Gouvernement du Canada | Government of Canada

Attitudes envers le Centre de la sécurité des télécommunications – Étude de suivi

Rapport final

Préparé pour le Centre de la sécurité des télécommunications

Nom du fournisseur : Phoenix SPI
Numéro du contrat : 2L165-200494-001-CY
Valeur du contrat : 84 978,57 $
Date d'attribution du contrat : 9 janvier 2020
Date de présentation du rapport : 30 avril 2020

Numéro d'enregistrement : 063-19
Pour obtenir de plus amples renseignements au sujet du présent rapport, veuillez communiquer avec le CST à l'adresse media@cse-cst.gc.ca

This report is also available in English.

Canada

Attitudes envers le Centre de la sécurité des télécommunications – Étude de suivi
Rapport final

Préparé pour le Centre de la sécurité des télécommunications
Nom du fournisseur : Phoenix Strategic Perspectives Inc.
Avril 2020

Ce rapport de recherche sur l'opinion publique présente les résultats d'un sondage téléphonique mené par Phoenix SPI pour le compte du Centre de la sécurité des télécommunications (CST) et administré à 2 505 Canadiens de 18 ans et plus entre le 11 février et le 7 mars 2020.

Cette publication est aussi offerte en anglais sous le titre : *Attitudes towards the Communications Security Establishment – Tracking Study*.

Numéro de catalogue :
D96-16/2020F-PDF

Numéro international normalisé du livre (ISBN) :
978-0-660-34496-6

Publications connexes (numéro d'enregistrement : POR 063-19) :

Numéro de catalogue (version anglaise du rapport final) D96-16/2020E-PDF
ISBN 978-0-660-34497-3

Table des matières

Liste des diagrammes

Sommaire

Le Centre de la sécurité des télécommunications (CST) a chargé Phoenix Strategic Perspectives (Phoenix SPI) de mener une enquête téléphonique nationale afin d'orienter les stratégies de communication de l'organisme.

1. But et objectifs de la recherche

L'un des objectifs organisationnels du CST consiste à améliorer le niveau de confiance de la population et des intervenants grâce à l'atteinte de résultats utiles et au respect constant de la loi et de la protection des renseignements personnels. Le CST a effectué une recherche sur l'opinion publique en 2017 afin d'appuyer cet objectif. Les résultats obtenus en 2017 servent de données de référence qui permettent de mesurer les changements au fil du temps. Les objectifs spécifiques de la présente recherche étaient les suivants : 1) suivre l'évolution des opinions concernant les organismes de renseignement au Canada et le CST; et 2) mieux comprendre les connaissances et les points de vue au sujet du Centre canadien pour la cybersécurité, mis sur pied en octobre 2018 afin de réunir dans un seul centre les principales unités opérationnelles de cybersécurité au sein du gouvernement du Canada. Les constats de cette recherche aideront le CST à susciter et à maintenir la confiance du public tout en aidant façonner de nouvelles stratégies de communication.

2. Méthodologie

Un sondage téléphonique à composition aléatoire, qui durait 12 minutes, a été administré à 2 505 Canadiens de 18 ans et plus entre le 11 février et le 7 mars 2020. Le sondage a été mené au moyen de la technologie de l'interview téléphonique assistée par ordinateur (ITAO). La méthode d'échantillonnage aléatoire fut utilisée afin d'extrapoler les résultats à l'ensemble de la population de Canadiens de 18 ans et plus. Une base d'échantillonnage double avec chevauchement (utilisateurs de téléphone fixe et de cellulaire) a été utilisée pour réduire au minimum les erreurs de couverture. L'échantillon était disproportionné sur le plan géographique afin d'améliorer l'exactitude des résultats régionaux. Les données ont été pondérées afin de s'assurer qu'elles reflètent correctement la répartition de la population d'adultes canadiens en ce qui a trait à l'âge, au sexe et à la province ou au territoire. Les données du Recensement de 2016 de Statistique Canada ont été utilisées à cette fin. Avec un échantillon de cette taille, les constats généraux sont jugés exacts avec une marge d'erreur de plus ou moins 2,2 %, 19 fois sur 20 (rajustée pour refléter l'échantillon disproportionné sur le plan géographique).

3. Principaux constats

Connaissance du CST

Le niveau de connaissance du CST n'est pas élevé et on note une proportion moins élevée qu'en 2017 pour ce qui est de la connaissance assistée.

Très peu de Canadiens connaissent, sans qu'on leur donne de plus amples renseignements, l'organisme gouvernemental chargé d'intercepter et d'analyser les communications étrangères et de contribuer à la protection des réseaux informatiques du gouvernement. Deux pour cent des répondants ont identifié correctement le CST et un pour cent de plus des participants ont fait mention du CST et du Centre pour la cybersécurité. En revanche, près d'un tiers des répondants ont dit, après avoir reçu certaines informations, qu'ils connaissaient le CST (20 % ont indiqué qu'ils avaient *assurément* entendu, vu ou lu quelque chose à ce sujet et 11 % ont dit que c'était *peut-être* le cas). Le niveau de connaissance spontanée du CST demeure inchangé par rapport à 2017, alors que le niveau de connaissance assistée est plus faible qu'en 2017 (31 % comparativement à 37 % en 2017).

Perceptions concernant la mission et les activités du CST

La majorité des Canadiens accordent de l'importance à la mission du CST et estiment que les activités liées à la sécurité nationale menées par le CST sont très importantes, mais plusieurs ne sont pas au courant des activités particulières réalisées par le CST pour appuyer la sécurité nationale.

Plus des trois quarts des répondants trouvent que le CST joue un rôle important pour ce qui est de la sécurité nationale du Canada (51 % ont dit que c'était *très* important et 27 % ont dit que c'était *plutôt* important). Ces résultats sont légèrement différents de ceux obtenus en 2017, c'est-à-dire qu'une plus petite proportion de répondants attribue une importance modérée à la mission du CST.

