Bibliothèque du Parlement souligne que « les dispositions relatives à la dotation énoncées à l'article 48 permettent au secrétariat d'embaucher des employés provenant de ministères et d'organismes, ce qui évoque la possibilité d'embaucher directement des membres du personnel d'agences du renseignement de la sécurité nationale ». Selon nous, bien que ces personnes aient certainement beaucoup d'expertise en la matière, elles n'auront généralement pas l'indépendance et la distance nécessaire, ou donneront l'impression de ne pas avoir l'indépendance et la distance nécessaire, pour effectuer des activités au sein de l'office de surveillance.

Recommandation 2.

Modifier l'article 48 de la *Loi sur l'Office de surveillance des activités en matière de sécurité nationale et de renseignement* afin d'interdire au secrétariat d'embaucher directement des membres du personnel d'agences du renseignement de la sécurité nationale, et d'imposer un délai raisonnable entre le moment où ces personnes cessent de travailler au sein d'une de ces agences et leur embauche au secrétariat.

Production de rapports sur la collecte de données portant sur des Canadiens ou se rapportant à des Canadiens

Le CST recueillera probablement un large éventail d'information concernant des Canadiens et des personnes se trouvant au Canada dans la réalisation des volets de son mandat touchant le renseignement étranger, la cybersécurité et l'assurance de l'information et l'assistance technique et opérationnelle. Cette information comprendra désormais l'information sur l'infrastructure et l'information accessible au public recueillie par le CST, qui comprendra l'information sur des Canadiens

[47] Tanya Dupuis, Chloé Forget, Holly Porteous et Dominique Valiquet, *Projet de loi C-59 : Loi concernant des questions de sécurité nationale*, publication n° 32-1-C59-F, Bibliothèque du Parlement, 2017, p. 4 et note de bas de page 12.

ou des personnes se trouvant au Canada. Compte tenu du régime permissif aux termes duquel le CST peut obtenir cette information, il devrait au moins produire des statistiques sur le nombre de fois qu'il a recueilli cette information, les motifs ou les volets de son mandat ayant justifié la collecte de l'information, le nombre de fois où de l'information anonymisée et non anonymisée a été communiquée à des partenaires étrangers, le nombre de fois où de l'information anonymisée et non anonymisée a été communiquée à des partenaires nationaux et les périodes de conservation de toute l'information recueillie. Ces rapports devraient également préciser le nombre de fois où le CST a mené des activités dans la réalisation du volet de son mandat touchant l'assistance technique et opérationnelle, et les organismes auxquels il a fourni une telle assistance. Enfin, le gouvernement du Canada devrait déclarer dans un rapport annuel les priorités en matière de renseignement étranger et de cybersécurité qu'il fixe pour le CST. Il faudrait confier soit au Comité des parlementaires sur la sécurité nationale et le renseignement[48] soit à l'OSASNR la tâche de compiler les statistiques fournies dans un rapport annuel qui sera publié, et leur donner l'autorisation d'examiner périodiquement la nécessité d'élargir les exigences en matière de tenue de documents imposées au CST, et, en conséquence, la nécessité d'ajouter des ensembles ou des sortes de statistiques dans le rapport annuel. La décision d'élargir les exigences imposées au CST en matière de production de rapports et la décision d'élargir la portée du rapport subséquent du Comité des parlementaires sur la sécurité nationale et le renseignement ou de l'OSASNR devraient revenir à leur organisme de surveillance ou d'examen respectif.

Recommandation 48.

Exiger au gouvernement du Canada de déclarer dans un rapport annuel rendu public les priorités en matière de renseignement étranger et de cybersécurité qu'il fixe pour le CST.

Recommandation 52.

Exiger la publication de la fréquence à laquelle le CST fournit une assistance technique et opérationnelle à d'autres entités ainsi que la publication du nom des organismes ayant obtenu cette assistance, dans les documents d'examen annuels du CST.

Recommandation 53.

Exiger à l'OSASNR d'examiner régulièrement la structure et l'information que fournit le CST dans son rapport annuel et donner à l'OSASNR l'autorisation de recommander que le CST ajoute des renseignements précis dans ses prochains rapports, y compris des données statistiques sur la nature et la portée de ses activités.

Recommandation 54.

Exiger la publication de rapports sur la fréquence des cyberopérations défensives et actives.

[48] Constitué par le projet de loi C-22, Loi sur le Comité des parlementaires sur la sécurité nationale et le renseignement, qui a reçu la sanction royale le 22 juin 2017, 1re session, 42e législature, 2017, http://www.parl.ca/Content/Bills/421/Government/C-22/C-22_4/C-22_4.PDF.

Surveillance et contrôle

En plus de créer l'OSASNR, le projet de loi C-59 remplace le commissaire du CST actuel par un nouveau commissaire au renseignement, ce qui se traduirait par l'instauration d'un degré de contrôle externe sur les activités du CST pour la première fois. Le commissaire au renseignement aura le pouvoir d'examiner certaines autorisations ministérielles et d'établir si les conclusions sur lesquelles reposent ces autorisations accordées ou modifiées sont raisonnables (*Loi sur le commissaire au renseignement*, art. 13-16). En particulier, le commissaire doit approuver toute autorisation ministérielle de renseignement étranger et de sécurité avant que le CST puisse mener toute activité conformément à ces autorisations, sauf « en cas d'urgence » (LCST, par. 41(2)).

Le commissaire au renseignement remédie à une lacune de longue date dans le cadre régissant le CST. À l'heure actuelle, le ministre de la Défense nationale est le principal responsable du contrôle juridique sur les activités du CST. En ce moment, le ministre délivre des autorisations que le CST doit obtenir avant d'intercepter des communications privées protégées par le *Code criminel* du Canada et est responsable d'accorder au CST tout pouvoir qu'il doit légalement avoir pour porter atteinte à des droits garantis par la *Charte*[49]. En application de la *Charte* canadienne, il faut que l'arbitre qui autorise de porter atteinte au droit de s'attendre raisonnablement à la protection de la vie privée soit une personne « tout à fait neutre et impartiale » en mesure d'agir judicieusement[50]. Toutefois, à l'heure actuelle, le ministre de la Défense nationale (aux côtés du reste du pouvoir exécutif) est responsable d'une part d'établir les priorités du CST en matière de renseignement, et d'autre part, d'autoriser l'ampleur des mesures que peut prendre le CST pour atteindre ces objectifs[51]. En général, les ministres sont régis par des facteurs liés à l'opportunité et l'intérêt public, et à leur devoir en tant que membre du pouvoir exécutif du gouvernement[52]. Ils n'ont pas l'impartialité, l'indépendance et l'objectivité nécessaire pour contrôler les activités d'un organisme comme le CST de manière judiciaire. Le commissaire du CST actuel, bien qu'il ait une certaine indépendance, n'a pas la capacité de contrôler des activités du CST – il peut uniquement procéder à un examen après coup, mais n'a aucunement le pouvoir d'engager les activités ultérieures du CST. En fait, le CST a tout simplement ignoré de nombreuses recommandations et interprétations juridiques proposées par les commissaires du CST au fil des ans.

En revanche, le commissaire au renseignement proposé peut refuser d'approuver des autorisations ministérielles se rapportant aux volets du mandat du CST touchant le renseignement étranger et la sécurité, ce qui assure un certain contrôle indépendant sur ces volets des activités du CST. Cependant,

---

[49] Tamir Israel, « Foreign Intelligence in an Inter-Networked World: Time for a Re-Evaluation », 2015, dans Michael Geist, dir., *Law, Privacy and Surveillance in Canada in the Post-Snowden Era*, Ottawa, Presses de l'Université d'Ottawa, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2960283.

[50] *Hunter c. Southam Inc,* [1984] 2 RCS 145, à 160—62; *R* c. *Vu,* [2013] 3 RCS 657, p. 46.

[51] Tamir Israel, « Foreign Intelligence in an Inter-Networked World: Time for a Re-Evaluation », 2015, dans Michael Geist, dir., *Law, Privacy and Surveillance in Canada in the Post-Snowden Era*, Ottawa, Presses de l'Université d'Ottawa, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2960283; *Loi sur la défense nationale*, al. 273.64(1)a); Bureau du commissaire du Centre de la sécurité des télécommunications, Foire aux questions, gouvernement du Canada, 2017, https://www.ocsec-bccst.gc.ca/s56/fra/frequently-asked-questions?wbdisable=true#tc-tm_9, « [l]a mise en place des priorités en matière de renseignement est une prérogative du pouvoir exécutif du gouvernement ».

[52] *Canada (Ministre du Revenu national) c. Coopers and Lybrand Ltd*, [1979] 1 RCS 495, p. 507-508.

bien que les déclarations gouvernementales décrivent le commissaire au renseignement comme le titulaire d'un poste indépendant et quasi judiciaire[53], le commissaire au renseignement n'a pas l'indépendance, les garanties procédurales ni les pouvoirs suffisants pour exercer une fonction judiciaire. La portée limitée des pouvoirs en matière de surveillance et de contrôle qui lui sont accordés entrave également le travail du titulaire de ce poste.

Nature quasi judiciaire du commissaire au renseignement

Bien que le poste de commissaire au renseignement ait toujours été décrit comme « quasi judiciaire[54] », il ne possède pas certaines caractéristiques de l'indépendance judiciaire qui auraient autrement pour effet de renforcer le rôle du commissaire. En particulier, le commissaire est nommé à titre inamovible et c'est le gouverneur en conseil qui fixe sa rémunération et prend la décision de renouveler son mandat. Ces facteurs entraînent des répercussions sur la stabilité des fonctions et peuvent avoir une incidence sur la capacité du commissaire à agir de façon entièrement indépendante ou sur la façon dont le public perçoit cette indépendance[55] (*Loi sur le commissaire au renseignement*, par. 4(1) et 4(4)). En revanche, l'homologue du commissaire au Royaume-Uni « ne peut être relevé de ses fonctions avant la fin de son mandat », sous réserve de certaines conditions non discrétionnaires énoncées explicitement, comme si le commissaire est reconnu coupable d'une infraction criminelle passible d'une peine d'emprisonnement[56]. Nous sommes aussi préoccupés par la mesure dans laquelle il est possible de s'attendre à ce que le commissaire s'acquitte significativement de ses fonctions à temps partiel (*Loi sur le commissaire au renseignement*, par. 4(3)).

Recommandation 3.

Modifier le paragraphe 4(3) de la *Loi sur le commissaire au renseignement* afin d'exiger ou au moins d'offrir la possibilité que le commissaire au renseignement exerce sa charge à temps plein.

Recommandation 4.

Modifier le paragraphe 4(4) de *la Loi sur le commissaire au renseignement* afin de prévoir que le traitement du commissaire au renseignement soit fixé en fonction du traitement d'un juge de la Cour fédérale aux termes de l'alinéa 10d) de la *Loi sur les juges* (si le commissaire continue d'exercer sa charge à temps partiel, ce traitement peut être fixé au prorata).

---

[53] Voir, par exemple, ministère de la Justice, *Énoncé concernant la Charte – Projet de loi C-59 : la Loi concernant des questions de sécurité nationale*, 20 juin 2017, http://www.justice.gc.ca/fra/sjc-csj/pl/charte-charter/sn-ns.html, « [...] la Partie 2 du projet de loi C-59, la *Loi sur le commissaire au renseignement*, créerait un poste indépendant et quasi judiciaire de commissaire au renseignement [...] ».

[54] Voir, par exemple, ministère de la Justice, *Énoncé concernant la Charte – Projet de loi C-59 : la Loi concernant des questions de sécurité nationale*, 20 juin 2017, http://www.justice.gc.ca/fra/sjc-csj/pl/charte-charter/sn-ns.html, « [...] la Partie 2 du projet de loi C-59, la *Loi sur le commissaire au renseignement*, créerait un poste indépendant et quasi judiciaire de commissaire au renseignement [...] ».

[55] *Renvoi relatif à la rémunération des juges de la Cour provinciale*, [1997] 3 RCS 3.

[56] Gouvernement du Royaume-Uni, « Investigatory Powers Act 2016 (Chapter 25) », *The National Archives*, 2016, par. 228(4) et 228(5), http://www.legislation.gov.uk/ukpga/2016/25/pdfs/ukpga_20160025_en.pdf.

Appel des décisions du commissaire au renseignement

Bien que le commissaire au renseignement doive rendre ses décisions par écrit, il est tenu de motiver sa décision uniquement lorsqu'il n'approuve pas une autorisation (*Loi sur le commissaire au renseignement*, comparer les alinéas 21a) et 21b)). Conjointement avec le fait que les décisions seront tout à fait secrètes et que le public n'y aura pas accès, cela signifie qu'il est possible d'interjeter appel des décisions du commissaire uniquement si celui-ci n'approuve pas une autorisation, et non si une autorisation a été approuvée, mais n'aurait peut-être pas dû l'être. Par conséquent, la capacité du commissaire à rendre des décisions sur les activités du CST qui feront jurisprudence demeure limitée. L'OSASNR aura la capacité d'examiner des autorisations, mais il n'existe aucun véritable mécanisme judiciaire permettant de contester des autorisations illégales ou inconstitutionnelles une fois que celles-ci ont été délivrées. En théorie, les autorisations ministérielles en soi peuvent faire l'objet d'un contrôle judiciaire, mais comme elles sont secrètes et que le public n'y a pas accès, aucune partie n'aurait les connaissances nécessaires ou le statut permettant de les contester. Il convient de souligner que même les décisions de la Foreign Intelligence Surveillance Court des États-Unis, bien qu'elles soient généralement très caviardées, sont parfois rendues publiques d'une certaine manière.

Recommandation 6.

Modifier l'alinéa 21a) de la *Loi sur le commissaire au renseignement* afin d'exiger au commissaire de motiver sa décision lorsqu'il approuve l'autorisation, la modification ou la détermination dont il est question dans cette disposition.

Recommandation 8.

Créer un mécanisme permettant de contester des décisions rendues par le commissaire au renseignement ou d'interjeter appel de ces décisions.

Recommandation 12.

Exiger, dans la mesure du possible, la publication à la fois des autorisations délivrées par le ministre et des décisions rendues par le commissaire au renseignement.

Recommandation 14.

Exiger au CST de prendre l'initiative de fournir à l'OSASNR toute interprétation juridique interne qu'il adopte si celle-ci est nouvelle ou a fait l'objet de changements importants.

Absence d'avis d'intervenants ou d'opposition

Compte tenu des importantes préoccupations constitutionnelles et relatives aux droits de la personne qui ont été soulevées, il manque une dimension d'opposition en général. Nous sommes heureux de savoir que le commissaire aura le pouvoir de retenir les services d'experts ou d'autres spécialistes (*Loi sur le commissaire au renseignement*, art. 10), mais aucun cadre ne prévoit la participation d'intervenants ou la formulation d'avis d'opposition. Le système d'examen revêt aussi une grande déférence à tous les niveaux : les ministres accordent une autorisation s'ils concluent qu'il y a « des motifs raisonnables de croire » que l'autorisation est nécessaire et que les conditions de sa délivrance

sont remplies; le commissaire au renseignement approuve ces autorisations selon la norme du caractère raisonnable; la norme du contrôle judiciaire des décisions du commissaire au renseignement (bien qu'elle ne soit pas mentionnée dans la loi) est sans doute aussi celle du caractère raisonnable.

Recommandation 5.

Modifier la *Loi sur le commissaire au renseignement* et la LCST pour veiller à ce que le commissaire au renseignement ait la capacité de soumettre les autorisations approuvées à des conditions; ait l'obligation de statuer sur la légalité, la constitutionnalité, la nécessité raisonnable et la proportionnalité de toute activité menée par le CST; et ait le pouvoir de prendre des décrets pour empêcher le CST de mener toute activité qui est illégale, inconstitutionnelle ou disproportionnée ou qui n'est pas raisonnablement nécessaire.

Recommandation 8.

Créer un mécanisme permettant de contester des décisions rendues par le commissaire au renseignement ou d'interjeter appel de ces décisions.

Recommandation 13.

Créer une certaine forme d'*amicus* ayant une autorisation de sécurité ou une autre forme d'avis d'opposition dans le processus d'autorisation des activités menées dans la réalisation des volets du mandat touchant le renseignement étranger, la cybersécurité et les cyberopérations.