La grande majorité des répondants accordent de l'importance à chacune des cinq activités du CST ayant trait à la sécurité nationale; au moins la moitié d'entre eux trouvent que ces activités sont *très* importantes. Au premier rang figure la protection des réseaux informatiques du Canada (97 % estiment que c'est important et 82 % sont d'avis que c'est *très* important). Un nombre presque aussi élevé de participants jugent important de défendre activement les réseaux au Canada (94 %) et de neutraliser les cybermenaces étrangères (93 %), alors que les trois quarts accordent une grande importance à chacune de ces activités. Finalement, 89 % des participants trouvent important d'aider les organismes d'application de la loi et de sécurité et 88 % partagent le même avis pour ce qui est de la collecte de renseignements étrangers (plus de la moitié des répondants estiment que chaque activité est très importante).

Pour ce qui est de la connaissance des activités du CST, près d'un quart des répondants ont dit qu'ils sont conscients que le CST appuie les missions des Forces armées canadiennes (24 %) et que le CST peut aider les principaux organismes chargés de la sécurité nationale (23 %). Quatorze pour cent des participants confirment savoir que la loi interdit au CST de cibler des Canadiens ou quiconque au Canada, alors que seulement 8 % ont dit être au courant que le CST bloque chaque jour plus de deux milliards de cyberactivités malveillantes.

Confiance envers le CST

On note une diminution, depuis 2017, du niveau de confiance envers le CST pour qu'il agisse de façon éthique et légale en remplissant son mandat.

Près des deux tiers des Canadiens se fient « quelque peu » (49 %) ou « totalement » (15 %) au CST pour qu'il agisse de façon éthique et légale. Le niveau de confiance envers le CST à cet égard a diminué au fil du temps (64 % comparativement à 73 % en 2017) alors que le niveau de méfiance est demeuré inchangé. La proportion de répondants qui disent ne pas avoir d'opinion a augmenté (24 % comparativement à 15 % en 2017).

Opinions concernant la sécurité nationale

La proportion de Canadiens qui croient que le Canada est plus dangereux maintenant qu'il y a cinq ans a augmenté depuis 2017.

Lorsqu'on a demandé aux participants s'ils avaient l'impression que le Canada est plus sûr, plus dangereux ou à peu de chose près le même qu'il y a cinq ans, environ un répondant sur 10 (11 %) a indiqué que le Canada est plus sûr et un tiers des participants (33 %) trouvent que le Canada est plus dangereux. Les autres (51 %) sont d'avis que, dans l'ensemble, le Canada est à peu de chose près le même qu'il y a cinq ans. La proportion de répondants qui jugent que le Canada est plus sûr a diminué légèrement au fil du temps (11 % comparativement à 15 % en 2017), alors que la proportion de participants qui estiment qu'il est plus dangereux a augmenté (33 % comparativement à 25 % en 2017).

Équilibre entre la sécurité et les libertés civiles

Sept Canadiens sur 10 sont d'accord que si des mesures ne sont pas prises pour protéger les ordinateurs et Internet, le Canada va encourir plus de risques de subir des attaques terroristes.

En utilisant une échelle de sept points, les répondants ont exprimé dans quelle mesure ils étaient d'accord ou en désaccord avec un ensemble d'énoncés concernant l'équilibre entre la sécurité et les libertés civiles. Le seul énoncé avec lequel la majorité des participants est au moins quelque peu d'accord est le suivant : « Si nous ne prenons pas de mesures pour assurer la sécurité de nos ordinateurs et d'Internet, nous encourrons plus de risques de faire l'objet d'une attaque terroriste ». Soixante-douze pour cent des répondants sont d'avis que le Canada sera plus à risque de subir des attaques terroristes si des mesures ne sont pas prises.

Près de la moitié des répondants se montrent d'accord dans une certaine mesure avec les énoncés suivants : « Les services de renseignement canadiens respectent la loi lorsqu'ils recueillent de l'information sur les Canadiens » (49 %) et « Je peux me fier au gouvernement du Canada pour trouver le juste équilibre entre la sécurité et les libertés civiles » (49 %), alors qu'une proportion légèrement moins élevée de participants (45 %) est d'accord avec l'énoncé « L'information que les services de renseignement du gouvernement peuvent recueillir à mon égard me préoccupe ».

Les répondants sont moins susceptibles d'être d'accord avec l'énoncé « Les services de police et de renseignement devraient avoir plus de pouvoirs pour assurer la sécurité, même si cela signifie que les Canadiens doivent renoncer à certaines mesures de protection de leur vie privée ». Quatre répondants sur 10 (41 %) sont d'accord avec le compromis, c'est-à-dire, ils renonceraient à certaines mesures de protection de leur vie privée pour assurer la sécurité, alors que plus du tiers des participants (36 %) ont manifesté leur désaccord, dont 18 % qui se disaient *fortement* en désaccord.

Comparativement à 2017, la diminution de la proportion de participants qui sont d'accord avec l'énoncé « Je peux me fier au gouvernement du Canada pour trouver le juste équilibre entre la sécurité et les libertés civiles » (49 % comparativement à 55 % en 2017) représente la différence la plus évidente.

Connaissance et perceptions du Centre pour la cybersécurité

On note une connaissance limitée du Centre pour la cybersécurité, mais la majorité des répondants croient que les activités du Centre ont au moins un effet modéré sur le Canada.

Plus de neuf répondants sur 10 (94 %) ne pouvaient pas identifier l'organisme qui fait partie du CST et dont la principale responsabilité est de fournir des conseils, des avis, des services et du soutien en matière de cybersécurité. Seulement 2 % ont bien nommé le Centre canadien pour la cybersécurité alias le Centre pour la cybersécurité. Lorsqu'on leur donnait un peu plus d'information, les répondants avaient une meilleure connaissance du Centre pour la cybersécurité. Quand on leur a demandé s'ils avaient entendu, vu ou lu quoi que ce soit au sujet du Centre canadien pour la cybersécurité ou du Centre pour la cybersécurité, 16 % ont dit qu'ils avaient *peut-être* ou *assurément* entendu, vu ou lu quelque chose à ce sujet. La grande majorité des participants (83 %) ont répondu par la négative.

Les répondants ont utilisé une échelle de sept points pour se prononcer sur l'effet qu'ont, à leur avis, les diverses activités du Centre pour la cybersécurité sur le Canada. Les activités suivantes semblent avoir le plus grand effet (cotes de 5 ou plus) : défendre les systèmes informatiques du Canada (76 %), protéger la cybersécurité en travaillant avec des partenaires (73 %), développer et mettre en commun des technologies et des outils pour la cyberdéfense (69 %) et renseigner le Canada et les Canadiens sur les questions de cybersécurité et offrir du leadership lors d'incidents liés à la cybersécurité (68 % chacun).

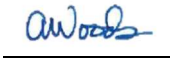
État de préparation en vue d'une cyberattaque

Les experts en la matière et les Canadiennes et les Canadiens sont plus susceptibles d'être perçus comme étant mal préparés en vue d'une cyberattaque.

Finalement, on a demandé aux répondants dans quelle mesure les divers intervenants ou institutions sont préparés, selon eux, à réagir en cas de cyberattaque. La majorité des répondants estiment que la plupart de ces entités sont préparées à lutter contre une cyberattaque, mais la taille de la majorité varie et les répondants sont beaucoup plus susceptibles de les considérer comme étant « quelque peu » préparés plutôt que « très bien » préparés. Un plus grand nombre de répondants sont d'avis que le gouvernement canadien est au moins quelque peu préparé (69 %). Suivent ensuite les grandes entreprises (65 %), les exploitants d'infrastructures essentielles (61 %) et les systèmes électoraux dans l'ensemble du Canada (56 %). À titre de comparaison, près des deux tiers des participants estiment que les petites et moyennes entreprises sont mal (36 %) ou très mal (27 %) préparées à cet égard, alors qu'un peu plus des trois quarts des participants sont d'avis que les Canadiennes et les Canadiens sont mal (33 %) ou très mal (43 %) préparés en vue d'une cyberattaque.

4. Certification de neutralité politique

En ma qualité de cadre supérieure de Phoenix Strategic Perspectives, je certifie par la présente que les produits livrés sont en tout point conformes aux exigences du gouvernement du Canada en matière de neutralité politique qui sont décrites dans la Politique de communication et l'image de marque du gouvernement du Canada et dans la Procédure de planification et d'attribution de marchés de services de recherche sur l'opinion publique. Plus particulièrement, les livrables ne comprennent pas de renseignements sur les intentions de vote aux élections, les préférences de partis politiques, les positions vis-à-vis de l'électorat ou l'évaluation de la performance d'un parti politique ou de son dirigeant.



Alethea Woods
Présidente
Phoenix SPI

5. Valeur du contrat

La valeur du contrat s'élevait à 84 978,57 $ (y compris la TVH).

Introduction

Le cabinet Phoenix Strategic Perspectives (Phoenix SPI) est ravi de présenter au Centre de la sécurité des télécommunications (CST) un rapport qui contient les résultats d'une recherche sur l'opinion publique de nature quantitative et d'envergure nationale réalisée pour orienter les stratégies de communication de l'organisme.

1. Contexte et objectifs

Le CST est l'organisme national de cryptologie du Canada. Unique au sein de la collectivité canadienne de la sécurité et du renseignement, le CST compte dans ses rangs des concepteurs et des perceurs de code qui lui permettent d'offrir au gouvernement du Canada des services de sécurité des technologies de l'information (sécurité des TI) et de renseignement étranger (SIGINT). Le CST fournit également une assistance technique et opérationnelle aux organismes fédéraux chargés de l'application de la loi et de la sécurité.

Le mandat et les pouvoirs du CST sont définis dans la *Loi sur le Centre de la sécurité des télécommunications* (partie 3 du projet de loi C-59, *Loi concernant des questions de sécurité nationale*) qui autorise le CST à faire ce qui suit :

1. Acquérir, 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 utiliser, analyser et diffuser l'information dans le but de fournir des renseignements étrangers, en conformité avec les priorités du gouvernement fédéral en matière de renseignement.
2. Fournir des avis, des conseils et des services pour aider à protéger les renseignements électroniques et les infrastructures de l'information pour le gouvernement du Canada, ainsi que des renseignements électroniques et des infrastructures de l'information désignés comme étant importantes pour le gouvernement du Canada en vertu du paragraphe 21(1); et acquérir, utiliser et analyser de l'information provenant de l'infrastructure mondiale de l'information ou d'autres sources afin de fournir de tels avis, conseils et services.
3. Mener 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 du Canada désignées comme telle en vertu du paragraphe 21(1).
4. Mener 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.
5. Fournir 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.

L'un des objectifs organisationnels du CST consiste à améliorer le niveau de confiance de la population et des intervenants grâce à l'atteinte de résultats utiles et au respect constant de la loi et de la protection des renseignements personnels. Afin d'appuyer cet objectif, le CST a effectué, en 2017, une recherche sur l'opinion publique. Les résultats obtenus en 2017 servent de données de référence qui permettent de mesurer les changements au fil du temps. Les objectifs spécifiques de la présente recherche étaient les suivants : 1) suivre l'évolution des opinions concernant les organismes de renseignement au Canada et le CST ; et 2) mieux comprendre les connaissances et les points de vue au sujet du Centre canadien pour la cybersécurité, mis sur pied en octobre 2018 afin de réunir dans un seul centre les principales unités opérationnelles de cybersécurité au sein du gouvernement du Canada. Les constats de cette recherche aideront le CST à susciter et à maintenir chez la population une certaine confiance, en plus de servir à façonner les stratégies de communication.