Absence de pouvoirs résultant de la vérification des faits et de pouvoirs permettant de prendre des arrêtés

Les pouvoirs d'un organisme quasi judiciaire efficace ne doivent pas se limiter au simple fait d'approuver ou non des autorisations ministérielles qui lui sont présentées en fonction des documents à la disposition du ministre qui a délivré l'autorisation. Un organisme quasi judiciaire efficace doit au moins avoir la capacité d'enquêter sur les faits sous-jacents sur lesquels il doit s'appuyer pour rendre ses décisions. Par exemple, le commissaire du CST actuel a tous les pouvoirs conférés à un commissaire en vertu de la partie II de la *Loi sur les enquêtes* (LDN, par. 273.63(4)). Les homologues du commissaire au renseignement au Royaume-Uni (le commissaire aux pouvoirs d'enquête nouvellement créé et d'autres commissaires judiciaires) ont également le pouvoir de « mener les enquêtes, les inspections et les vérifications que le commissaire [en question] juge appropriées dans l'exercice de ses fonctions », peuvent exiger la communication de toute information ou de tout document exigé et peuvent même inspecter des lieux et des installations techniques au besoin dans l'exercice de leurs fonctions[57]. De même, comme il est mentionné ci-dessous, le commissaire au renseignement doit être en mesure d'exercer une surveillance et un contrôle non seulement sur les autorisations ministérielles, mais aussi sur les activités sous-jacentes du CST pour s'assurer qu'elles sont légitimes, proportionnelles et raisonnablement nécessaires. Pour atteindre cet objectif, le commissaire au renseignement devrait se

[57] Gouvernement du Royaume-Uni, « Investigatory Powers Act 2016 (Chapter 25) », *The National Archives*, 2016, art. 235, http://www.legislation.gov.uk/ukpga/2016/25/pdfs/ukpga_20160025_en.pdf [TRADUCTION].

voir accorder le pouvoir de prendre des arrêtés afin qu'il puisse empêcher le CST de mener toute activité ou de l'obliger à appliquer certaines mesures s'ajoutant à celles énoncées dans les autorisations ministérielles, au besoin. S'il y a lieu, ces pouvoirs peuvent être subordonnés à l'approbation de la Cour fédérale.

Recommandation 5.

Modifier la *Loi sur le commissaire au renseignement* et la LCST pour veiller à ce que le commissaire au renseignement ait la capacité de soumettre les autorisations approuvées à des conditions; ait l'obligation de statuer sur la légalité, la constitutionnalité, la nécessité raisonnable et la proportionnalité de toute activité menée par le CST; et ait le pouvoir de prendre des décrets pour empêcher le CST de mener toute activité qui est illégale, inconstitutionnelle ou disproportionnée ou qui n'est pas raisonnablement nécessaire.

Recommandation 7.

Modifier la *Loi sur le commissaire au renseignement* afin de conférer au commissaire au renseignement tous les pouvoirs qui sont conférés aux commissaires en vertu de la partie II de la *Loi sur les enquêtes*, comme ceux conférés au commissaire du CST actuel aux termes du paragraphe 273.63(4) de la LDN.

Portée limitée des pouvoirs en matière de surveillance et de contrôle

Selon le libellé actuel du projet de loi C-59, le commissaire au renseignement ne sera pas en mesure d'exercer le contrôle envisagé. Les autorisations ministérielles pourraient encore être délivrées, et le seraient probablement dans la majorité des cas, pour des « catégories d'activités », et non pour des activités, des opérations ou des programmes précis menés par le CST. Par conséquent, par leur nature, les autorisations n'auraient pas le niveau de précision nécessaire pour permettre au commissaire de bien évaluer ce qui est autorisé ou de veiller à ce que les activités du CST demeurent proportionnelles. Par exemple, une autorisation ministérielle en particulier peut établir un cadre général régissant l'acquisition de données sur Internet. Le cadre en soi peut être raisonnable, mais des activités d'acquisition problématiques bien précises – de celles visant à compromettre des liens de données dans le centre de données d'un fournisseur de services infonuagiques à celles visant à contraindre un administrateur de système à donner accès à un réseau – seraient probablement trop petites dans l'ensemble de la catégorie pour que le commissaire au renseignement les examine. En outre, lorsque le commissionnaire doit prendre une décision sur une autorisation concernant les activités du CST, seulement deux choix s'offrent à lui : approuver ou rejeter l'autorisation (*Loi sur le commissaire au renseignement*, par. 21(1)). En revanche, lorsque le commissaire au renseignement examine la conservation d'un ensemble de données étranger par le SCRS en application du cadre prévu dans le projet de loi C-59, il est en mesure d'approuver une autorisation assortie de conditions (*Loi sur le commissaire au renseignement*, al. 21(2)b)). Si le commissaire était en mesure d'assortir toutes les autorisations d'autres conditions, cela favoriserait le dialogue au début du processus d'autorisation et accorderait au commissaire le pouvoir de participer plus activement à l'établissement des limites et des mesures de protection de la *Charte* que le CST doit respecter.

Recommandation 5.

Modifier la *Loi sur le commissaire au renseignement* et la LCST pour veiller à ce que le commissaire au renseignement ait la capacité de soumettre les autorisations approuvées à des conditions; ait l'obligation de statuer sur la légalité, la constitutionnalité, la nécessité raisonnable et la proportionnalité de toute activité menée par le CST; et ait le pouvoir de prendre des décrets pour empêcher le CST de mener toute activité qui est illégale, inconstitutionnelle ou disproportionnée ou qui n'est pas raisonnablement nécessaire.

Le commissaire ne peut pas non plus examiner des autorisations en cas d'urgence ni prendre de décisions au sujet de telles autorisations (LCST, par. 41(2)). Le CST peut obtenir une autorisation en cas d'urgence sans l'approbation du commissaire au renseignement si le ministre a des motifs raisonnables de croire que les conditions sont remplies, mais que « le temps requis pour obtenir l'approbation du commissaire rendrait inutile l'autorisation » (LCST, par. 41(1)). Bien que ces autorisations soient assujetties aux mêmes normes du caractère raisonnable et de la proportionnalité que les autorisations habituelles (LCST, par. 35(1)), il semble que le temps soit le seul facteur additionnel justifiant une autorisation en cas d'urgence, ce qui constitue un seuil extrêmement bas pour un cadre régissant les situations « d'urgence ». Le minimum constitutionnel pour contourner les exigences d'une autorisation dans l'objectif d'intercepter des communications privées est la « situation d'urgence », que la Cour suprême du Canada a définie de façon étroite[58]. L'exercice du pouvoir d'agir dans une situation d'urgence devrait être possible uniquement lorsque le contournement du processus d'autorisation est nécessaire pour éviter des dommages sérieux. Il serait possible de reprendre une formulation légèrement meilleure qui est employée dans le contexte des ensembles de données du SCRS. Dans ce contexte, il est justifié, dans une situation d'urgence, d'autoriser l'interrogation d'un ensemble de données autrement impossible à autoriser lorsque cette interrogation est nécessaire afin « de préserver la vie ou la sécurité d'un individu » ou « d'acquérir des renseignements d'une importance considérable pour la sécurité nationale, dont la valeur sera réduite ou perdue si le Service s'en tient aux processus d'autorisation » (*Loi sur le Service canadien du renseignement de sécurité*, al. 11.22(1)b)). Cette dernière condition constitue elle aussi un seuil relativement faible, mais au moins, elle oblige le directeur du SCRS à appliquer un processus visant à établir précisément la valeur des renseignements précis recherchés et l'importance des motifs justifiant leur recherche (*Loi sur le Service canadien du renseignement de sécurité*, par. 11.22(2)). Le commissaire au renseignement participe à l'examen de ces autorisations d'interroger des ensembles de données du SCRS délivrées dans une situation d'urgence (*Loi sur le Service canadien du renseignement de sécurité*, art. 11.23), mais aux termes de la LCST, les autorisations en cas d'urgence ne peuvent faire l'objet d'un examen du commissaire au renseignement, même après coup (LCST, par. 41(2)).

Recommandation 11.

Modifier la LCST afin d'exiger que le commissaire au renseignement examine après coup toute autorisation en cas d'urgence délivrée aux termes de l'article 41.

[58] *R. c. Tse*, 2016 CSC 16, par. 10.

Recommandation 34.

Modifier la LCST afin qu'il soit possible de délivrer des autorisations en cas d'urgence uniquement lorsqu'il s'agit réellement d'une situation d'urgence.

Enfin, les activités menées dans la réalisation du volet du mandat du CST touchant les cyberopérations défensives, les cyberopérations actives ainsi que l'assistance technique et opérationnelle ne sont aucunement assujetties à l'approbation du commissaire au renseignement. L'absence d'approbation du commissaire au renseignement sur les activités se rapportant à l'assistance technique et opérationnelle reflète l'absence d'autorisation ministérielle et aggrave les problèmes soulevés par cette absence[59].

Recommandation 10.

Exiger que les activités menées dans la réalisation du volet du mandat du CST touchant l'assistance technique et opérationnelle soient assujetties à la fois à l'approbation du commissaire au renseignement et à l'autorisation du ministre.

Il est très problématique que ni le commissaire au renseignement ni aucune autre institution pouvant exercer de façon indépendante un contrôle et une surveillance ne participent au processus d'approbation des autorisations pour les activités du CST qui pourraient être menées dans la réalisation des volets de son mandat touchant les cyberopérations actives et défensives. Les autorisations délivrées dans ces deux volets laisseront au CST beaucoup plus de latitude que celle qu'il a actuellement en application de la LDN. Bien que le CST ait toujours mené, dans une certaine mesure, des activités d'interruption comme celles qui seraient autorisées aux termes de l'article 32 — par exemple en utilisant des logiciels malveillants ou en exploitant des vulnérabilités latentes des logiciels et de l'équipement pour faciliter la collecte de renseignement étranger —, en théorie, ces activités ont été menées dans l'objectif de faciliter ou de permettre la réalisation d'autres volets du mandat du CST. En revanche, les modifications proposées dans la LCST sont importantes, car elles permettraient au CST d'agir de manière offensive et préventive sans être tenu d'avoir comme objectif de contribuer aux efforts du CST en matière de renseignement étranger ou de cybersécurité.

L'absence de contrôle du commissaire au renseignement dans ces deux volets du mandat semble s'appuyer sur l'hypothèse du gouvernement selon laquelle « les cyberopérations de nature défensive ne mettraient pas par définition en jeu les droits et libertés garantis par la *Charte*[60] ». Le gouvernement reconnaît que certaines cyberopérations peuvent mettre en jeu les droits et les libertés, mais laisse sous-entendre que la nature des opérations, les limites supplémentaires interdisant les activités visant l'infrastructure canadienne, les limites supplémentaires interdisant de causer la mort ou des lésions corporelles ou de tenter de détourner le cours de la justice et de la démocratie sont suffisantes pour se passer de l'approbation du commissaire au renseignement, qui est exigée pour

[59] Ces problèmes sont décrits précédemment. Voir la section intitulée « Assistance opérationnelle et technique ».

[60] Ministère de la Justice, *Énoncé concernant la Charte – Projet de loi C-59 : la Loi concernant des questions de sécurité nationale*, 2017, http://www.justice.gc.ca/fra/sjc-csj/pl/charte-charter/sn-ns.html.

d'autres autorisations délivrées au CST[61]. Dans l'énoncé concernant la *Charte* qu'il a préparé pour le projet de loi C-59, le gouvernement du Canada précise avec raison que le ministre doit tenir compte des valeurs de la *Charte* lorsqu'il exerce son pouvoir discrétionnaire, ce qui oblige le ministre à tenir compte des répercussions sur les droits garantis par la *Charte* lorsqu'il délivre des autorisations de cyberopérations[62]. Cependant, comme il a été mentionné précédemment, le ministre n'a pas l'impartialité, l'indépendance et l'objectivité nécessaires pour prendre de telles décisions de façon judicieuse.

Il est essentiel de souligner qu'il est difficile de justifier l'hypothèse sous-jacente du gouvernement selon laquelle les activités autorisées dans la réalisation des volets du mandat touchant les cyberopérations sont moins susceptibles de mettre en jeu les libertés et les droits garantis par la *Charte*. Par leur nature, les cyberopérations sont au moins aussi susceptibles que les autres activités d'avoir des répercussions sur toutes sortes d'intérêts protégés par la *Charte* et de soulever des préoccupations relatives aux droits internationaux de la personne encore plus graves et complexes que les activités menées dans la réalisation des autres volets du mandat du CST. Il est possible de s'attendre à ce que les cyberopérations portent régulièrement atteinte à la réputation, à la liberté d'expression, aux droits garantissant la liberté de circulation, à la protection contre l'emprisonnement arbitraire et à d'autres droits. De nombreuses cyberopérations n'ont pas été soumises à l'examen rigoureux d'un tribunal, ce qui signifie que la mesure dans laquelle ils peuvent avoir des répercussions sur les intérêts garantis par la *Charte* n'est pas définie. Par conséquent, il est encore plus nécessaire d'avoir un décideur impartial agissant judicieusement.

Il est particulièrement troublant qu'il n'y ait aucun cadre significatif de surveillance ou de contrôle régissant les cyberopérations du CST compte tenu des débats parallèles sur les pouvoirs de « réduire les menaces » conférés au SCRS au départ dans la *Loi antiterroriste de 2015* (auparavant le projet de loi C-51). Les types d'activités qui peuvent être autorisées dans la réalisation des volets du mandat touchant les cyberopérations actives et défensives aux termes de la LCST ressemblent en grande partie au régime controversé dans le contexte de la *Loi sur le Service canadien du renseignement de sécurité*. Le projet de loi de 2015 accordait au SCRS de nouveaux pouvoirs très controversés de « prendre, au Canada ou à l'extérieur du Canada, des mesures pour réduire une menace envers la sécurité du Canada », ce qui lui permettait éventuellement de diffuser de la fausse information, d'entraver le fonctionnement d'outils de communication, de se faire passer pour des journalistes et de mener d'autres opérations problématiques secrètement (*Loi sur le Service canadien du renseignement de sécurité*, art. 12.1, 12.2, 21.1). Le projet de loi C-59 modifierait ces pouvoirs afin de préciser qu'un juge devrait décerner un mandat autorisant la prise de toute mesure par le SCRS qui aurait pour effet de limiter une liberté ou un droit garanti par la *Charte*. Cependant, en ce qui concerne les « cyberopérations actives » – l'équivalent numérique des nouveaux pouvoirs conférés au SCRS – la LCST et le projet de loi C-59 ne comprennent aucun cadre exigeant la délivrance d'autorisations judiciaires au préalable lorsque des activités menées par le CST limitent une liberté ou un droit garanti

[61] Ministère de la Justice, *Énoncé concernant la Charte – Projet de loi C-59 : la Loi concernant des questions de sécurité nationale*, 2017, http://www.justice.gc.ca/fra/sjc-csj/pl/charte-charter/sn-ns.html.
[62] Ministère de la Justice, *Énoncé concernant la Charte – Projet de loi C-59 : la Loi concernant des questions de sécurité nationale*, 2017, http://www.justice.gc.ca/fra/sjc-csj/pl/charte-charter/sn-ns.html.

par la *Charte*. En fait, le libellé actuel du projet de loi ne comporte même pas les formes de surveillance les plus fondamentales effectuées par le commissaire au renseignement.

Recommandation 9.
Exiger que toutes les autorisations de cyberopérations actives et défensives délivrées aux termes des articles 30 et 31 soient à la fois assujetties à l'approbation du commissaire au renseignement et au consentement du ministre des Affaires étrangères.

Pour exercer un contrôle indépendant significatif, le commissaire au renseignement doit au moins être en mesure d'examiner toutes les autorisations du CST et de se prononcer sur la légalité, la constitutionnalité et la proportionnalité de toute activité du CST. Bien que le projet de loi C-59 vise à soumettre les activités du CST à un contrôle quasi judiciaire, il n'y arrive finalement pas. Le processus demeure essentiellement dirigé par le ministre, et le commissaire au renseignement n'a ni l'indépendance, ni le contrôle, ni les mécanismes de procédure, ni les pouvoirs de surveillance suffisants pour assurer un contrôle quasi judiciaire significatif.

ii. « Aucune activité visant les Canadiens », sauf...

Aucune activité visant les Canadiens et les personnes se trouvant au Canada
23(1) Les activités menées par le Centre dans la réalisation des volets de son mandat touchant le renseignement étranger, la cybersécurité et l'assurance de l'information, les cyberopérations défensives ou les cyberopérations actives ne peuvent viser des Canadiens ou des personnes se trouvant au Canada.

Aucune activité : infrastructure mondiale de l'information au Canada ou sans autorisation
(2) Les activités menées par le Centre dans la réalisation des volets de son mandat touchant les cyberopérations défensives ou les cyberopérations actives ne peuvent viser une portion de l'infrastructure mondiale de l'information qui est au Canada ou être menées sans une autorisation délivrée en vertu des paragraphes 30(1) ou 31(1).

Aux termes de la *Loi sur la défense nationale*, les activités du CST menées dans la réalisation des volets du mandat touchant le renseignement étranger et la cybersécurité ne peuvent « viser des » Canadiens ou toute personne se trouvant au Canada (al. 273.64(2)a)). En plus de ces activités, le projet de loi C-59 limite également les activités menées dans la réalisation des nouveaux volets du mandat touchant les cyberopérations actives et défensives (LCST, par. 23(1)), et précise que les cyberopérations « ne peuvent viser une portion de l'infrastructure mondiale de l'information qui est au Canada » (par. 23(2)).

L'interdiction de mener des activités visant des Canadiens est présentée – tant sur le plan juridique que dans les débats publics – une des restrictions les plus importantes s'appliquant aux activités du CST. Il s'agit du motif généralement invoqué pour justifier les pouvoirs distinctifs et étendus qui ne sont conférés à aucun autre organisme canadien. Voici un extrait du Rapport annuel 2015-2016 du commissaire du CST qui explique ce motif :

> « Les activités du CST sont distinctes des activités de collecte de renseignements criminels et en matière de sécurité menées par d'autres organismes. Il s'agit dans leur cas d'information sur des activités qui pourraient menacer la sécurité du Canada ou la sécurité publique et que l'on obtient généralement en ciblant des Canadiens. Or, le CST se voit expressément interdire de cibler des Canadiens ou des personnes au Canada[63] ».

Ce motif ressort de nombreuses communications publiques, d'audiences parlementaires sur le CST et de décisions de tribunaux[64]. Du point de vue juridique, il s'appuie sur l'hypothèse selon laquelle l'obligation juridique du CST de respecter les droits des personnes, au sens des lois canadiennes et de la *Charte*, s'applique uniquement dans une faible mesure (voire aucunement) aux répercussions des activités du CST sur les droits et les intérêts des personnes non canadiennes.

Bien que la justification des activités étendues du CST s'appuie d'une façon fondamentale sur cette interdiction de mener des activités visant des Canadiens, cette limite relève en grande partie de la fiction et offre une faible protection des droits à la vie privée. Dans la réalité des échanges numériques modernes au sein d'un réseau, il est inévitable que des données canadiennes soient profondément mêlées à des données non canadiennes. Comme le CST a le pouvoir presque illimité de recueillir toute donnée non canadienne tant qu'il ne dépasse pas la portée de son mandat, il est ouvertement prévu que de nombreuses données canadiennes seront recueillies, utilisées et analysées de façon incidente des suites des activités du CST. Il est fort probable que ces données canadiennes soient recueillies lorsque le CST procède à la collecte massive d'information non sélectionnée (c.-à-d. surveillance à grande échelle) dans la réalisation du volet de son mandat touchant le renseignement étranger sans même tenter de limiter cette collecte d'information pour un quelconque motif, même dans l'objectif de réduire les répercussions de ces activités sur les Canadiens.

Notamment, le verbe « viser » n'est pas défini dans la LCST. En outre, le paragraphe 24(2) autorise explicitement le fait d'acquérir « incidemment » de l'information qui se rapporte à un Canadien ou à une personne se trouvant au Canada au cours d'activités de renseignement de sécurité et de cybersécurité menées au titre d'une autorisation, y compris lorsque ces activités sont menées au titre d'une autorisation en cas d'urgence. Le terme « incidemment » est nouvellement défini dans la LCST proposée. Il désigne des situations où l'information acquise « n'était pas délibérément recherchée et où le Canadien ou la personne se trouvant au Canada à qui elle se rapporte n'était pas visé par l'acquisition » (LCST, par. 24(5)). Autrement dit, l'acquisition de grandes quantités d'informations sur des Canadiens et des personnes se trouvant au Canada est non seulement inévitable dans le cadre des activités générales de collecte de données du CST, mais elle est légitime et codifiée dans la LCST.

L'interaction entre la collecte de manière « incidente » et le verbe « viser » a suscité la controverse par le passé. Il y a certaines décisions sur le terme « viser », mais celles-ci ont principalement été rendues récemment et portent sur les activités du SCRS se rapportant à l'étranger. Par exemple, en 2012, la Cour fédérale a rejeté une interprétation du verbe « viser » que le SCRS et ses avocats ont défendue

---

[63] Commissaire du Centre de la sécurité des télécommunications, *Rapport annuel 2015-2016*, gouvernement du Canada, 2015, p. 8, http://publications.gc.ca/collections/collection_2016/bccst-ocsec/D95-2016-fra.pdf.

[64] Voir Tamir Israel, « Foreign Intelligence in an Inter-Networked World: Time for a Re-Evaluation », 2015, dans Michael Geist, dir., *Law, Privacy and Surveillance in Canada in the Post-Snowden Era*, Ottawa, Presses de l'Université d'Ottawa, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2960283.

dans une affaire concernant les activités du SCRS[65], et en 2014, le CST a suspendu certaines activités non précisées de sa propre initiative des suites de cette décision[66]. Cependant, ce terme n'a fait l'objet d'aucune décision approfondie dans le contexte des activités uniques du CST. En outre, en 2016, le commissaire du CST a déclaré publiquement que le CST avait communiqué à des organismes étrangers, de manière inappropriée, de l'information permettant d'identifier des Canadiens. Bien que ces renseignements permettant d'identifier des personnes aient été communiqués involontairement, cet incident a montré que l'information recueillie « incidemment » peut s'avérer très révélatrice et que le CST recueille d'importants volumes d'informations de la sorte, même s'il lui est interdit de mener des activités visant des Canadiens ou des personnes se trouvant au Canada[67]. De plus, le CST est généralement reconnu pour utiliser les métadonnées compilées par ses partenaires du Groupe des cinq, qui ne sont aucunement tenus de supprimer les métadonnées canadiennes qu'ils recueillent incidemment et dont les bases de données sont reconnues pour comporter de très nombreuses métadonnées canadiennes[68]. Dans l'ensemble, malgré l'interdiction essentielle de mener des activités visant des Canadiens, le CST a accès à de grandes quantités de données canadiennes qu'il consulte régulièrement.

Recommandation 18.

Préciser que dans la réalisation du volet de son mandat touchant le renseignement étranger, il est interdit au CST d'acquérir, d'utiliser et d'analyser de l'information concernant des événements survenus au cours d'un échange entre deux parties ou plus de l'infrastructure mondiale de l'information qui sont, certainement ou probablement, des dispositifs finaux se trouvant au Canada.

Recommandation 19.

Modifier le paragraphe 23(2) de la LCST proposée pour empêcher le CST, dans la réalisation du volet de son mandat touchant le renseignement étranger, de mener des activités visant toute partie de l'infrastructure mondiale de l'information se trouvant au Canada.

Loin de régler ce problème de longue date, la LCST le complexifie en ajoutant au paragraphe 24(1) trois exceptions majeures à la règle générale interdisant de mener des activités visant des Canadiens ou des personnes se trouvant au Canada. Dans la présente section, nous traiterons de chacune d'entre elles.

---

[65] *Renvoi relatif aux articles 16 et 21 de la Loi sur le Service canadien du renseignement de sécurité (Re)*, 2012 CF 1437.

[66] Commissaire du Centre de la sécurité des télécommunications, *Rapport annuel 2015-2016*, gouvernement du Canada, 2015, p. 23, http://publications.gc.ca/collections/collection_2016/bccst-ocsec/D95-2016-fra.pdf.

[67] Tamir Israel et Christopher Parsons, « Why We Need to Reevaluate How We Share Intelligence Data With Allies », *Just Security*, 2016, https://www.justsecurity.org/29138/reevaluate-share-intelligence-data-allies.

[68] Voir la couverture de LEVITATION, p. ex. dans Amber Hildebrandt, Michael Pereira et Dave Seglins, « CSE tracks millions of downloads daily: Snowden documents », *CBC News*, 2015, http://www.cbc.ca/news/canada/cse-tracks-millions-of-downloads-daily-snowden-documents-1.2930120; Ryan Gallagher et Glenn Greenwald, « Canada Casts Global Surveillance Dragnet Over File Downloads «, *The Intercept,* 2015, https://theintercept.com/2015/01/28/canada-cse-levitation-mass-surveillance/; diapositives accessibles à Christopher Parsons, « LEVITATION and the FFU Hypothesis », *Canadian SIGINT Summaries*, https://christopher-parsons.com/writings/cse-summaries/#levitation-and.

Information accessible au public

> **Activités du Centre**
> 24(1) Malgré les paragraphes 23(1) et (2), le Centre peut mener les activités ci-après dans la réalisation de son mandat :
> a) acquérir, utiliser, analyser, conserver et divulguer de l'information accessible au public;
> **~**
> 2 ***information accessible au public*** Information publiée ou diffusée à l'intention du grand public, accessible au public dans l'infrastructure mondiale de l'information ou ailleurs ou disponible au public sur demande, par abonnement ou achat. (publicly available information)

Aux termes du paragraphe 24(1) de la LCST proposée, le CST peut acquérir, utiliser, analyser, conserver et divulguer « de l'information accessible au public » malgré les restrictions prévues aux paragraphes 23(1) et 23(2), qui interdisent au CST de mener des activités visant des Canadiens ou l'infrastructure canadienne. La définition de l'expression « information accessible au public » donnée dans la LCST est large et comprend l'information publiée ou diffusée à l'intention du grand public, accessible au public dans l'infrastructure mondiale de l'information ou ailleurs ou disponible au public sur demande, par abonnement ou achat (LCST, art. 2). Bien que le paragraphe 24(2) permette uniquement au CST de travailler avec de l'information accessible au public dans la réalisation de son mandat, il ne veille aucunement à ce que cette information soit acquise, utilisée, analysée, conservée ou communiquée uniquement au titre d'une autorisation ministérielle ou sous la surveillance et le contrôle du commissaire au renseignement. Par conséquent, les protections et les limites dont sont assorties les autorisations s'appliquent uniquement à l'« information accessible au public » si le CST estime que ces pratiques relatives à cette information contreviennent à une loi canadienne ou à la *Charte*.

En outre, bien que les mesures prévues à l'article 25 de la LCST pour protéger la vie privée des Canadiens s'appliquent à l'utilisation, à l'analyse, à la conservation et à la communication de l'« information accessible au public », aucune disposition ne prévoit de mesures de protection quant à l'acquisition » ou à la « collecte » de cette information, ce qui ouvre la voie à la surveillance de masse. Il a aussi été souligné que l'« utilisation du mot "communiquer" dans les nouveaux pouvoirs proposés pour le CST donne à penser que des entités externes utiliseront les renseignements accessibles au public acquis et analysés par le CST et que la banalisation de la communication est nécessaire[69] ». En fait, bien que la capacité du CST à communiquer à d'autres organismes des données permettant d'identifier des Canadiens soit principalement limitée (à l'exception de quelques situations dans la réalisation du volet de son mandat touchant le renseignement étranger, voir l'art. 44), le paragraphe 24(1) impose peu de limites à ses capacités en matière de communication. Cela peut s'avérer problématique, car si le CST communique à d'autres organismes des hypothèses se rapportant à des Canadiens, la communication de ces renseignements peut avoir de profondes répercussions et est susceptible de faire en sorte que la personne concernée soit considérée comme « suspecte » ou

[69] Tanya Dupuis, Chloé Forget, Holly Porteous et Dominique Valiquet, *Projet de loi C-59 : Loi concernant des questions de sécurité nationale*, publication n° 32-1-C59-F, Bibliothèque du Parlement, 2017, p. 8.

pire encore[70]. Les répercussions de ces communications ne sont pas atténuées par le fait que les hypothèses s'appuient sur de l'« information accessible au public ». Enfin, par le passé, de nombreuses activités de surveillance de masse du CST rendues publiques semblaient être axées sur la collecte et l'analyse de métadonnées, mais il importe de souligner que l'exception relative à l'« information accessible au public » englobe les métadonnées et du contenu sur des Canadiens et des personnes se trouvant au Canada ainsi que du contenu créé par ceux-ci.

Les activités par lesquelles le CST acquiert de l'information accessible au public sont assujetties à une seule limite, à savoir que ces activités d'acquisition doivent entrer dans la portée des volets de son mandat touchant le renseignement étranger, la cybersécurité et l'assurance de l'information ou l'assistance opérationnelle et technique[71]. Ensemble, ces mandats sont extrêmement vastes et limitent autrement de façon minimale l'information que le CST peut acquérir. En fait, de nombreux organismes du renseignement étranger équivalents au CST ont comme perspective « de tout recueillir et de trouver quoi faire avec l'information par la suite », ce qui justifie la collecte de presque toute forme d'information[72]. De plus, la capacité du CST à recueillir et à utiliser de telles données dans la réalisation du volet de son mandat touchant l'assistance est troublante. Dans la réalisation de ce mandat, le CST est limité par l'autorité légitime de l'organisme auquel il fournit une assistance. Cependant, le CST peut justifier l'acquisition antérieure d'information accessible au public pour un motif que ne peut invoquer l'organisme auquel il fournit une assistance, puis justifier la communication de ces données à l'organisme en question en s'appuyant sur un motif en accord avec l'autorité légitime de cet organisme. En conséquence, l'organisme obtenant de l'assistance peut faire quelque chose qu'il ne pourrait pas faire autrement.

L'exemption de l'« information accessible au public » s'appuie sur l'hypothèse tenace, quoiqu'erronée, selon laquelle les personnes n'ont aucun droit à la vie privée en ce qui concerne de l'information « publique ». Bien qu'elle soit intuitive, cette hypothèse est erronée à la fois sur le plan des lois et des normes, et l'accumulation illimitée de données « publiques » peut avoir de vastes répercussions sur la vie privée. À cet égard, il convient de souligner que la LPRPDE, la *Loi sur la protection des renseignements personnels* et la *Charte* prévoient toutes des mesures de protection des renseignements personnels, même lorsque ceux-ci sont « publics », et qu'elles en empêchent la collecte dans certaines circonstances[73]. En fait, comme l'article 25 exige également au CST de prendre

---

[70] Commission d'enquête sur les actions des responsables canadiens relativement à Maher Arar, *Rapport sur les événements concernant Maher Arar*, Ottawa, Travaux publics et Services gouvernementaux, 2006; *CBC News*, « Ottawa Reaches $10M Settlement with Arar », *CBC News*, 25 janvier 2007, http://www.cbc.ca/news/canada/ottawa-reaches-10m-settlement-with-arar-1.682875.

[71] Remarque : Il est interdit au CST d'acquérir de l'information dans le cadre de toute activité menée dans la réalisation des volets de son mandat touchant les cyberopérations. Voir le par. 23(2) (le CST peut mener des activités dans le cadre des volets de son mandat touchant les cyberopérations défensives et actives uniquement conformément à une autorisation) et le par. 35(4) (une autorisation de cyberopération active ou défensive peut être délivrée uniquement s'il y a des motifs raisonnables de croire « qu'aucune information ne sera acquise au titre de l'autorisation »).

[72] Elle Nakashima et Joby Warrick, « For NSA Chief, Terrorist Threat Drives Passion to 'Collect it All', Observers Say », *Washington Post*, 14 juillet 2013, https://www.washingtonpost.com/world/national-security/for-nsa-chief-terrorist-threat-drives-passion-to-collect-it-all/2013/07/14/3d26ef80-ea49-11e2-a301-ea5a8116d211_story.html?utm_term=.56130fc26087.

[73] *R. c. Wise*, [1992] 1 RCS 527; Tamir Israel et Christopher A. Parsons, « Gone Opaque? An Analysis of Hypothetical IMSI Catcher Overuse in Canada », *Citizen Lab // CIPPIC*, août 2016, https://ssrn.com/abstract=2901522; *Règlement précisant les*

des mesures pour protéger la vie privée des Canadiens et des personnes se trouvant au Canada en ce qui a trait à l'utilisation, à l'analyse, à la conservation et à la divulgation de l'« information accessible au public », il est explicitement reconnu que les types d'« information accessible au public » prévus à l'alinéa 24(1)a) sont susceptibles de porter atteinte aux droits des personnes en matière de protection de la vie privée. Le droit constitutionnel canadien reconnaît depuis longtemps qu'en l'absence de mesures de protection clairement définies (ce qui comprend souvent l'absence de surveillance judiciaire), les dispositions législatives qui permettent de ne pas répondre à des attentes raisonnables en matière de protection de la vie privée sont incohérentes avec l'article 8 de la *Charte canadienne des droits et libertés*. Telle qu'elle est actuellement formulée, la LCST exigerait au CST d'agir au titre d'une autorisation ministérielle (et des mesures de protection connexes de cette autorisation) s'il recueille de l'information accessible au public sur des Canadiens d'une façon qui ferait autrement intervenir l'article 8 de la *Charte* (LCST, par. 23(3) et 23(4)), mais la structure de l'alinéa 24(1)a) laisse entendre que cette information doit être traitée comme une catégorie d'information qu'il est possible d'acquérir sans restriction. Par conséquent, à notre avis, les dispositions de la LCST concernant l'« information accessible au public » ne respectent pas le seuil minimal des protections exigées par l'article 8.

Enfin, l'exception relative à l'information accessible au public limite d'une certaine manière l'information concernée, mais ces limites sont insuffisantes. Dans la mesure où l'expression « information accessible au public » comprend l'information faisant partie des messages radiodiffusés publiquement ou de publication ou de document publiés, le paragraphe 24(1) est moins controversé. Cela permettrait au CST d'acquérir des rapports universitaires, des rapports sur le renseignement ou de l'information sur des Canadiens diffusés à la radio ou à la télévision ou publiés dans des sites Web auquel le public a facilement accès, comme Wikipédia, et il ne serait pas nécessaire qu'un cadre de protection rigoureuse de la vie privée régisse ces activités.