2. Méthodologie

Un sondage téléphonique à composition aléatoire, qui durait 12 minutes, a été administré à 2 505 Canadiens de 18 ans et plus entre le 11 février et le 7 mars 2020. Le sondage a été mené au moyen de la technologie de l'interview téléphonique assistée par ordinateur (ITAO). Une base d'échantillonnage double avec chevauchement (utilisateurs de téléphone fixe et de cellulaire) a été utilisée pour réduire au minimum les erreurs de couverture. L'échantillon était disproportionné sur le plan géographique afin d'améliorer l'exactitude des résultats régionaux. Avec un échantillon de cette taille, les constats généraux sont jugés exacts avec une marge d'erreur de plus ou moins 2,2 %, 19 fois sur 20 (rajustée pour refléter l'échantillon disproportionné sur le plan géographique). La marge d'erreur est plus grande pour les résultats ayant trait aux sous-groupes de l'échantillon total. L'annexe Caractéristiques techniques de la recherche du présent rapport renferme de plus amples renseignements au sujet de la méthodologie.

3. Notes au lecteur

- Tous les résultats du rapport sont exprimés en pourcentages, sauf indication contraire.
- Les pourcentages peuvent ne pas toujours totaliser 100 % en raison de l'arrondissement.
- Les différences sur le plan démographique sont mentionnées dans le rapport. Lorsqu'on fait état des écarts entre les sous-groupes, seules les différences significatives à un niveau de confiance de 95 % et qui ont trait à un échantillon de plus de 30 répondants (n=30) sont indiquées.
- Les données tabulées sont disponibles sous pli séparé.

Constats détaillés

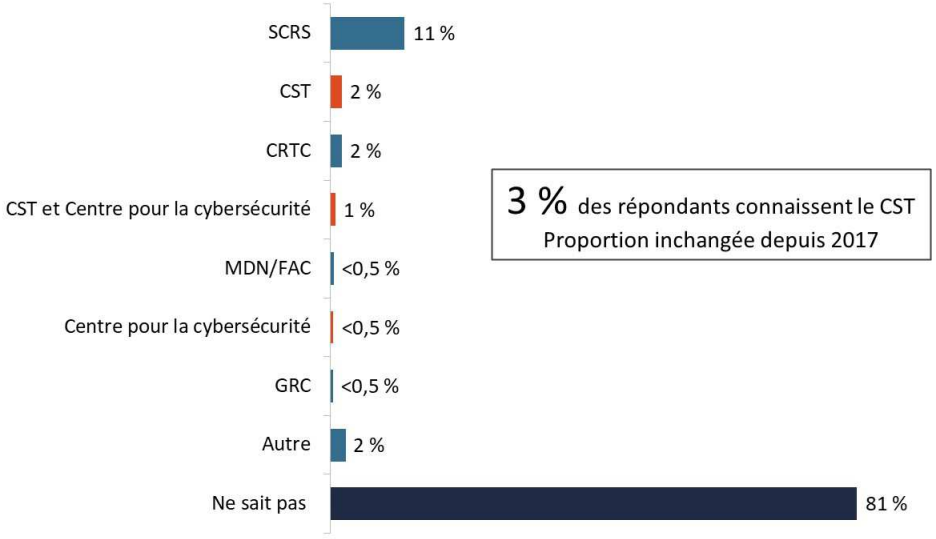
1. Connaissance du CST

Faible niveau de connaissance spontanée du CST

Lorsqu'on leur a demandé s'ils connaissaient un organisme gouvernemental chargé d'intercepter et d'analyser les communications étrangères et qui contribue à la protection des réseaux informatiques du gouvernement, une grande majorité (81 %) de Canadiens ont indiqué qu'ils ne pouvaient pas identifier un tel organisme. Comme le montre le graphique ci-dessous, le seul organisme mentionné à une certaine fréquence est le Service canadien de renseignement sur la sécurité (SCRS) (11 %). Seulement 3 % ont fait mention du CST (2 % ont nommé le CST et 1 %, le CST et le Centre pour la cybersécurité).

Les résultats sont les mêmes qu'en 2017.

Diagramme 1 : Connaissance spontanée du CST



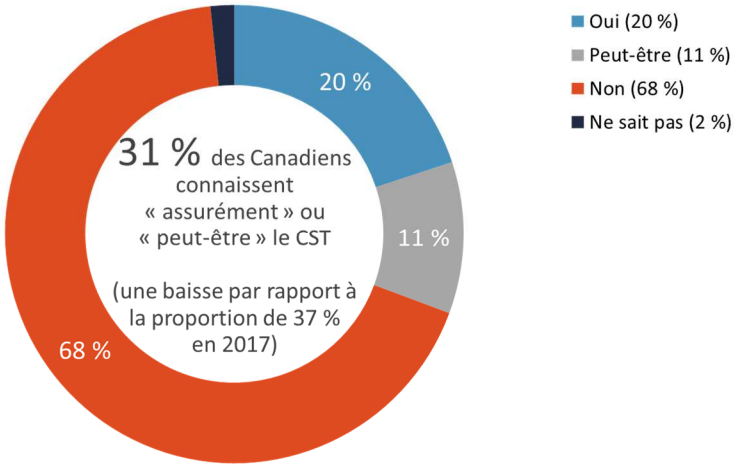
Base de référence : n=2 505; tous les répondants
Q1. Comme vous le savez peut-être déjà, il y a un organisme gouvernemental qui est chargé d'intercepter et d'analyser des communications étrangères et de contribuer à la protection des réseaux informatiques du gouvernement. Pouvez-vous nommer cet organisme?

Près de trois personnes sur dix connaissent le CST.

Après leur avoir dit que le Centre de la sécurité des télécommunications est l'organisme gouvernemental chargé d'intercepter et d'analyser les communications étrangères et de contribuer à la protection des réseaux informatiques du gouvernement, on a demandé aux répondants s'ils avaient entendu, vu ou lu quoi que ce soit au sujet du CST. Un peu plus des deux tiers (68 %) des Canadiens ont répondu par la négative. Une personne sur cinq (20 %) a indiqué qu'elle avait *assurément* entendu, vu ou lu quelque chose concernant le CST, alors qu'un répondant sur 10 (11 %) a mentionné que c'était *peut-être* le cas.

Le pourcentage relatif à la connaissance assistée a diminué au fil du temps (31 % comparativement à 37 % en 2017).

Diagramme 2 : Connaissance assistée du CST



Base de référence : n=2 505; tous les répondants
Q4. Diriez-vous que vous avez déjà lu, vu ou entendu quoi que ce soit sur le Centre de la sécurité des télécommunications du Canada (CST)?

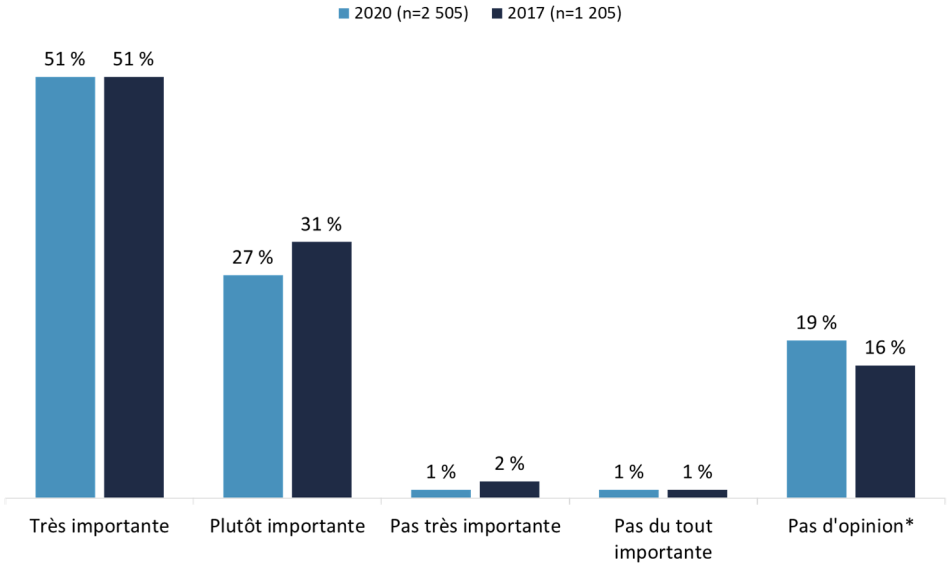
Une connaissance certaine du CST, *lorsqu'on donnait de plus amples renseignements aux participants (connaissance assistée),* est plus élevée chez les hommes (23 % comparativement à 17 % des femmes) et chez les personnes ayant un niveau de scolarité plus élevé (24 % des titulaires d'un diplôme universitaire comparativement à 14 % des personnes ayant au plus un diplôme d'études secondaires). La connaissance certaine *de manière assistée* augmente également avec l'âge (de 16 % des participants âgés entre 18 et 34 ans à 23 % des personnes de 55 ans et plus). Au niveau régional, on note un sommet de 25 % en Colombie-Britannique et un seuil de 15 % au Québec.

2. Perceptions concernant la mission et les activités du CST

La moitié des répondants estiment que la mission du CST est très importante pour la sécurité nationale.

Plus des trois quarts des Canadiens estiment que le CST joue un rôle important pour assurer la sécurité nationale du Canada : 51 % jugent sa mission très importante à cet égard et 27 % sont d'avis qu'elle est plutôt importante. Ces résultats sont légèrement différents de ceux obtenus en 2017, étant donné la proportion moins élevée de répondants qui accordent une importance modérée à la mission du CST.

Diagramme 3 : Importance de la mission du CST pour la sécurité nationale



Q5. Selon cette description et les connaissances que vous possédez peut-être déjà sur le Centre de la sécurité des télécommunications du Canada (ou CST), diriez-vous que sa mission est très importante, plutôt importante, pas très importante ou pas du tout importante pour la sécurité nationale du Canada? *Comprend les réponses « Ne sait pas ».

Les Canadiens plus âgés sont plus susceptibles que les plus jeunes d'attribuer de l'importance à la mission du CST (81 % des personnes de 55 ans et plus comparativement à 74 % des répondants de 18 à 34 ans). On note la même tendance chez les titulaires d'un diplôme universitaire (83 % comparativement à 78 % des personnes ayant une formation collégiale ou professionnelle et à 73 % des personnes ayant au plus un diplôme d'études secondaires).

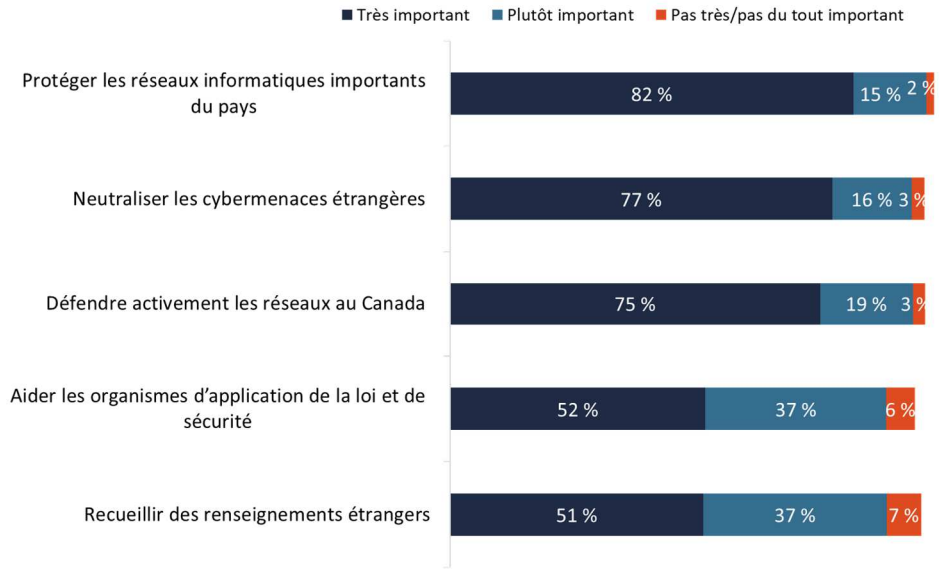
Pratiquement tout le monde juge important de protéger les réseaux informatiques du Canada, mais la neutralisation des cybermenaces est considérée comme l'activité la plus importante.