La carte blanche accordée au CST en ce qui a trait aux autres formes d'information considérée comme accessible au public est plus problématique. Outre les rapports météorologiques, les articles de presse ou les publications gouvernementales, cette définition comprend de grandes quantités d'informations personnelles et privées que les personnes voudront probablement protéger ardemment conformément à leur droit à la protection de la vie privée. Par exemple, cette exception permet au CST de procéder à la collecte massive d'informations publiées ou accessibles dans les médias sociaux, comme Facebook et Twitter, y compris à l'imagerie faciale, aux publications, aux photographies, aux vidéos, aux relations, aux données de localisation publiques, aux habitudes de comportement et plus encore. Il est loin d'être clair que les Canadiens et les personnes se trouvant au Canada comprennent de façon éclairée la mesure dans laquelle leurs activités numériques créent des données qui peuvent être « accessibles ». Les gens s'attendent à un certain degré d'anonymat ou d'obscurité pratique dans la majorité de leurs activités sur Internet, et cette attente d'anonymat fait l'objet d'une protection constitutionnelle. De plus, il est nécessaire de protéger expressément des droits en matière de protection de la vie privée contre les vastes capacités du CST, au-delà de la protection prévue à l'article 8.

---

renseignements auxquels le public a accès, DORS/2001-7, 22 mars 2006, https://www.canlii.org/fr/ca/legis/regl/dors-2001-7/derniere/dors-2001-7.html.

La nature très ambiguë de certains types de métadonnées et leur transmission dans des contextes numériques sont également problématiques. Des organismes d'enquête de l'État ont parfois fait valoir que les identificateurs numériques, comme les adresses IP, sont « accessibles au public », car ils sont transmis sur Internet, précisément aux fournisseurs de services, afin de faciliter l'envoi des messages[74]. Compte tenu de cette accessibilité au public, des organismes ont avancé que ces identificateurs n'ont pas un caractère très privé et n'entraînent pas la protection de la vie privée, y compris aux termes de l'article 8 de la *Charte*, qui protège les attentes raisonnables en matière de protection de la vie privée. Ces arguments sont avancés malgré le fait que ces identificateurs sont très délicats et révélateurs, ce qui signifie qu'ils devraient entraîner la protection de la vie privée[75]. Dans une affaire en particulier, le gouvernement (en l'espèce au nom du SCRS) a fait valoir que son activité consistant à intercepter des identificateurs uniques d'appareils mobiles n'était pas visée par la protection prévue à l'article 8 de la *Charte*[76]. Les identificateurs étaient décrits comme « accessibles au public », car ils étaient transmis à des stations cellulaires sur les ondes publiques pour faciliter la prestation de services mobiles[77]. Bien que la Cour fédérale ait rejeté l'argument du SCRS dans cette affaire, ni le ministre ni le commissaire au renseignement n'auront une occasion semblable d'évaluer toute déclaration similaire que peut faire le CST aux termes de l'alinéa 24(1)a).

Les courtiers en données et en renseignements personnels ont également accès à un marché international majeur sur lequel ils vendent des renseignements permettant d'identifier une personne. Ces renseignements peuvent comprendre, par exemple, « les antécédents de crédit, l'historique de la navigation sur Internet, les achats en ligne, les contacts sur les réseaux sociaux, la situation matrimoniale et différents renseignements qui permettent la construction de profils personnels détaillés[78] ». Ils peuvent aussi comprendre de plus en plus souvent des profils psychologiques très élaborés sur des personnes et même des données détaillées sur leur état émotif[79]. Les données

---

[74] Tamir Israel et Christopher A. Parsons, « Gone Opaque? An Analysis of Hypothetical IMSI Catcher Overuse in Canada », *Citizen Lab // CIPPIC*, août 2016, https://ssrn.com/abstract=2901522.

[75] Christopher Parsons et Tamir Israel, « Gone Opaque? An Analysis of Hypothetical IMSI Catcher Overuse in Canada », *Citizen Lab // CIPPIC*, août 2016, https://ssrn.com/abstract=2901522.

[76] Dans ce cas-ci, les identificateurs en particulier recueillis par le SCRS comprennent les numéros d'identité internationale d'abonnement mobile (IMSI) et d'identité internationale d'équipement mobile (IMEI), qui sont toujours associés à des appareils mobiles et dont se servent les fournisseurs de services de télécommunications pour identifier des clients en particulier et leur combiné lorsque ces clients se connectent au réseau mobile des fournisseurs de services de télécommunications. Voir Christopher Parsons et Tamir Israel, « Gone Opaque? An Analysis of Hypothetical IMSI Catcher Overuse in Canada », *Citizen Lab // CIPPIC*, 2016, https://ssrn.com/abstract=2901522.

[77] *X (Re)*, 2017 CF 1047, par. 74 et 158 : « Enfin [le SCRS] a souligné que les IMEI et IMSI recueillies par les ESB ne sont pas cryptées et sont libres d'accès. [...] La procureure générale accorde une grande importance au fait que les IMSI et les IMEI obtenues dans le cadre d'une opération fondée sur les ESB l'ont été sur les ondes publiques, dans un contexte où ces informations sont "offertes" aux tours de téléphonie cellulaire par l'appareil mobile de la cible. À cet égard, la procureure générale établit un parallèle entre les IMEI et les IMSI communiquées "de plein gré" aux SFT et les informations relatives à la consommation d'électricité fournies aux distributeurs d'électricité dans Plant, précité. Elle établit également un parallèle avec des affaires comme Patrick, précité, où la Cour a statué qu'une attente raisonnable en matière de vie privée n'existe pas à l'égard d'informations qui ont été "abandonnées" à la poubelle. »

[78] Tanya Dupuis, Chloé Forget, Holly Porteous et Dominique Valiquet, *Projet de loi C-59 : Loi concernant des questions de sécurité nationale*, publication n° 32-1-C59-F, Bibliothèque du Parlement, 2017, p. 9.

[79] Jonathan Albright, « Cambridge Analytica : the Geotargeting and Emotional Data Mining Scripts », *Medium - TOW Center*, 2017, https://medium.com/tow-center/cambridge-analytica-the-geotargeting-and-emotional-data-mining-scripts-bcc3c428d77f.

contenues dans ces profils, bien qu'elles entrent dans la définition stricte de l'« information accessible au public » que le projet de loi C-59 propose d'inclure dans la LCST, sont néanmoins hautement privées. Nos tribunaux ont conclu que le simple fait que certains ont accès à des données hautement privées ne permet pas à l'État d'acquérir librement ces données sans aucune restriction, particulièrement dans les contextes numériques[80].

L'un des problèmes fondamentaux de l'exception de l'« information accessible au public » (outre sa portée) réside dans l'absence de toute obligation d'évaluer la façon dont cette information est devenue accessible au public ou même la légalité de cette accessibilité au public. Cependant, de nombreuses entreprises accumulant ces données afin de les distribuer à des fins commerciales ou même non commerciales sont reconnues pour ne pas respecter les lois canadiennes en matière de protection des données, comme la LPRPDE. Cette situation s'explique entre autres par le caractère international de ces entreprises, dont les données proviennent souvent de sites de médias sociaux et d'autres sources dont les activités sont principalement régies par des lois non canadiennes[81].

Cette disposition semble même permettre au CST d'acquérir de l'information que le public ne pourrait acheter ou à laquelle il ne pourrait autrement avoir accès sans contrevenir à une loi, même s'il y a néanmoins « accès ». Par conséquent, elle semble englober l'information acquise grâce à des atteintes à la protection des données, à des activités de piratage ou à des fuites intentionnelles. Dans d'autres contextes, il est reconnu que l'utilisation d'information d'« origine illicite[82] » soulève par nature de graves problèmes sur le plan éthique et pratique. Par exemple, à la suite de l'importante faille de sécurité du site Web canadien d'Ashley Madison en 2015 (décrit comme le « site le plus reconnu dans le domaine de l'infidélité et des rencontres extraconjugales » [TRADUCTION], des gigaoctets de données sur des échanges numériques de nature très délicate et sur l'activité des comptes provenant du site ont été versés sur Internet[83]. Il est difficile de savoir ce qui empêcherait le CST d'inclure ces données délicates sur les aventures extraconjugales des Canadiens (et autres) dans les bases de données qu'il utilise à des fins de profilage aux termes de l'alinéa 24(1)a). L'insouciance quant à la question de savoir si l'information a été obtenue légalement peut même signifier que telle que la LCST est actuellement rédigée, l'« information accessible au public » engloberait l'information communiquée en violation d'une loi fédérale ou provinciale en matière de protection de la vie privée, ou l'information communiquée en violation d'une entente contractuelle (par exemple entre un fournisseur de services

---

[80] *R. c. Duarte*, [1990] 1 R.C.S. 30; *R. c. Marakah*, 2017 CSC 59; *R. c. Jones*, 2017 CSC 60.

[81] Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique, Protection de la vie privée et médias sociaux à l'ère des mégadonnées, Chambre des communes, 1re session, 41e législature, avril 2013, https://www.noscommunes.ca/DocumentViewer/fr/41-1/ETHI/rapport-5; Affidavit de Tamir Israel, fait sous serment le 11 septembre 2015, *Douez* c. *Facebook Inc*, demande d'autorisation d'intervention, dossier no 36616 de la CSC, https://cippic.ca/en/news/CIPPIC_to_intervene_in_Douez_SCC_online_jurisdiction_appeal.

[82] D.R. Thomas, S. Pastrana Portillo, A. Hutchings, R.N. Clayton et A.R. Beresford, « Ethical issues in research using datasets of illicit origin », *Proceedings of the 2017 Internet Measurement Conference*, 2017, https://dl.acm.org/citation.cfm?doid=3131365.3131389. Pour obtenir une description de l'opération portant sur les marchés criminels de données, voir OCDE, *Exploring the Economics of Personal Data*, DSTI/ICCP/IE/REG(2011)2/FINAL, 2 avril 2013, p. 27 et suivantes, http://dx.doi.org/10.1787/5k486qtxldmq-en.

[83] Kim Zetter, « Hackers Finally Post Stolen Ashley Madison data », *Wired*, 2015, https://www.wired.com/2015/08/happened-hackers-posted-stolen-ashley-madison-data/. Il convient de souligner que ce type d'information peut être utilisé dans le cadre d'opérations axées sur les effets ou d'autres activités conçues pour pousser des personnes à agir comme le souhaiteraient le CST ou le gouvernement du Canada.

Internet et un abonné). En fait, les organismes du renseignement comme le CST sont reconnus pour considérer qu'à des fins de collecte de renseignements, ils peuvent légitimement mener des activités d'interception de données même s'ils savent que des criminels ont obtenu ces données illégalement[84]. En supposant que le CST éviterait d'acquérir des données s'avérant illégales, en l'absence d'une obligation de se renseigner sur la source de données accessibles publiquement ou commercialement, la question de savoir comment le CST utiliserait l'« information accessible au public » demeure très problématique. De nombreux marchés commerciaux de renseignements personnels sont « gris » et ne comportent aucun moyen de savoir comment les données ont été acquises (c.-à-d. par des moyens criminels ou non).

Compte tenu du libellé actuel de cette disposition, les acteurs du secteur privé pourraient penser que le gouvernement est à la recherche de nouveaux types de renseignements sur les Canadiens et les personnes se trouvant au Canada[85]. Ces entreprises – qui consacrent déjà beaucoup de ressources à des technologies, à des sources et à des méthodes sophistiquées de collecte, de regroupement et d'analyse de renseignements personnels – pourraient être incitées à créer et à recueillir des formes de données canadiennes qu'elles n'auraient jamais cherché à obtenir ou à exploiter auparavant, mais qui pourraient présenter un intérêt particulier pour le CST. Une demande croissante d'un organisme bien financé comme le CST pour des données canadiennes commerciales accessibles pourrait envoyer le message, y compris aux groupes criminels, que le CST est à la recherche d'information de cette nature, peu importe comment elle a été obtenue.

Recommandation 40.

Redéfinir l'expression « information accessible au public » dans la LCST pour qu'elle s'applique uniquement aux messages diffusés et aux publications accessibles sur le marché.

Recommandation 25.

Modifier l'alinéa 24(1)a) afin que le CST, malgré les restrictions prévues aux paragraphes 23(1) et 23(2), puisse uniquement acquérir, utiliser, analyser et conserver de l'information si cette information fait partie d'un ensemble de données que le commissaire au renseignement a approuvé, car il l'a jugé raisonnablement nécessaire à la réalisation des volets du mandat du CST touchant le renseignement étranger ou la cybersécurité et l'assurance de l'information.

Recommandation 26.

Modifier l'alinéa 24(1)a) afin qu'il ne s'applique plus à la « divulgation » de l'information accessible au public, ou encore, modifier l'article 25 afin qu'il garantisse que les activités visant des Canadiens qui constitueraient une divulgation de l'information accessible au public peuvent uniquement être menées au titre de l'article 44.

---

[84] National Security Agency, *Fourth Party Opportunities*, 2011 ou plus tard, https://snowdenarchive.cjfe.org/greenstone/collect/snowden1/index/assoc/HASH0188/45620b38.dir/doc.pdf [TRADUCTION].

[85] Joshua L. Simmons, « Buying You: The Government's Use of Fourth-Parties to Launder Data about 'The People' », *Columbia Business Law Review*, vol. 2009, n° 3, p. 950.

Information sur l'infrastructure

Activités du Centre
24(1) Malgré les paragraphes 23(1) et (2), le Centre peut mener les activités ci-après dans la réalisation de son mandat :

[...]

b) acquérir, utiliser, analyser, conserver et divulguer de l'information sur l'infrastructure à des fins de recherche et de développement ou de mise à l'essai de systèmes ou pour mener des activités de cybersécurité et d'assurance de l'information dans l'infrastructure à partir de laquelle celle-ci a été acquise;

~

24 (5) **information sur l'infrastructure** Information liée :
a) soit à un élément fonctionnel, physique ou logique, de l'infrastructure mondiale de l'information;
b) soit aux événements qui se produisent lors de l'interaction entre au moins deux dispositifs fournissant des services sur un réseau — à l'exclusion des dispositifs d'extrémité qui sont liés à des utilisateurs individuels — ou entre une personne physique et une machine, lorsque l'interaction concerne strictement un élément fonctionnel de l'infrastructure mondiale de l'information.

La présente définition ne vise pas l'information qui pourrait être liée à une personne identifiable.

L'alinéa 24(1)b) de la LCST proposée permet au CST de mener des activités visant des personnes se trouvant au Canada ou l'infrastructure canadienne s'il acquiert, utilise, analyse, conserve ou divulgue de l'« information sur l'infrastructure » à des fins de recherche et de développement ou de mise à l'essai de systèmes ou pour mener des activités de cybersécurité et d'assurance de l'information. L'information sur l'infrastructure est ensuite définie au paragraphe 25(5) comme de l'information liée :

> a) soit à un élément fonctionnel, physique ou logique, de l'infrastructure mondiale de l'information;
> b) soit aux événements qui se produisent lors de l'interaction entre au moins deux dispositifs fournissant des services sur un réseau — à l'exclusion des dispositifs d'extrémité qui sont liés à des utilisateurs individuels — ou entre une personne physique et une machine, lorsque l'interaction concerne strictement un élément fonctionnel de l'infrastructure mondiale de l'information.
>
> La présente définition ne vise pas l'information qui pourrait être liée à une personne identifiable.

Lorsque le CST s'appuie sur cette exception à l'interdiction de mener des activités visant des Canadiens ou l'infrastructure canadienne, il doit agir dans la portée de son mandat. Plus précisément, lorsqu'il s'appuie sur cette exception, le CST pourra acquérir de l'information dans la réalisation du volet de son mandat touchant le renseignement étranger, la cybersécurité et l'assurance de l'information ou

l'assistance technique et opérationnelle[86]. Il est inquiétant de savoir que le CST pourra aussi utiliser l'information sur l'infrastructure canadienne pour la réalisation des volets de son mandat touchant les cyberopérations actives et défensives ou à des fins de recherche et de développement ou de mise à l'essai.

Comme c'est essentiellement le cas pour l'alinéa 24(1)a), qui permet au CST de viser des Canadiens lorsqu'il mène des activités touchant de l'information accessible au public, l'exception prévue à l'alinéa 24(1)b) semble s'appuyer sur la présomption selon laquelle l'« information sur l'infrastructure » n'est pas privée de nature, et par conséquent, il n'est pas nécessaire qu'elle soit visée par les protections qu'impose la LCST pour d'autres types de données. Le fait que la définition de l'« information sur l'infrastructure » exclut l'information liée à une personne identifiable est sans doute jugé suffisant pour limiter les répercussions sur la vie privée des Canadiens. Par conséquent, l'« information sur l'infrastructure » est encore moins protégée que l'« information accessible au public ». Bien que le CST, après avoir obtenu de l'« information accessible au public », doive prendre des mesures pour protéger la vie privée des Canadiens (aux termes de l'article 25), il n'a aucune obligation de cette nature en ce qui concerne l'« information sur l'infrastructure ».