On a demandé aux répondants d'évaluer l'importance des activités suivantes du CST en ce qui a trait à la sécurité nationale :

- Recueillir des renseignements étrangers, ce qui comprend l'interception et l'analyse de communications étrangères.
- Protéger les réseaux informatiques importants du pays contre les cyberattaques.
- Aider les organismes d'application de la loi et de sécurité en participant à la collecte et à l'analyse de communications.
- Défendre activement les réseaux au Canada contre les cybermenaces étrangères.
- Neutraliser les cybermenaces étrangères avant qu'elles nuisent au Canada ou aux Canadiens.

La grande majorité des Canadiens accordent de l'importance à chacune de ces activités, et la moitié ou plus estiment que ces activités sont *très* importantes. Au premier rang figure la protection des réseaux informatiques du Canada ; pratiquement tous les répondants (97 %) y accordent de l'importance, et 82 % jugent que c'est *très* important. Un nombre presque tout aussi élevé de participants attribuent de l'importance à la défense active des réseaux au Canada (94 %) et à la neutralisation des cybermenaces étrangères (93 %); trois quarts des personnes trouvent que ces activités sont très importantes. Finalement, 89 % des répondants accordent de l'importance à l'aide aux organismes d'application de la loi et de sécurité et 88 %, à la collecte de renseignements étrangers (plus de la moitié estiment que chacune de ces activités est très importante).

Diagramme 4 : Importance des activités du CST pour la sécurité nationale



Base de référence : n=2 505; tous les répondants
Q6. Je vais vous lire une liste des principales choses que fait le Centre de la sécurité des télécommunications du Canada (ou CST). Pour chacune d'elles, j'aimerais que vous me disiez si vous trouvez que c'est quelque chose de très important, plutôt important, pas très important ou pas important du tout pour la sécurité nationale du Canada?

Pour ce qui est de la perception de l'importance de ces activités, les écarts entre les sous-groupes sont limités et comprennent ce qui suit :

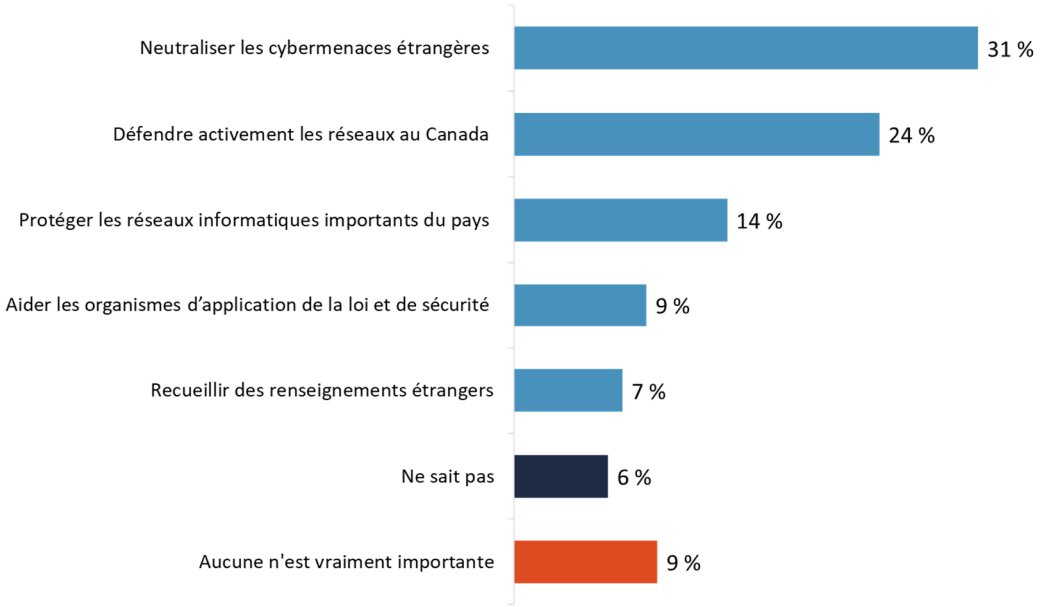
- Les Canadiens de plus de 35 ans (95 % comparativement à 91 % des personnes âgées entre 18 et 35 ans) sont plus susceptibles d'être d'avis que la neutralisation des cybermenaces étrangères est plutôt ou très importante.

- Les Canadiens plus âgés ont plus tendance que les plus jeunes (90 % des personnes de 55 ans et plus comparativement à 85 % des répondants âgés entre 18 et 34 ans) à trouver que la collecte de renseignements étrangers est plutôt ou très importante. Cette activité est également jugée plus importante par les personnes ayant un niveau de scolarité plus élevé (85 % des personnes ayant au plus un diplôme d'études secondaires comparativement à 91 % des titulaires d'un diplôme universitaire).

Plus de huit Canadiens sur 10 (85 %) sont d'avis qu'au moins l'une des activités du CST est importante pour la sécurité nationale du Canada. Afin de comprendre l'importance relative de ces activités, on a demandé aux répondants de choisir l'activité qui est, selon eux, la plus importante parmi les activités qu'ils considéraient comme étant *très* importantes. Trois répondants sur 10 (31 %) ont fait mention de la neutralisation des cybermenaces étrangères, alors que près d'un quart (24 %) des participants estiment

que la protection des réseaux informatiques du Canada est l'activité la plus importante. Par la suite, en ordre décroissant, figurent la défense des réseaux au Canada (14 %), l'aide aux organismes d'application de la loi et de sécurité (9 %) et la collecte de renseignements étrangers (7 %).

Diagramme 5 : L'activité du CST la plus importante pour la sécurité nationale



Base de référence : n=2 505; tous les répondants
Q7. Laquelle des activités suivantes est la plus importante pour ce qui est de la sécurité nationale du Canada?

Les écarts suivants entre les sous-groupes ont pu être constatés :

- Les Canadiens plus jeunes (37 % des personnes de 18 à 34 ans comparativement à 26 % des répondants de 35 à 54 ans) ont plus tendance à trouver très importante la neutralisation des cybermenaces étrangères.

- Les résidents du Québec (31 % comparativement à une proportion totalisant entre 19 % et 24 % des Canadiens résidant ailleurs au pays) et les titulaires d'un diplôme universitaire (27 % comparativement à 21 % des personnes ayant au plus un diplôme d'études secondaires) sont plus susceptibles d'être d'avis que la protection des réseaux informatiques est l'activité la plus importante.

- Les personnes âgées entre 35 et 54 ans (17 % comparativement à 12 % des répondants ayant entre 18 et 34 ans et à 13 % des personnes de 55 ans et plus) et les résidents de l'Alberta (18 %) et de l'Ontario (17 % comparativement à 11 % des habitants du Québec et de la Colombie-Britannique) sont plus nombreux à attribuer la plus grande importance à la défense active des réseaux au Canada contre les cybermenaces étrangères.

- Les Canadiens plus âgés (9 % des répondants de 55 ans et plus comparativement à 5 % des personnes âgées entre 18 et 34 ans) ont plus tendance à estimer que la collecte de renseignements étrangers est l'activité la plus importante.

Faible connaissance du mandat du CST

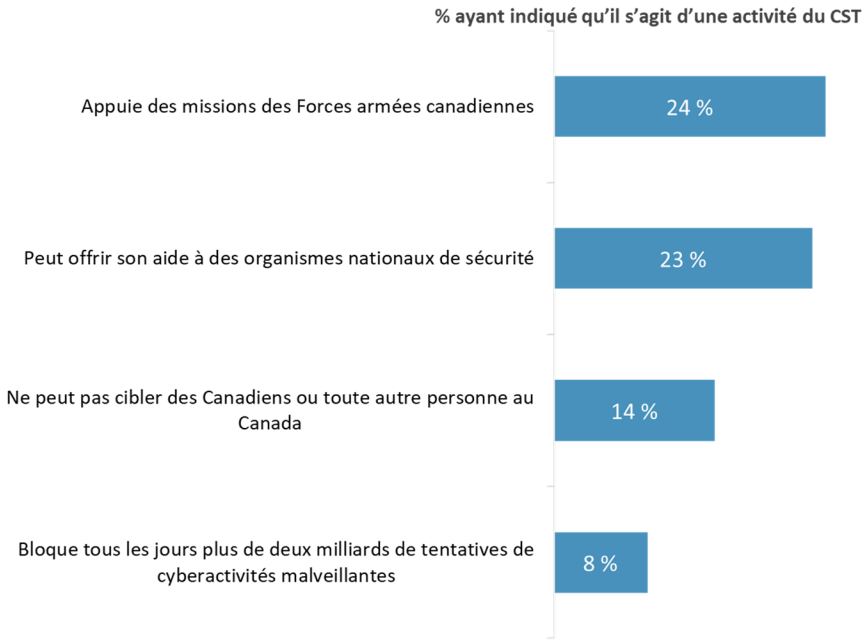
On a demandé aux répondants s'ils étaient au courant de ce qui suit concernant le CST :

- La loi interdit au CST de cibler les Canadiens, où qu'ils soient, ou quiconque se trouvant au Canada.

- Le CST peut offrir son aide à des organismes nationaux de sécurité.
- Dans l'ensemble du gouvernement, le CST bloque tous les jours plus de deux milliards de tentatives de cyberactivités malveillantes.
- Le CST appuie des missions des Forces armées canadiennes, notamment lorsque des Canadiens sont kidnappés à l'étranger.

Moins d'un quart des Canadiens sont au courant de ces faits. Près d'un quart des répondants ont indiqué qu'ils savaient que le CST « appuie des missions des Forces armées canadiennes » (24 %) et que le CST « peut offrir son aide à des organismes nationaux de sécurité » (23 %). Quatorze pour cent ont dit qu'ils savaient que « la loi interdit au CST de cibler les Canadiens ou quiconque se trouvant au Canada », alors que seulement 8 % étaient au courant que le CST « bloque tous les jours plus de deux milliards de tentatives de cyberactivités malveillantes ».

Diagramme 6 : Connaissance du mandat du CST



Base de référence : n=2 505; tous les répondants
Q8. Êtes-vous au courant que… Ne sait pas : entre 3 % et 4 %

Les hommes sont plus nombreux à savoir que la loi interdit au CST de cibler des Canadiens, où qu'ils se trouvent, ou quiconque au Canada (17 % comparativement à 12 % des femmes) et que le CST peut offrir son aide aux organismes nationaux de sécurité (27 % comparativement à 19 % des femmes).