Cependant, comme c'est le cas pour l'« information accessible au public », la définition de la catégorie de l'« information sur l'infrastructure » est assez vaste pour entraîner des répercussions importantes sur les droits et les intérêts des Canadiens. Il en est de même pour l'information qui n'est pas liée directement à une personne en particulier, ce qui entraînerait l'application de la restriction sur l'inclusion d'information sur une personne identifiable. Cependant, le CST peut tout de même demeurer en mesure de rendre cette information identifiable par d'autres moyens après sa collecte.

Par exemple, en application de cette exception, le CST pourrait éventuellement compiler dans des bases de données détaillées l'emplacement de tous les routeurs Wi-Fi au Canada ainsi que les adresses IP et d'autres renseignements d'identification d'appareils ou de réseaux connexes, ce qui constituerait de l'« information sur l'infrastructure ». Cependant, une fois obtenue, cette information peut être exploitée de différentes manières très révélatrices, particulièrement si le CST peut se servir de ces données pour fournir une assistance à des organismes nationaux chargés de l'application de la loi, dans la réalisation du volet de son mandat touchant l'assistance technique et opérationnelle. Par exemple, l'un des programmes d'essai du CST utilisait ce type d'information sur l'emplacement de routeurs Wi-Fi pour prédire les déplacements de personnes en particulier après l'atterrissage de l'avion dans lequel ils prenaient place à des aéroports canadiens, et ce programme s'est avéré assez précis pour établir l'emplacement de personnes faisant des appels téléphoniques anonymes à répétition à partir d'une ville canadienne[87]. Pour donner un autre exemple, mentionnons qu'un programme de la NSA a acquis et analysé de l'« information sur l'infrastructure » détaillée au sujet de réseaux virtuels privés liés à des établissements précis (comme des réseaux liés à certains établissements bancaires) afin de créer une

[86] Comme il a été souligné en ce qui concerne l'alinéa 24(1)a) [information accessible au public] de la LCST proposée, les volets du mandat du CST touchant les cyberopérations entraîneront rarement l'application de l'alinéa 24(1)b), car ces volets de son mandat lui empêchent d'acquérir toute information. Cependant, dans les deux cas, le CST peut analyser ou utiliser l'information en question en temps réel pour mener des cyberopérations.

[87] Centre de la sécurité des télécommunications, *IP Profiling Analytics & Mission Impacts*, gouvernement du Canada, 2012, https://christopher-parsons.com/writings/cse-summaries/#ip-profiling.

« empreinte » reconnaissable des situations dans lesquelles des VPN liés à ces entreprises sont utilisés[88]. Lorsque de telles bases de données sont créées, elles peuvent servir, par exemple, à suivre les déplacements à l'étranger de représentants de cette entreprise en particulier. Il suffirait au CST (ou à l'un de ses partenaires) de chercher l'« empreinte » liée au VPN à un endroit donné.

L'information sur l'infrastructure peut aussi comprendre, par exemple, les échanges entre des personnes qui transmettent de l'information à des parties fondamentales de l'infrastructure mondiale de l'information à des fins de commande et de contrôle, y compris des commandes à des routeurs ou des certificats cryptographiques nécessaires pour protéger l'information pendant la transmission de celle-ci sur Internet. Cette information peut servir à cibler et à identifier des administrateurs de systèmes canadiens. Lorsque l'emplacement non pas de personnes en particulier, mais bien de l'information fonctionnelle transmise à une composante de l'infrastructure mondiale de l'information est déterminé, aux termes de l'alinéa 24(1)b), cette information peut ensuite être communiquée aux partenaires internationaux du CST. Elle peut alors servir à cibler l'administrateur du système pour des opérations plus intrusives, ce qui est susceptible de porter atteinte à la sécurité du réseau privé canadien en question[89]. Dans certains cas, il est même possible d'« analyser » et d'« utiliser » l'information sur l'infrastructure pour suivre les déplacements de personnes se trouvant au Canada si, par exemple, leurs appareils mobiles sont configurés comme des points d'accès sans fil, et par conséquent, n'entrent pas dans la portée de l'exclusion des « appareils terminaux » prévue à l'alinéa 24(1)b). Enfin, l'information sur l'infrastructure peut servir à porter atteinte à l'activité en ligne anonyme au Canada. Plus précisément, la collecte et l'analyse illimitées de l'information sur l'infrastructure au Canada peuvent servir à porter atteinte à la protection de la vie privée dans les VPN et les réseaux de préservation de l'anonymat, comme Tor, en analysant le temps, la taille et la nature des échanges ainsi que des composantes fonctionnelles essentielles de l'infrastructure mondiale de l'information au Canada[90].

Le CST et ses partenaires internationaux peuvent aussi utiliser l'information sur l'infrastructure pour trouver des vulnérabilités ou des faiblesses cryptologiques dans l'objectif soit d'exfiltrer de l'information, soit d'établir des proxys afin de masquer les activités ultérieures du CST. Grâce à cette exception, le CST peut être en mesure de trouver des vulnérabilités précises sur des réseaux ou des systèmes informatiques canadiens en particulier à des fins de « mise à l'essai » ou de recherche. Il peut ainsi contourner les restrictions qui lui sont imposées dans le volet de son mandat touchant la cybersécurité, qui lui interdisent d'accéder aux systèmes canadiens sans le consentement du propriétaire du système et sans désignation confirmant que le système en question est « important » aux termes du paragraphe 22(1). Cette information sur une vulnérabilité en particulier peut aussi être communiquée aux partenaires étrangers du CST en application de l'alinéa 24(1)b) à des fins de

---

[88] Voir Colin Freeze et Christine Dobby, « NSA trying to map Rogers, RBC communications traffic, leak shows », *Globe and Mail*, 2015, https://www.theglobeandmail.com/news/national/nsa-trying-to-map-rogers-rbc-communications-traffic-leak-shows/article23491118/.

[89] National Security Agency, *I hunt sysadmins (part 2)*, gouvernement des États-Unis d'Amérique, 2012, https://theintercept.com/document/2014/03/20/hunt-sys-admins/.

[90] National Security Agency, *Peeling Back the Layers of TOR with EGOTISTICALGIRAFFE*, gouvernement des États-Unis d'Amérique, 2012 ou plus tard, https://snowdenarchive.cjfe.org/greenstone/collect/snowden1/index/assoc/HASH32d5.dir/doc.pdf.

recherche et de développement ou de mise à l'essai de systèmes. Cependant, lorsque ces vulnérabilités sont communiquées, rien ne limite les fins auxquelles les partenaires étrangers en question peuvent les utiliser. Cela peut avoir directement pour effet de réduire la sécurité des réseaux canadiens, et non de l'améliorer.

Enfin, l'alinéa 24(1)b) pourrait servir à mener des cyberopérations de nature perturbatrice dans l'infrastructure canadienne à des fins de recherche et de développement ou de mise à l'essai. Ces activités seraient menées au titre d'une autorisation ministérielle (et des mesures de protection connexes), mais elles pourraient perturber les réseaux canadiens, car il n'existe aucune obligation visant à limiter ou à adapter la portée et l'échelle des opérations de mise à l'essai effectuées conformément à cette exception[91]. En fait, par le passé, le CST a effectué des « mises à l'essai » très variées touchant les données de centaines de milliers de Canadiens dans une ville donnée[92]. Les pouvoirs du CST en matière de cyberopérations sont parmi ses capacités les plus perturbatrices. La décision d'accorder au CST la latitude d'utiliser ces capacités dans les réseaux canadiens — même s'il le fait uniquement à des fins de mise à l'essai ou de recherche — peut entraîner d'importantes répercussions sur l'intégrité des réseaux et des systèmes au Canada.

Recommandation 24.

Modifier l'alinéa 24(1)b) pour faire en sorte que les activités autorisées puissent porter uniquement sur les informations électroniques et les infrastructures de l'information décrites à l'alinéa 18a) de la LCST, et être menées uniquement dans la réalisation du volet de son mandat touchant la cybersécurité et l'assurance de l'information.

Mise à l'essai

Activités du Centre

24(1) Malgré les paragraphes 23(1) et (2), le Centre peut mener les activités ci-après dans la réalisation de son mandat :

…

c) mettre à l'essai ou évaluer des produits, des logiciels et des systèmes, notamment pour des vulnérabilités.

L'alinéa 23(1)c) de la LCST proposée autoriserait le CST à « mettre à l'essai ou à évaluer des produits, des logiciels et des systèmes, notamment pour des vulnérabilités » même si ces activités visent des Canadiens ou de l'infrastructure au Canada. Bien que cette exception n'autorise pas explicitement le CST à acquérir de l'information (y compris de l'information personnelle ou autre) provenant des produits, des logiciels et des systèmes qu'il met à l'essai ou qu'il évalue, l'acquisition de cette

[91] Centre de la sécurité des télécommunications, *CASCADE : Joint Cyber Sensor Architecture*, gouvernement du Canada, 2011, https://christopher-parsons.com/writings/cse-summaries/#cse-cascade-joint.

[92] Centre de la sécurité des télécommunications, *IP Profiling Analytics & Mission Impacts*, gouvernement du Canada, 2012, https://christopher-parsons.com/writings/cse-summaries/#ip-profiling.

information n'est pas expressément interdite. Les activités doivent être menées dans la réalisation d'un des cinq volets de son mandat, et compte tenu de leur nature, les activités sont susceptibles de concerner les cinq volets du mandat. Bien que cette exception semble conçue pour faciliter la sécurité des réseaux et des appareils, sa large portée peut également avoir pour effet de porter atteinte à l'intégrité des réseaux de communication et des systèmes informatiques.

L'alinéa 24(1)c) comprend de nombreux termes nouveaux qui ne sont pas définis. Selon l'interprétation la plus limitée de cette exception, le CST pourrait mener des activités touchant un ensemble restreint de logiciels et de produits afin de trouver des vulnérabilités sur le plan de la sécurité dans l'objectif de les corriger. Cette interprétation, qui est la plus irrépréhensible, demeure toutefois préoccupante, car la disposition comprend le terme « systèmes », qui, dans le contexte de l'alinéa 24(1)b), fait clairement référence aux réseaux et aux systèmes de l'infrastructure mondiale de l'information, c'est-à-dire Internet. Cela signifie que le CST aurait le pouvoir de faire des recherches dans les réseaux et l'infrastructure du Canada à distance et subrepticement. En effet, cela contourne, d'une part, l'exigence selon laquelle le CST doit obtenir le consentement de l'opérateur du système canadien avant d'accéder à son réseau, et d'autre part, les restrictions empêchant le CST d'accéder à des réseaux canadiens qui ne sont pas considérés comme « important[s] » aux termes du paragraphe 22(1). Cependant, selon une interprétation élargie du terme « systèmes », il serait plausible de considérer qu'il englobe les réseaux internes de personnes ou d'entités canadiennes.

Ces activités de recherche dans des logiciels, des produits ou des systèmes, que ce soit en personne ou à distance, peuvent être menées dans la réalisation de tous les volets du mandat du CST. Cela comprend les volets de son mandat touchant les cyberopérations, qui s'appuient en grande partie sur l'exploitation des vulnérabilités des réseaux, et le volet de son mandat touchant le renseignement étranger. Par conséquent, le CST a le pouvoir non seulement de ne pas divulguer les vulnérabilités qu'il découvre afin de les exploiter ultérieurement[93], mais aussi de cibler un Canadien ou une infrastructure au Canada en particulier pour faire des essais et des recherches précisément dans l'objectif de trouver une vulnérabilité, puis de l'exploiter. Il en est ainsi malgré l'interdiction générale imposée au CST, qui l'empêche de mener des cyberopérations actives visant l'infrastructure au Canada ou des personnes se trouvant au Canada. Par exemple, le CST pourrait cibler des ordinateurs portables ou des appareils mobiles actifs sur les réseaux d'un aéroport pour trouver des vulnérabilités à exploiter lorsque les personnes de passage au Canada seront de retour chez elles. En outre, dans la réalisation du volet de son mandat touchant le renseignement étranger, le CST pourrait s'appuyer sur l'alinéa 24(1)c) pour intercepter intentionnellement de l'équipement de réseau expédié à un État étranger en passant par le Canada dans le but précis de l'évaluer pour des vulnérabilités. S'il trouve des vulnérabilités, le CST pourrait les exploiter immédiatement, car rien ne l'empêche de cibler de l'infrastructure au Canada au

[93] Après avoir découvert une faille dans UC Browser, un navigateur Web chinois largement utilisé, le CST et ses partenaires ont trouvé une façon de recueillir l'information qui fuyait du navigateur et qui pouvait être utilisée à des fins de mise à l'essai et de recherche. Voir Centre de la sécurité des télécommunications, Defense Signals Directorate, Government Communications Headquarters, Government Communications Security Bureau et National Security Agency, *Synergising Network Analysis Tradecraft : Network Tradecraft Advancement Team (NTAT)*, 2012 ou plus tard, https://christopher-parsons.com/writings/cse-summaries/#cse-synergising-network; Jakub Dalek, Katie Kleemola, Adam Senft, Christopher Parsons, Andrew Hilts, Sarah McKune, Jason Q. Ng, Masashi Crete-Nishihata, John Scott-Railton et Ron Deibert, « A Chatty Squirrel: Privacy and Security Issues with UC Browser », *Citizen Lab*, 2015, https://citizenlab.ca/2015/05/a-chatty-squirrel-privacy-and-security-issues-with-uc-browser/.

titre du volet de son mandat touchant le renseignement étranger. En théorie, lorsqu'il met à l'essai un système dans la réalisation du volet de son mandat touchant les cyberopérations actives, le CST pourrait activement perturber l'infrastructure canadienne dans l'objectif d'évaluer son niveau de sensibilité et de résilience. Même les activités de cette nature entreraient dans la portée de la vaste exception de la « mise à l'essai » qui est prévue actuellement.

La gamme de logiciels, de produits et de systèmes que le CST peut mettre à l'essai conformément à cette exception semble être intentionnellement vaste et presque illimitée. Elle peut comprendre les véhicules « intelligents », tout ce qui se rapporte à l'Internet des objets, en pleine expansion, la serrure en réseau installée sur la porte d'entrée de quiconque, l'équipement et les capteurs médicaux, comme un stimulateur cardiaque connecté à un réseau, les systèmes militaires ou les systèmes de défense, les routeurs Internet, les systèmes de réseau intelligent et les logiciels de systèmes électoraux, pour ne nommer que ceux-ci. Dans la majorité des cas, cette gamme est susceptible de comprendre tous les ordinateurs portables, les appareils mobiles, les appareils informatiques individuels et les périphériques réseau. Comme les services et les produits contemporains de presque tous les domaines comportent un logiciel (ou un code numérique), cette disposition permettrait au CST de mettre à l'essai ou d'évaluer presque la totalité des produits en vente aujourd'hui et des services contenant un élément numérique. Le nombre de produits qui sont numérisés et modifiés dans l'objectif de transmettre de l'information sur Internet et d'en recevoir augmente. Ainsi, le défaut de définir le terme « logiciels » permettrait au CST d'examiner n'importe quel produit ou service sans être tenu de tenter par la suite de remédier aux vulnérabilités découvertes. Des problèmes semblables se posent en ce qui concerne les termes « produits » – il est difficile de savoir ce qui n'entre pas dans la définition d'un produit – et « systèmes », qui peut actuellement être interprété comme tout ensemble de choses fonctionnant de concert.

Ce qu'on entend par « mettre à l'essai ou évaluer » est tout aussi flou. La mise à l'essai et l'évaluation peuvent consister à trouver des failles dans la façon dont un logiciel établit des communications cryptographiques ou des failles dans la conception d'un logiciel qui permettent au CST de désactiver le matériel ou d'interrompre autrement le fonctionnement normal du logiciel. Les mises à l'essai et les évaluations peuvent aussi comprendre des activités visant à interrompre activement des produits, des logiciels ou des systèmes au Canada dans l'objectif d'évaluer leur niveau de sensibilité et de résilience en prévision d'une cyberopération active que le CST mènera à l'étranger. La mise à l'essai et l'évaluation ne sont pas limitées dans le temps. Le CST pourrait, de sa propre initiative et sans le consentement du propriétaire du système ciblé au Canada, effectuer des recherches dans le système à répétition (c.-à-d. à la suite de chaque mise à niveau). Si le CST a trouvé une vulnérabilité dans un produit ou une partie d'un logiciel ou d'un système qu'il a déjà mis à l'essai, il pourrait mener des « essais » pour établir si cette vulnérabilité est présente dans des produits, des logiciels ou des systèmes semblables qui ne relèvent pas directement de son mandat. En fait, comme l'expression « mettre à l'essai ou évaluer » n'est pas définie, aucune restriction ne s'applique aux types d'activités que le CST peut mener.

Comme nous le verrons à la partie iii de la section II du présent document, le mandat du CST comporte une tension inhérente, car il exige au CST, d'une part, d'améliorer la cybersécurité du Canada en exploitant les vulnérabilités des systèmes afin de faciliter la surveillance, et d'autre part, de mener des

cyberopérations contre d'autres. L'exception prévue à l'alinéa 24(1)c) permet au CST de tirer profit de cette tension de façons très problématiques pouvant entraîner de profondes répercussions sur l'intégrité des réseaux de communication et des systèmes informatiques, et sur les biens et les intérêts des Canadiens.

Recommandation 27.
Modifier l'alinéa 21(4)c), afin, au moins, d'exiger l'obtention du consentement libre et éclairé de toute personne dont les logiciels, les produits ou les systèmes sont mis à l'essai ou évalués.

Recommandation 28.
Modifier l'alinéa 21(4)c) afin, au moins, qu'il puisse être utilisé uniquement à des fins de cybersécurité.

Caractère généralement insuffisant des mesures de protection de la vie privée prévues à l'article 25

Mesures pour protéger la vie privée
25 Le Centre veille à ce que des mesures pour protéger la vie privée des Canadiens et des personnes se trouvant au Canada soient en place en ce qui a trait à l'utilisation, à l'analyse, à la conservation et à la divulgation :
a) de l'information qui se rapporte à eux et qui a été acquise dans la réalisation des volets de son mandat touchant le renseignement étranger ou la cybersécurité et l'assurance de l'information;
b) de l'information accessible au public qui a été acquise en vertu de l'alinéa 24(1)a).

Dans la réalisation des volets de son mandat touchant le renseignement étranger et la cybersécurité, le CST est actuellement tenu de prendre des mesures de protection de la vie privée des Canadiens « lors de l'utilisation et de la conservation » des renseignements interceptés (LDN, 274.64(2)a)). L'article 25 de la LCST élargit de deux façons importantes cette protection. Premièrement, cette protection engloberait la vie privée non seulement des Canadiens, mais aussi des « personnes se trouvant au Canada ». Deuxièmement, il est précisé que des mesures doivent être prises pour protéger la vie privée « en ce qui a trait à l'utilisation, à l'analyse, à la conservation et à la divulgation » de l'information acquise dans la réalisation des volets du mandat touchant le renseignement étranger et la cybersécurité (LCST, al. 25a)). Notamment – et délibérément, compte tenu des activités de surveillance à grande échelle du CST –, ces exigences ne s'appliquent ni à l'acquisition ni à la collecte d'information.

Ces mesures doivent être prises en compte à l'étape d'autorisation des activités se rapportant au renseignement étranger et à la cybersécurité (LCST, al. 35(2)c) et 35(3)d)). Cependant, telles qu'elles sont rédigées, ces dispositions pourraient favoriser l'aveuglement volontaire quant à la question de savoir si l'information que le CST a acquise se rapporte à des Canadiens ou à des personnes se trouvant au Canada. Les dispositions qui imposent la prise de mesures de protection de la vie privée en ce qui a trait aux autorisations de renseignement étranger, de cybersécurité et d'assurance de l'information

protègent uniquement l'information qui « est identifiée comme se rapportant à un Canadien ou à une personne se trouvant au Canada » (voir les al. 35(2)c) et 35(3)d)). Si le CST n'identifie pas cette information comme se rapportant à un Canadien ou à une personne se trouvant au Canada, les mesures de protection de la vie privée ne semblent pas nécessaires. Il y a un contraste entre ce libellé et le libellé plus vaste utilisé ailleurs dans le projet de loi, qui énonce les circonstances dans lesquelles le CST peut communiquer « de l'information qui pourrait être utilisée pour identifier un Canadien ou une personne se trouvant au Canada ».

Les mesures de protection de la vie privée dont il est question à l'article 25 ne s'appliquent pas à l'information acquise dans la réalisation du volet du mandat touchant l'assistance (car ces activités relèveraient du cadre juridique de l'organisme demandant de l'assistance, comme le SCRS, la GRC ou les Forces canadiennes) ni à l'information acquise dans la réalisation des volets du mandat touchant les cyberopérations (LCST, art. 25). L'article 25 ne semble pas s'appliquer aux cyberopérations actives ou défensives, car leur autorisation doit, entre autres, satisfaire à la condition suivante : le ministre doit avoir des motifs raisonnables de croire « qu'aucune information ne sera acquise au titre de l'autorisation, sauf conformément à une autorisation délivrée en vertu des paragraphes 27(1), 28(1) ou (2) ou 41(1) » (LCST, par. 35(4)). Autrement dit, lorsque de l'information est acquise au cours de ces activités, une autorisation distincte est requise et les mesures de protection de la vie privée seront (théoriquement) prises en compte dans ce cadre. Cependant, ce système ne répond pas aux préoccupations générales concernant les répercussions des activités du CST sur la vie privée des Canadiens et des personnes se trouvant au Canada (et des droits en matière de protection de la vie privée de personnes se trouvant ailleurs dans le monde en général). Comme il est précisé ailleurs dans le présent rapport, les activités du CST sont susceptibles d'avoir une incidence sur la sécurité de l'infrastructure mondiale de l'information de différentes façons qui compromettent grandement le droit à la vie privée, la liberté d'expression et la sécurité des personnes se trouvant au Canada et ailleurs dans le monde. Tel qu'il est rédigé, l'article 25 n'empêche aucunement le CST de porter atteinte à des technologies des communications protégées, à des logiciels de chiffrement ou à des outils d'anonymat utilisés par le grand public, ou à entraver le fonctionnement de ceux-ci, malgré le fait que ces activités menacent, par leur nature, les droits à la protection de la vie privée des utilisateurs.

Il est difficile de savoir en quoi consistent les « mesures » prévues à l'article 25. Aux termes de la LCST proposée, ces mesures seraient entièrement établies dans un règlement pris par le gouverneur en conseil au lieu de faire l'objet d'un débat public rigoureux, d'un examen démocratique minutieux ou de la surveillance du commissaire à la protection de la vie privée. Par conséquent, ces mesures risquent de demeurer vagues, superficielles et assujetties aux décisions internes et secrètes du CST en soi. Nous voulons également souligner l'existence d'un autre problème majeur concernant l'article 61 de la LCST, qui permet au gouverneur en conseil de modifier « la définition de tout terme défini à l'article 2 ou aux paragraphes 24(5) ou 45(3) afin de répondre, de façon directe ou indirecte, aux changements technologiques » (al. 61c)). Autrement dit, cette disposition permettrait au pouvoir exécutif de revoir entièrement la définition de termes essentiels de la CST d'une façon qui pourrait, d'une part, changer profondément le cadre juridique régissant le CST (et entraîner des répercussions connexes sur les droits de la personne), et d'autre part, contourner l'exigence de tenir des débats publics ou de rendre

des comptes au Parlement. Il est aussi difficile de savoir si le Parlement peut constitutionnellement déléguer au gouverneur en conseil son pouvoir de modifier une loi.

Recommandation 39.
Supprimer l'alinéa 61c) de la LCST.

Enfin, la LCST proposée ne tient aucunement compte des droits des étrangers à la vie privée, malgré le fait qu'il s'agit d'une importante question à régler dans le domaine des droits internationaux de la personne. Des questions ont été soulevées à savoir si la LPRPDE pourrait cesser d'être considérée comme adéquate aux termes du *Règlement général sur la protection des données* de l'Union européenne.

Recommandation 42.
Veiller à ce que toutes les mesures prévues à l'article 25 et adoptées par règlement en application de l'alinéa 61b) dans l'objectif de protéger la vie privée des Canadiens et des personnes se trouvant au Canada soient accessibles au public afin que celui-ci puisse les analyser et formuler des commentaires à leur sujet.

Recommandation 43.
Exiger au Commissariat à la protection de la vie privée du Canada d'évaluer annuellement les protections offertes aux Canadiens et aux personnes se trouvant au Canada en application de l'article 25, et veiller à ce qu'il soit en mesure de formuler des recommandations au CST et au commissaire au renseignement.

iii. Objectifs et tensions entre les volets du mandat

La LCST proposée soulève des questions fondamentales sur la signification des activités de « cybersécurité » menées au nom d'un État et sur l'objectif général des organismes comme le CST au XXI^{e} siècle. Pour reprendre les termes de Ron Deibert :

> « Que voulons-nous dire lorsque nous parlons de "cybersécurité"? De quoi exactement assurons-nous la sécurité? Et pour qui? Est-ce que nous assurons la sécurité de l'Internet en entier, soit la vaste infrastructure mondiale de l'information qui est omniprésente dans le monde, du code des satellites aux appareils portatifs en passant par tout ce qu'il y a entre les deux.
>
> Voulons-nous plutôt dire que "nous protégeons d'abord le cyberespace de notre pays, puis les autres, si possible"? Considérons-nous qu'il est permis d'"exploiter" les réseaux des autres pays pour obtenir un avantage concurrentiel?
>
> La tension entre ces points de vue n'est pas propre à la cybersécurité. Elle reflète une tension profonde au cœur de la politique mondiale aujourd'hui, qui oppose, d'une part, un nouveau

> sens de la citoyenneté et de la responsabilité mondiale, et d'autre part, le vieux système westphalien de l'État-nation[94]. »

Cette tension est au cœur du cadre juridique régissant le CST dans le projet de loi C-59, et la LCST proposée est précisément le reflet de cette vieille façon de voir le monde. Cependant, dans un écosystème technologique mondial très interdépendant, extrêmement complexe et dont dépendent les droits de la personne partout dans le monde, cette façon de voir le monde est archaïque en plus de nuire activement aux intérêts généraux du Canada en matière de sécurité.

Les frontières nationales sont des limites inadéquates

Le paragraphe 23(2) de la LCST précise que les activités menées dans la réalisation du volet du mandat du CST touchant les cyberopérations défensives ou actives « ne peuvent viser une portion de l'infrastructure mondiale de l'information qui est au Canada ». L'absence de toute protection dans cette disposition de la LCST pour les étrangers, leurs droits et leur infrastructure — prise conjointement avec l'optique selon laquelle les intérêts en matière de sécurité des Canadiens et des personnes se trouvant au Canada sont confinés exclusivement à l'intérieur des frontières du pays — illustre cette façon « westphalienne » de voir le monde.

Cette limite territoriale contribue à limiter les répercussions et la portée des activités du CST se rapportant aux cyberopérations. Cependant, le fait qu'une partie de l'infrastructure mondiale de l'information se trouve réellement ou non « au » Canada n'est pas déterminant quant à l'ampleur des répercussions de l'accès à cette infrastructure ou du fait d'entraver le fonctionnement de celle-ci sur la sécurité, la vie privée ou les droits garantis par la *Charte* des Canadiens et des personnes se trouvant au Canada. Par exemple, les efforts déployés pour affaiblir, déjouer ou autrement miner des éléments de l'infrastructure mondiale de l'information qui sont utilisés par les Canadiens pour faciliter des communications chiffrées ou anonymes et qui ne se trouvent pas physiquement « au » Canada peuvent avoir d'importantes conséquences collatérales sur les droits de la personne des Canadiens et la sécurité mondiale en général. Le fait d'entraver le fonctionnement de parties du réseau Tor situées à l'extérieur du Canada ou de les attaquer n'est qu'un exemple d'une telle situation (notamment, le réseau Tor est responsable de protéger l'anonymat non seulement des défenseurs des droits de la personne, des chercheurs et des journalistes partout dans le monde, mais aussi des personnes travaillant pour des organismes militaires et des organismes du renseignement[95]. Dans certains cas, ces activités peuvent aussi avoir une incidence sur les droits garantis par la *Charte*, y compris, non exclusivement, ceux garantis par l'alinéa 2b) (qui protège la liberté de pensée, de croyance, d'opinion et d'expression, y compris la liberté de la presse et des autres moyens de communication), l'article 7 (le droit à la vie, à la liberté et à la sécurité de sa personne; il ne peut être porté atteinte à ce droit

---

[94] Ron Deibert, « The Cyber Security Syndrome », *OpenCanada*, 2014, https://www.opencanada.org/features/the-cyber-security-syndrome/ [TRADUCTION].

[95] Le projet Tor est un logiciel libre et un réseau ouvert qui aide les utilisateurs à se défendre contre les analyses du trafic, à préserver leur anonymat en ligne et à contourner la censure sur Internet. Tor est un réseau anonyme distribué qui achemine des données par l'entremise de « noeuds » qui se trouvent dans de nombreux pays. Voir *The Tor Project*, https://www.torproject.org/.

qu'en conformité avec les principes de justice fondamentale) et l'article 8 (le droit à la protection contre les fouilles, les perquisitions ou les saisies abusives).

Les limites prévues au paragraphe 23(2) offrent seulement une faible protection des droits des Canadiens et des personnes se trouvant au Canada. Simultanément, cette disposition ne tient pas compte des droits et des intérêts des personnes, y compris des Canadiens, à l'étranger, et peut créer des conditions permettant au CST de faire fi de ses obligations internationales en matière de droits de la personne au cours de ses cyberopérations actives et défensives. En plus des limites étroites et mal définies restreignant l'exercice de ces pouvoirs qui sont prévues à l'article 33 de la LCST (décrites précédemment), il est fort probable que le CST mène des activités qui finiront par nuire aux intérêts internationaux du Canada, menacer les droits de la personne et compromettre la sécurité de l'infrastructure mondiale de l'information.

> **Aucune activité : infrastructure mondiale de l'information au Canada ou sans autorisation**
> 23(2) Les activités menées par le Centre dans la réalisation des volets de son mandat touchant les cyberopérations défensives ou les cyberopérations actives ne peuvent viser une portion de l'infrastructure mondiale de l'information qui est au Canada [...]

Le CST contre le CST

Il existe une tension profonde entre plusieurs volets du mandat du CST, qui exigent au CST, d'une part, d'améliorer la cybersécurité du Canada en exploitant les vulnérabilités des systèmes afin de faciliter la surveillance, et d'autre part, de défendre l'information et l'infrastructure en menant des cyberopérations offensives contre d'autres. Pour reprendre les termes de Ron Deibert :

> « On peut espérer que certains organismes se concentrent sur la correction d'erreurs logicielles et s'attendre à ce qu'ils le fassent, mais simultanément, ces mêmes organismes les convoitent et les conservent, et vont même jusqu'à les acheter pour s'en servir... comme des armes. Des organismes comme la NSA ont la tâche, d'une part, de défendre des infrastructures essentielles, et d'autre part, d'alimenter une industrie de produits et de services de plusieurs millions de dollars pour les exploiter. La protection de l'intégrité des systèmes de communication est un élément essentiel de la mission, mais il est tout aussi important de créer des "portes dissimulées", une sorte de faille de sécurité prévue; ces programmes conçus pour affaiblir de façon proactive la sécurité de l'information s'appuient sur des motifs consistant à renforcer la sécurité nationale[96]. »

Par exemple, le CST met son expertise au service d'organismes de normalisation internationaux en matière de cryptographie lorsqu'il fournit des avis, des conseils et des services se rapportant à la cybersécurité et à l'assurance de l'information. On s'attend à ce que le CST, avec de multiples autres experts internationaux, relève des lacunes dans les normes proposées, propose des améliorations et joue un rôle important dans l'établissement de normes qui seront finalement adoptées par le

[96] Ron Deibert, « The Cyber Security Syndrome », *OpenCanada*, 2014, https://www.opencanada.org/features/the-cyber-security-syndrome/ [TRADUCTION].

gouvernement du Canada ainsi que par les propriétaires et les opérateurs de l'infrastructure du secteur privé.

Cependant, le CST a déjà collaboré avec la NSA pour diffuser sciemment un générateur de pseudo-aléa appelé Dual EC DRBG à des forums internationaux et au Canada même s'il savait que celui-ci était défectueux[97]. Grâce à la diffusion de cette norme, le CST et ses alliés du Groupe des cinq ont été en mesure de porter subtilement atteinte à la sécurité des communications qui utilisaient cette norme, comme d'autres parties qui ont trouvé la vulnérabilité, même si cela n'était pas prévu. Des chercheurs ont soulevé des questions concernant les lacunes de cette norme afin que l'atteinte à la sécurité ait été confirmée dans les révélations d'Edward Snowden, mais cela n'a pas empêché Dual EC DRBG d'être adopté, normalisé et intégré dans des outils commerciaux au fil des ans[98].

Cet exemple souligne les tensions entre les volets du mandat du CST touchant la cybersécurité et le renseignement étranger (ou, peut-être, les cyberopérations actives et défensives). La complicité du CST dans l'acte consistant à affaiblir délibérément des outils dont l'adoption a par la suite été recommandée au gouvernement du Canada et à l'industrie soulève des interrogations fondamentales sur la question de savoir si, et quand, les conseils formulés contribuent à l'atteinte d'un objectif se rapportant à la cybersécurité ou au renseignement étranger, et sur la question de savoir comment le CST concilie les tensions entre ces deux volets. Les alliés du Canada en matière de renseignement ont des antécédents encore plus problématiques en ce qui concerne les interventions dans les technologies de sécurité : certains programmes, comme le programme Bullrun de la NSA et le programme Edgehill du GCHQ[99], ont été précisément conçus pour réduire et miner les protections offertes par les outils de chiffrement, et pour leur porter atteinte.

Les nouveaux volets du mandat touchant les cyberopérations défensives et actives sont susceptibles d'amplifier cette tension. Dans la réalisation du volet de son mandat touchant les cyberopérations défensives, le CST pourrait « mettre à l'essai ou évaluer des produits, des logiciels et des systèmes, notamment pour des vulnérabilités » (LCST, al. 24(1)c)), mais rien ne l'oblige à divulguer publiquement les résultats de ces essais. La grande variété des activités prévues dans la réalisation du volet du mandat touchant les cyberopérations actives permettra au CST non seulement de profiter de ces vulnérabilités, mais aussi de prendre des mesures offensives d'une façon qui peut finalement accroître les tensions, provoquer des représailles ou compromettre autrement la sécurité du Canada et ses intérêts en matière de sécurité publique.

Les révélations selon lesquelles des organismes de renseignement ont déjà mené des activités dans l'objectif de porter atteinte à la sécurité d'outils de communication suscitent beaucoup de scepticisme lorsque ces mêmes organismes cherchent à donner des conseils à des organismes de normalisation

---

[97] Christopher Parsons et Tamir Israel, « Canada's Quiet History Of Weakening Communications Encryption », *Citizen Lab*, 2015, https://citizenlab.ca/2015/08/canadas-quiet-history-of-weakening-communications-encryption/.

[98] Matthew Green, « Hopefully the last post I'll ever write on Dual EC DRBG », *A Few Thoughts on Cryptographic Engineering*, 2015, https://blog.cryptographyengineering.com/2015/01/14/hopefully-last-post-ill-ever-write-on/.

[99] Voir par exemple James Ball, Julian Borger et Glenn Greenwald, « Revealed: how US and UK spy agencies defeat internet privacy and security », *The Guardian*, 2013, https://www.theguardian.com/world/2013/sep/05/nsa-gchq-encryption-codes-security; Jeff Larson, « Revealed: The NSA's Secret Campaign to Crack, Undermine Internet Security », *ProPublica*, 2013, https://www.propublica.org/article/the-nsas-secret-campaign-to-crack-undermine-internet-encryption.

internationaux et à des acteurs du secteur privé[100]. Cette méfiance affaiblit la crédibilité du CST lorsqu'il prend des mesures pour assurer l'adoption des normes et des pratiques les meilleures et les plus sûres au Canada et à l'échelle internationale. La collusion entre des organismes du renseignement et des acteurs du secteur privé mine aussi la confiance du public et des consommateurs envers les technologies de communication et de stockage offertes sur le marché. Par exemple, la perception accrue selon laquelle les équipes d'intervention en cas d'urgence informatique agissent comme des « instruments de concurrence entre États » limite la communication d'information, compromet la rapidité des interventions en réponse aux menaces et nuit aux mesures de coordination des institutions qui se veulent apolitiques[101].

Ailleurs, des chercheurs du Citizen Lab ont fait valoir que ces activités non seulement portent atteinte à la sécurité de l'infrastructure de l'information directement, mais entraînent d'importantes répercussions en aval. Les textes législatifs comme le projet de loi C-59, qui prévoit un cadre autorisant la surveillance de masse et le piratage offensif dirigé par l'État, donne un exemple problématique à la communauté internationale, car il favorise un « nivellement vers le bas » en matière de sécurité mondiale. Ce nivellement vers le bas entraîne des répercussions inquiétantes pour les personnes qui vivent dans un pays qui n'est pas régi par la primauté du droit ou qui ne bénéficient pas de protections efficaces des droits de la personne. La tendance à mener les types d'activités prévus à l'article 32 de la LCST proposée – comme l'interruption, le piratage, le fait d'entraver et la modification illégale de données – aura pour effet d'encourager et de légitimer le marché international des logiciels espions et des outils de piratage, qui finissent invariablement dans les mains d'acteurs étatiques trompeurs, d'organisations criminelles et d'autres acteurs malveillants malgré le fait qu'ils soient commercialisés pour les organismes du renseignement et les organismes chargés de l'application de la loi[102].

Pour minimiser la tension entre le rôle du CST consistant à protéger la sécurité et son rôle consistant à mener des opérations offensives dans le cyberespace, il peut s'avérer nécessaire soit de confier à un autre organisme le volet du mandat du CST touchant la cybersécurité et l'assurance de l'information – ce qui permet de séparer les opérations du CST en matière de sécurité et de renseignement –, soit de modifier le projet de loi afin de limiter la capacité du CST à mener des activités dans deux objectifs différents. Toutefois, même une modification de cette nature ne permettrait pas d'apaiser entièrement les tensions causées par la participation du gouvernement du Canada à des opérations à la fois offensives et défensives. Elle ne permettrait pas non plus de rendre illégitime le marché des logiciels espions et des outils de piratage qui servent souvent à cibler des journalistes, des législateurs, des défenseurs des droits de la personne ou des avocats.

---

[100] Joseph Menn, « Distrustful U.S. allies force spy agency to back down in encryption fight », *Reuters*, 2017, http://mobile.reuters.com/article/amp/idUSKCN1BW0GV.

[101] Voir le renvoi aux commentaires de Yuri Ito au Forum sur la gouvernance de l'Internet de 2013 à Bali dans Ron Deibert, « The Cyber Security Syndrome », *OpenCanada,* 2014, https://http://www.opencanada.org/features/the-cyber-security-syndrome/.

[102] Sarah McKune et Ron Deibert, « Who's Watching Little Brother? A Checklist for Accountability in the Industry Behind Government Hacking », *Citizen Lab*, 2017, https://citizenlab.ca/2017/03/whos-watching-little-brother-checklist-accountability-industry-behind-government-hacking/.

Recommandation 35.

Exiger au Parlement de mener une étude sur les avantages, les enjeux et la faisabilité de scinder le CST en deux organismes distincts; l'un serait exclusivement responsable de la cybersécurité, de l'assurance de l'information et de la défense, et l'autre serait exclusivement responsable des activités se rapportant au renseignement étranger et aux cyberopérations.

iv. Absence d'un processus officiel d'évaluation équitable des vulnérabilités

Dans le cadre du volet de son mandat touchant la cybersécurité et l'assurance de l'information, le CST a la tâche de détecter les menaces à l'information électronique et à l'infrastructure de l'information contrôlée par le gouvernement du Canada ainsi que les menaces équivalentes à des systèmes d'importance pour le gouvernement du Canada (LDN, al. 273.64(1)b), LCST, art. 18). Cela signifie en partie que lorsque le CST trouve des vulnérabilités sur le plan de la sécurité ou des faiblesses dans certaines parties de l'infrastructure mondiale de l'information, on s'attend à ce qu'il fournisse des avis, des conseils et des services afin d'aider le gouvernement du Canada ou des parties exploitant des systèmes d'importance pour le gouvernement du Canada à atténuer ces risques ou à y réagir. Le CST peut également communiquer les menaces et les vulnérabilités aux fabricants ou aux développeurs responsables de la production ou du maintien des moyens par lesquels l'information électronique est encodée ou l'infrastructure de l'information est protégée. En l'absence d'un cadre clair prévoyant si les vulnérabilités sont divulguées, et, le cas échéant, dans quelles circonstances et comment elles doivent l'être, l'industrie et le public n'ont aucun moyen de comprendre dans quelles conditions le CST peut décider de ne pas révéler ses découvertes pour répondre à ses propres besoins. Par exemple, lorsqu'une vulnérabilité en matière de sécurité est inconnue du public ou des développeurs et qu'elle permet au CST de contourner les mesures de protection offertes par le chiffrement, il est possible d'exploiter cette vulnérabilité pour faciliter la collecte de renseignements étrangers. Cependant, la décision de conserver – et de ne pas divulguer – ce type de vulnérabilités soulève la possibilité que des adversaires, y compris des États étrangers et des organisations criminelles, les exploitent eux aussi.

Le gouvernement des États-Unis a établi un processus d'évaluation équitable des vulnérabilités, intitulé Vulnerabilities Equities Process (VEP), qui est « responsable d'établir s'il convient d'informer le fournisseur de la vulnérabilité pour que celui-ci la corrige, ou de limiter le nombre de personnes connaissant la vulnérabilité afin qu'elle puisse être utilisée à des fins de sécurité nationale ou d'application de la loi[103] ». De nombreux organismes du gouvernement fédéral des États-Unis participent à l'évaluation de la question de savoir si une vulnérabilité devrait être gardée secrète et utilisée, ou divulguée aux fournisseurs ou aux développeurs responsables, puis corrigée. Ce système d'évaluation n'est pas exigé aux termes d'une loi. Il est plutôt issu d'efforts de transparence déployés en réponse à des préoccupations quant au fait que la NSA a déjà gardé secrètes de nombreuses

[103] Rob Joyce, *Improving and Making the Vulnerability Equities Process Transparent is the Right Thing to Do*, The White House, 2017, https://www.whitehouse.gov/articles/2017/11/15/improving-and-making-vulnerability-equities-process-transparent-right-thing-do [TRADUCTION].

vulnérabilités par le passé, et que ces vulnérabilités peuvent semer le chaos si des acteurs étrangers y accèdent et les diffusent[104].

Le CST applique actuellement un programme d'évaluation équitable des vulnérabilités, mais les détails sur son fonctionnement demeurent secrets[105]. Il est absolument impossible pour le public de connaître le cadre qui établit qui est responsable d'évaluer si le CST gardera des vulnérabilités secrètes ou les divulguera, les parties qui participent au processus d'évaluation et les types de vulnérabilités ou de failles techniques qui donnent lieu à une évaluation dans le cadre du programme. Par conséquent, il est impossible pour le public ou les acteurs de l'industrie de comprendre la nature des calculs qu'effectue le CST lorsqu'il divulgue une vulnérabilité (ou ne le fait pas), ou de tenir le CST pour responsable dans l'éventualité où les politiques ne servent pas les intérêts publics, car elles limitent inadéquatement la divulgation d'information de façon responsable. Pour que le public continue d'avoir confiance envers le CST et de croire que celui-ci fournit activement des avis, des conseils et des services complets tout en s'acquittant du volet de son mandat touchant la cybersécurité et l'assurance de l'information, le projet de loi C-59 – ou tout autre document de politique clair, public, détaillé et à jour – doit donner des précisions sur ce programme. En outre, le CST devrait être tenu de déclarer régulièrement ses résultats au titre de ce cadre, y compris le taux auquel les vulnérabilités de différentes catégories sont gardées secrètes et divulguées, et ces rapports, dans la mesure du possible, devraient être fournis non seulement à l'OSASNR, mais aussi au grand public.

Recommandation 49

Exiger l'établissement d'un programme d'évaluation équitable des vulnérabilités pour le CST exigeant que les critères d'évaluation de la divulgation soient entièrement publics.

Recommandation 50.

Exiger que les critères du programme d'évaluation équitable des vulnérabilités précisent qu'il faut accorder avant tout la priorité à l'intérêt public et à la sécurité publique, au détriment de l'atteinte des objectifs opérationnels du CST se rapportant à la collecte de renseignements et aux interruptions. Permettre au commissaire au renseignement et à des experts non gouvernementaux indépendants de promouvoir ces préoccupations relatives à l'intérêt public.

Recommandation 51.

Exiger la production de rapports publics sur le programme d'évaluation équitable des vulnérabilités, précisant entre autres la fréquence à laquelle le CST divulgue des vulnérabilités aux équipes d'intervention en cas d'urgence informatique, aux institutions publiques, aux organismes privés et à d'autres entités.

---

[104] Jason Healey, « The U.S. Government and Zero-Day Vulnerabilities », *Journal of International Affairs*, novembre 2016; Brad Smith, *The need for urgent collective action to keep people safe online: Lessons from last week's cyberattack*, Microsoft, 2017, https://blogs.microsoft.com/on-the- issues/2017/05/14/need-urgent-collective-action-keep-people-safe-online-lessons-last-weeks-cyberattack/.

[105] Matt Braga, « When do Canadian spies disclose the software flaws they find? There's a policy, but few details », *CBC News*, 2017, http://www.cbc.ca/news/technology/canada-cse-spies-zero-day-software-vulnerabilities-1.4276007.

v. Ententes avec des entités étrangères et internationales

Pour s'acquitter de son mandat, le CST a déjà conclu différentes « ententes » avec des entités ayant des obligations et des pouvoirs semblables aux siens, y compris avec des entités nationales et des organismes du renseignement étranger. La LCST proposée reconnaît ces ententes, les assujettit à un cadre juridique et précise qu'elles peuvent comprendre la communication de l'information et d'autres formes de coopération (LCST, art. 55). Selon le modèle proposé, les ententes avec des « institutions d'États étrangers ou des organisations internationales d'États ou leurs institutions » doivent être approuvées par le ministre, qui est tenu de consulter le ministre des Affaires étrangères au préalable (LCST, par. 55(2)). Cependant, il n'est pas nécessaire que le ministre des Affaires étrangères donne son consentement aux ententes, et les ententes ne nécessitent aucune forme de surveillance ou d'approbation de la part du commissaire au renseignement.

Il est possible de conclure des ententes en ce qui concerne tous les volets du mandat du CST. Lorsqu'une loi ou une autorisation approuvée par le commissaire au renseignement limite les activités du CST ou l'information qu'il peut recueillir, les ententes avec un organisme étranger peuvent offrir au CST un moyen de contourner ces obstacles. En collaborant avec des parties étrangères, le CST peut être en mesure d'accéder à de l'information ou à des réseaux auxquels il ne pourrait pas avoir accès autrement en raison de l'insuffisance de ses capacités techniques internes. Des ententes pourraient aussi permettre au CST de développer des systèmes interexploitables et interconnectés – comme des réseaux de capteurs – avec des entités étrangères dont des acteurs étrangers pourraient ensuite se servir pour mener des activités violant des normes internationales en matière de droits de la personne ou qui seraient illégales si elles étaient menées par le CST lui-même. Les ententes de communication d'information avec des entités étrangères sont aussi susceptibles de soulever des préoccupations, car elles permettent au CST d'acquérir, de recueillir, d'utiliser ou d'analyser de l'information que le CST n'aurait jamais pu acquérir légalement lui-même, y compris de l'information acquise d'une manière qui poserait des problèmes juridiques en plus de susciter des préoccupations relatives aux droits internationaux de la personne. En outre, bien que le CST puisse utiliser des ententes de communication d'information pour empêcher des partenaires étrangers de communiquer de l'information acquise au cours d'activités de surveillance étrangère visant des Canadiens et des personnes se trouvant au Canada, l'information acquise incidemment qui se rapporte à des Canadiens ou à des personnes se trouvant au Canada demeure probablement un enjeu.

Le CST peut recueillir de l'information accessible au public qui se rapporte à des Canadiens et à des personnes se trouvant au Canada en application de l'alinéa 24(1)a) de la LCST proposée, en plus de mener des activités de collecte massive de données, qui sont également susceptibles de comprendre de l'information sur des Canadiens ou des personnes se trouvant au Canada. La LCST comprend une exigence prévoyant que le CST doit prendre des mesures pour protéger la vie privée des Canadiens ou des personnes se trouvant au Canada lorsque de l'information se rapportant à eux est recueillie dans la réalisation des volets du mandat du CST touchant le renseignement étranger et la cybersécurité ou dont l'information est recueillie en application de l'exception concernant l'« information accessible au public » prévue à l'alinéa 24(1)a). Le cadre régissant les ententes devrait être interprété conjointement avec les dispositions relatives à la communication d'informations, qui se trouvent aux articles 44 à 47, et avec les limites interdisant de mener des activités visant des Canadiens, qui sont énoncées à

l'article 23 de la LCST. Aux termes de l'article 44, le CST peut communiquer aux personnes désignées en vertu de l'article 47 de l'information nominative sur un Canadien qui a été utilisée, analysée ou conservée au titre d'une autorisation de renseignement étranger s'il estime que la communication de cette information est essentielle aux affaires internationales, à la défense, à la sécurité ou à la cybersécurité. Aux termes de l'article 45, le CST peut communiquer de l'information acquise, utilisée ou analysée au cours d'activités menées dans le cadre du volet de son mandat touchant la cybersécurité et l'assurance de l'information, y compris des communications privées interceptées et une mention de l'existence d'une telle communication (par. 45(2)), s'il conclut que la communication est raisonnablement nécessaire pour atteindre les objectifs des volets de son mandat touchant la cybersécurité et l'assurance de l'information. Cependant, au-delà des limites qu'impose cette disposition, il semble que toute information qui relève du CST ou qui est en sa possession peut faire l'objet d'une entente de communication d'informations aux termes de l'article 55. Il convient de souligner que par le passé, les mesures visant à limiter la communication d'information sur des Canadiens à des tiers n'ont pas toujours été efficaces[106].

Recommandation 44.

Modifier l'article 55 de la LCST afin d'exiger au ministre de faire approuver par le commissaire au renseignement toutes les ententes avec des institutions d'États étrangers ou des organisations internationales d'États ou leurs institutions.

Recommandation 45.

Modifier l'article 55 de façon à interdire au CST de conclure sciemment des ententes avec des institutions d'États étrangers ou d'autres entités soupçonnées de commettre des actes de torture.

Recommandation 46.

Modifier l'article 55 de la LCST afin d'exiger au commissaire, lorsqu'il approuve une entente, de veiller à ce que toutes les activités qui seront menées dans la réalisation du mandat du CST aux termes de l'entente (y compris aux fins de communication de l'information ou d'autres formes de coopération) soient légitimes, constitutionnelles, raisonnablement nécessaires et proportionnelles.

Recommandation 47.

Modifier l'article 55 de la LCST pour y ajouter un cadre d'examen et de renouvellement périodique de toutes les ententes conclues par le CST. Lorsqu'il s'agit d'ententes avec des institutions d'États étrangers ou des organisations internationales d'États ou leurs institutions, le processus de renouvellement devrait comprendre le consentement du ministre des Affaires étrangères et l'approbation du commissaire au renseignement.

[106] Bureau du commissaire du Centre de la sécurité des télécommunications, *Rapport annuel 2014-2015*, gouvernement du Canada, 2015, https://www.ocsec-bccst.gc.ca/s21/s20/fra/2014-2015-annual-report; voir aussi Tamir Israel et Christopher Parsons, « Why We Need to Reevaluate How We Share Intelligence Data With Allies », *Just Security*, 2016, https://www.justsecurity.org/29138/reevaluate-share-intelligence-data-allies/.

Section III – Recommandations

Examen, surveillance, contrôle et responsabilité

1. Modifier l'article 9 de la *Loi sur l'Office de surveillance des activités en matière de sécurité nationale et de renseignement* afin de préciser que l'OSASNR a le droit d'avoir accès aux informations qui relèvent de tout ministère ou qui sont en la possession de tout ministère, y compris à des documents en provenance de gouvernements étrangers, de leurs organismes du renseignement respectifs et d'organismes internationaux, malgré toute limite imposée par ces organismes étrangers ou par le « droit de regard de la source ».

2. Modifier l'article 48 de la *Loi sur l'Office de surveillance des activités en matière de sécurité nationale et de renseignement* afin d'interdire au secrétariat d'embaucher directement des membres du personnel d'agences du renseignement de la sécurité nationale, et d'imposer un délai raisonnable entre le moment où ces personnes cessent de travailler au sein d'une de ces agences et leur embauche au secrétariat.

3. Modifier le paragraphe 4(3) de la *Loi sur le commissaire au renseignement* afin d'exiger ou au moins d'offrir la possibilité que le commissaire au renseignement exerce sa charge à temps plein.

4. Modifier le paragraphe 4(4) de la *Loi sur le commissaire au renseignement* afin de prévoir que le traitement du commissaire au renseignement soit fixé en fonction du traitement d'un juge de la Cour fédérale aux termes de l'alinéa 10d) de la *Loi sur les juges* (si le commissaire continue d'exercer sa charge à temps partiel, ce traitement peut être fixé au prorata).

5. Modifier la *Loi sur le commissaire au renseignement* et la LCST pour veiller à ce que le commissaire au renseignement ait la capacité de soumettre les autorisations approuvées à des conditions; ait l'obligation de statuer sur la légalité, la constitutionnalité, la nécessité raisonnable et la proportionnalité de toute activité menée par le CST; et ait le pouvoir de prendre des décrets pour empêcher le CST de mener toute activité qui est illégale, inconstitutionnelle ou disproportionnée ou qui n'est pas raisonnablement nécessaire.

6. Modifier l'alinéa 21a) de la *Loi sur le commissaire au renseignement* afin d'exiger au commissaire de motiver sa décision lorsqu'il approuve l'autorisation, la modification ou la détermination dont il est question dans cette disposition.

7. Modifier la *Loi sur le commissaire au renseignement* afin de conférer au commissaire au renseignement tous les pouvoirs qui sont conférés aux commissaires en vertu de la partie II de la *Loi sur les enquêtes*, comme ceux conférés au commissaire du CST actuel aux termes du paragraphe 273.63(4) de la LDN.

8. Créer un mécanisme permettant de contester des décisions rendues par le commissaire au renseignement ou d'interjeter appel de ces décisions.

9. Exiger que toutes les autorisations de cyberopérations actives et défensives délivrées aux termes des articles 30 et 31 soient à la fois assujetties à l'approbation du commissaire au renseignement et au consentement du ministre des Affaires étrangères.

10. Exiger que les activités menées dans la réalisation du volet du mandat du CST touchant l'assistance technique et opérationnelle soient assujetties à la fois à l'approbation du commissaire au renseignement et à l'autorisation du ministre.

11. Modifier la LCST afin d'exiger que le commissaire au renseignement examine après coup toute autorisation en cas d'urgence délivrée aux termes de l'article 41.

12. Exiger, dans la mesure du possible, la publication à la fois des autorisations délivrées par le ministre et des décisions rendues par le commissaire au renseignement.

13. Créer une certaine forme d'amicus ayant une autorisation de sécurité ou une autre forme d'avis d'opposition dans le processus d'autorisation des activités menées dans la réalisation des volets du mandat touchant le renseignement étranger, la cybersécurité et les cyberopérations.

14. Exiger au CST de prendre l'initiative de fournir à l'OSASNR toute interprétation juridique interne qu'il adopte si celle-ci est nouvelle ou a fait l'objet de changements importants.

Portée du mandat et pouvoirs

15. Redéfinir le « renseignement étranger » afin qu'il englobe l'information et le renseignement sur les moyens, les intentions ou les activités de groupes terroristes étrangers, d'États étrangers et de leurs agents se rapportant aux affaires internationales, à la défense ou à la sécurité, mais limite l'inclusion d'information ou de renseignement sur les moyens, les intentions ou les activités d'étrangers aux situations présentant une menace pour la sécurité du Canada, selon la définition donnée dans la *Loi sur le Service canadien du renseignement de sécurité*.

16. Modifier les paragraphes 23(3) et 23(4) pour veiller à ce que les activités menées dans la réalisation des volets du mandat du CST concernant le renseignement étranger et la cybersécurité ainsi que l'assurance de l'information puissent toucher incidemment un Canadien ou une personne se trouvant au Canada ou s'y rapporter uniquement si elles sont menées conformément à une autorisation prévue aux paragraphes 27(1), 28(1), 28(2) et 41(1).

17. Modifier le seuil obligeant le CST à obtenir une autorisation (« les activités menées par le Centre […] ne doivent pas contrevenir aux autres lois fédérales, à moins d'être menées au titre d'une autorisation ») (LCST, par. 23(3) et 23(4)) afin d'ajouter que le CST ne doit pas contrevenir aux lois provinciales et à la common law.

18. Préciser que dans la réalisation du volet de son mandat touchant le renseignement étranger, il est interdit au CST d'acquérir, d'utiliser et d'analyser de l'information concernant des événements survenus au cours d'un échange entre deux parties ou plus de l'infrastructure mondiale de l'information qui sont, certainement ou probablement, des dispositifs finaux se trouvant au Canada.

19. Modifier le paragraphe 23(2) de la LCST proposée pour empêcher le CST, dans la réalisation du volet de son mandat touchant le renseignement étranger, de mener des activités visant toute partie de l'infrastructure mondiale de l'information se trouvant au Canada.

20. Ajouter dans la LCST les critères qu'applique le ministre pour désigner comme « étant importantes pour le gouvernement fédéral » de l'information électronique, des infrastructures de l'information ou des catégories d'information électronique ou d'infrastructures de l'information aux termes du paragraphe 22(1) de la LCST.

21. Modifier le paragraphe 22(1) de la LCST pour veiller à ce que les critères qui y sont établis garantissent que l'information électronique et les infrastructures de l'information désignées sont uniquement celles d'une « importance essentielle ».

22. Modifier la LCST afin de permettre à toute institution fédérale, au sens de l'article 2, de présenter une demande écrite au ministre afin de cesser de recevoir des conseils en matière de cybersécurité, des services de surveillance et d'autres services fournis par le CST, y compris, mais sans s'y limiter, toute activité du CST qui pourrait autrement être autorisée aux termes de l'article 28.

23. Pour qu'une autorisation soit délivrée aux termes du paragraphe 28(1), exiger que l'institution fédérale en question demande par écrit l'autorisation de mener l'activité, de la même façon que le prévoit le paragraphe 34(3) pour les autorisations délivrées aux termes du paragraphe 28(2).

24. Modifier l'alinéa 24(1)b) pour faire en sorte que les activités autorisées puissent porter uniquement sur les informations électroniques et les infrastructures de l'information décrites à l'alinéa 18a) de la LCST, et être menées uniquement dans la réalisation du volet de son mandat touchant la cybersécurité et l'assurance de l'information.

25. Modifier l'alinéa 24(1)a) afin que le CST, malgré les restrictions prévues aux paragraphes 23(1) et 23(2), puisse uniquement acquérir, utiliser, analyser et conserver de l'information si cette information fait partie d'un ensemble de données que le commissaire au renseignement a approuvé, car il l'a jugé raisonnablement nécessaire à la réalisation des volets du mandat du CST touchant le renseignement étranger ou la cybersécurité et l'assurance de l'information.

26. Modifier l'alinéa 24(1)a) afin qu'il ne s'applique plus à la « divulgation » de l'information accessible au public, ou encore, modifier l'article 25 afin qu'il garantisse que les activités visant des Canadiens qui constitueraient une divulgation de l'information accessible au public peuvent uniquement être menées au titre de l'article 44.

27. Modifier l'alinéa 21(4)c), afin, au moins, d'exiger l'obtention du consentement libre et éclairé de toute personne dont les logiciels, les produits ou les systèmes sont mis à l'essai ou évalués.

28. Modifier l'alinéa 21(4)c) afin, au moins, qu'il puisse être utilisé uniquement à des fins de cybersécurité.

29. Préciser que les données acquises dans la réalisation des volets du mandat du CST touchant le renseignement étranger ainsi que la cybersécurité et l'assurance de l'information ne peuvent être utilisées, analysées ou communiquées au cours d'activités menées dans la réalisation du volet du mandat du CST touchant l'assistance technique et opérationnelle.

30. Empêcher le CST de donner accès à l'information ou aux capacités de ses partenaires internationaux lorsqu'il fournit une assistance technique ou opérationnelle à des organismes nationaux chargés de l'application de la loi et à d'autres organismes — autrement dit, dans la réalisation du volet de son mandat touchant l'assistance, le CST devrait fournir uniquement une expertise « interne ».

31. Modifier l'article 33 de la LCST afin qu'il s'applique à tous les volets du mandat et à toutes les activités du CST (sous réserve de l'exclusion éventuelle d'activités menées dans le cadre du volet du mandat touchant l'assistance).

32. Ajouter les alinéas suivants au paragraphe 33(1) de la LCST :

    [...]

    c) porter atteinte à l'intégrité sexuelle d'un individu;

    d) soumettre un individu à la torture ou à d'autres peines ou traitements cruels, inhumains ou dégradants, au sens de la Convention contre la torture;

    e) détenir un individu;

    f) causer la perte de biens ou des dommages importants à ceux-ci si cela porterait atteinte à la sécurité d'un individu;

    g) mener des activités qui sont susceptibles de compromettre l'intégrité de technologies de communications, de réseaux et de services utilisés par le grand public, y compris en affaiblissant ou en entravant les normes et les protocoles de sécurité.

33. Modifier l'alinéa 33(1)b) de la façon suivante : « [...] tenter intentionnellement de quelque manière d'entraver, de détourner ou de contrecarrer le cours de la justice ou de la démocratie, notamment en tentant intentionnellement d'entraver, de détourner ou de contrecarrer le cours de toute procédure judiciaire ou de tout processus électoral, directement ou indirectement. »

34. Modifier la LCST afin qu'il soit possible de délivrer des autorisations en cas d'urgence uniquement lorsqu'il s'agit réellement d'une situation d'urgence.

35. Exiger au Parlement de mener une étude sur les avantages, les enjeux et la faisabilité de scinder le CST en deux organismes distincts; l'un serait exclusivement responsable de la cybersécurité, de l'assurance de l'information et de la défense, et l'autre serait exclusivement responsable des activités se rapportant au renseignement étranger et aux cyberopérations.

36. Exiger au Parlement de mener une étude portant, d'une part, sur la division du travail et la répartition des rôles entre le CST et les Forces canadiennes en ce qui a trait aux

cyberopérations, et d'autre part, sur la division du travail et la répartition des rôles entre le CST et le SCRS en ce qui a trait aux activités se rapportant au renseignement étranger.

Problèmes concernant des termes définis (et non définis)

37. Modifier la LCST afin de préciser que les termes « intercepter », « analyse », « interception » et « acquisition » ont le même sens que dans la partie VI du *Code criminel*.

38. Définir les termes « acquérir », « utiliser », « analyser » et « recueillir » dans la LCST afin, d'une part, d'énoncer explicitement en quoi consiste une « acquisition » et une « collecte », et d'autre part, d'établir clairement la distinction entre l'analyse et l'utilisation d'information déjà recueillie et l'analyse et l'utilisation d'information que le CST n'a pas encore recueillie.

39. Supprimer l'alinéa 61c) de la LCST.

40. Redéfinir l'expression « information accessible au public » dans la LCST pour qu'elle s'applique uniquement aux messages diffusés et aux publications accessibles sur le marché.

41. Modifier l'article 44 afin d'éliminer le terme « cybersécurité », qui n'est pas défini dans la LCST et qui n'est pas mentionné autrement en ce qui a trait aux activités du CST touchant le renseignement étranger.

42. Veiller à ce que toutes les mesures prévues à l'article 25 et adoptées par règlement en application de l'alinéa 61b) dans l'objectif de protéger la vie privée des Canadiens et des personnes se trouvant au Canada soient accessibles au public afin que celui-ci puisse les analyser et formuler des commentaires à leur sujet.

43. Exiger au Commissariat à la protection de la vie privée du Canada d'évaluer annuellement les protections offertes aux Canadiens et aux personnes se trouvant au Canada en application de l'article 25, et veiller à ce qu'il soit en mesure de formuler des recommandations au CST et au commissaire au renseignement.

Ententes

44. Modifier l'article 55 de la LCST afin d'exiger au ministre de faire approuver par le commissaire au renseignement toutes les ententes avec des institutions d'États étrangers ou des organisations internationales d'États ou leurs institutions.

45. Modifier l'article 55 de façon à interdire au CST de conclure sciemment des ententes avec des institutions d'États étrangers ou d'autres entités soupçonnées de commettre des actes de torture.

46. Modifier l'article 55 de la LCST afin d'exiger au commissaire, lorsqu'il approuve une entente, de veiller à ce que toutes les activités qui seront menées dans la réalisation du mandat du CST aux termes de l'entente (y compris aux fins de communication de l'information ou d'autres formes de coopération) soient légitimes, constitutionnelles, raisonnablement nécessaires et proportionnelles.

47. Modifier l'article 55 de la LCST pour y ajouter un cadre d'examen et de renouvellement périodique de toutes les ententes conclues par le CST. Lorsqu'il s'agit d'ententes avec des institutions d'États étrangers ou des organisations internationales d'États ou leurs institutions, le processus de renouvellement devrait comprendre le consentement du ministre des Affaires étrangères et l'approbation du commissaire au renseignement.

Production de rapports et mesures favorisant la transparence

48. Exiger au gouvernement du Canada de déclarer dans un rapport annuel rendu public les priorités en matière de renseignement étranger et de cybersécurité qu'il fixe pour le CST.

49. Exiger l'établissement d'un programme d'évaluation équitable des vulnérabilités pour le CST exigeant que les critères d'évaluation de la divulgation soient entièrement publics.

50. Exiger que les critères du programme d'évaluation équitable des vulnérabilités précisent qu'il faut accorder avant tout la priorité à l'intérêt public et à la sécurité publique, au détriment de l'atteinte des objectifs opérationnels du CST se rapportant à la collecte de renseignements et aux interruptions. Permettre au commissaire au renseignement et à des experts non gouvernementaux indépendants de promouvoir ces préoccupations relatives à l'intérêt public.

51. Exiger la production de rapports publics sur le programme d'évaluation équitable des vulnérabilités, précisant entre autres la fréquence à laquelle le CST divulgue des vulnérabilités aux équipes d'intervention en cas d'urgence informatique, aux institutions publiques, aux organismes privés et à d'autres entités.

52. Exiger la publication de la fréquence à laquelle le CST fournit une assistance technique et opérationnelle à d'autres entités ainsi que la publication du nom des organismes ayant obtenu cette assistance, dans les documents d'examen annuels du CST.

53. Exiger à l'OSASNR d'examiner régulièrement la structure et l'information que fournit le CST dans son rapport annuel et donner à l'OSASNR l'autorisation de recommander que le CST ajoute des renseignements précis dans ses prochains rapports, y compris des données statistiques sur la nature et la portée de ses activités.

54. Exiger la publication de rapports sur la fréquence des cyberopérations défensives et actives.