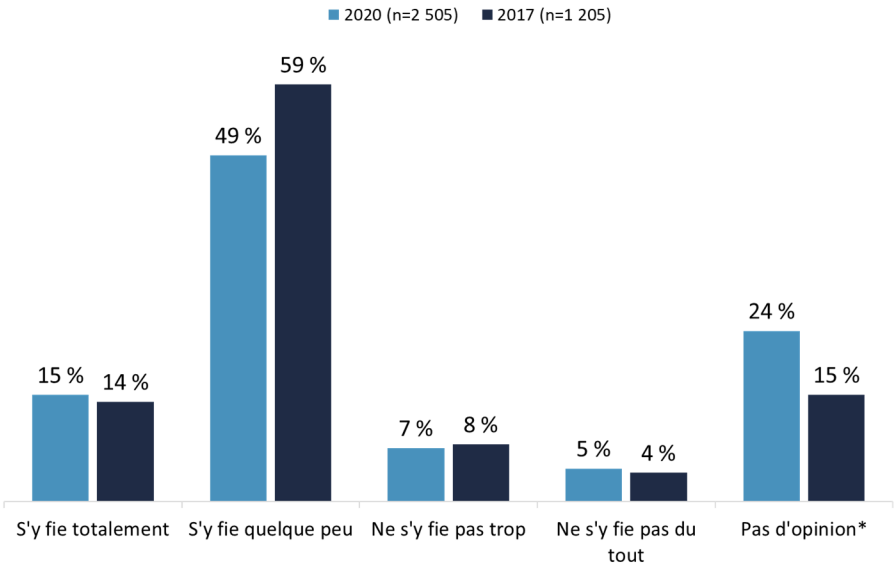
3. Confiance envers le CST

Près des deux tiers des répondants font confiance au CST pour qu'il agisse de manière éthique et légale.

Près des deux tiers des Canadiens se fient « quelque peu » (49 %) ou « totalement » (15 %) au CST pour qu'il agisse de façon éthique et légale. En revanche, 12 % des répondants ne s'y fient « pas du tout » ou « pas trop ». Près d'un quart des répondants (24 %) ont dit qu'ils n'avaient pas d'opinion à ce sujet.

Le niveau de confiance envers le CST par rapport à cette question a décliné au fil du temps (64 % comparativement à 73 % en 2017), bien que le niveau de méfiance demeure inchangé. La proportion de répondants ayant indiqué qu'ils n'avaient pas d'opinion a augmenté avec le temps (24 % comparativement à 15 % en 2017).

Diagramme 7 : Confiance envers le CST : 2020 comparativement à 2017



Q9. À quel point diriez-vous que vous avez confiance que le Centre de la sécurité des télécommunications du Canada agisse de façon éthique et légale dans l'exécution de son mandat? *Comprend les réponses « Ne sait pas ».

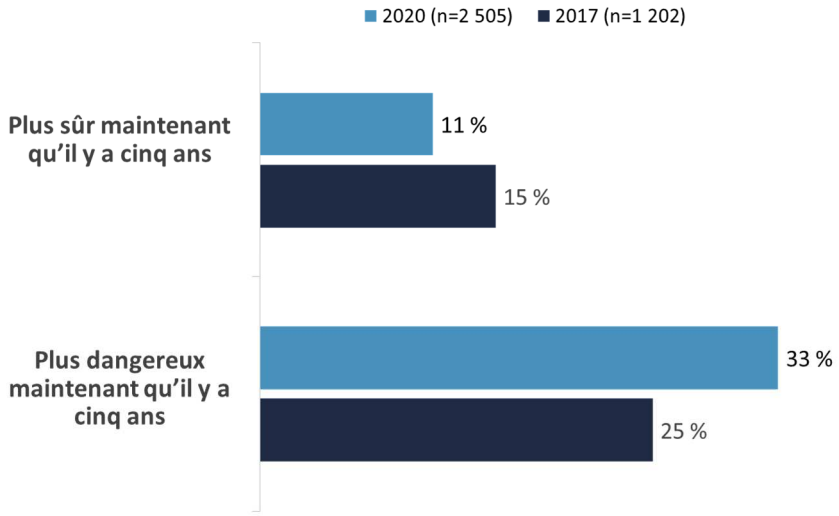
Comparativement aux personnes ayant au plus un diplôme d'études secondaires (58 %), les titulaires d'un diplôme universitaire (68 %) se fient davantage au CST pour qu'il agisse de façon éthique et légale, du moins dans une certaine mesure. La méfiance envers le CST à cet égard est plus importante chez les hommes (16 % comparativement à 9 % des femmes).

4. Opinions concernant la sécurité nationale

Environ un répondant sur 10 estime que le Canada est plus sûr maintenant qu'il y a cinq ans.

Lorsqu'on a demandé aux participants si le Canada était plus sûr, plus dangereux ou à peu de chose près le même qu'il y a cinq ans, environ un répondant sur 10 (11 %) a indiqué que le Canada est plus sûr et un tiers des gens (33 %) estiment que le Canada est plus dangereux. Parmi les autres participants, une majorité (51 %) jugent que, dans l'ensemble, le Canada est à peu de chose près le même qu'il y a cinq ans. La proportion de Canadiens qui estiment que le Canada est plus sûr a diminué légèrement (11 % comparativement à 15 % en 2017), alors que la proportion de ceux qui croient que le Canada est plus dangereux a augmenté au fil du temps (33 % comparativement à 25 % en 2017).

Diagramme 8 : Perceptions de la sécurité du Canada : 2020 comparativement à 2017



Q2. Avez-vous l'impression que, de façon globale, le Canada est plus sûr qu'il y a cinq ans, plus dangereux ou à peu de chose près le même?

La perception que le Canada est plus sûr maintenant qu'il y a cinq ans diminue avec l'âge (elle passe de 17 % chez les répondants de 18 à 34 ans à 8 % chez les personnes de 55 ans et plus) et varie entre 13 % en Ontario et 8 % en Alberta. La perception que le Canada est plus dangereux augmente avec l'âge (de 26 % chez les personnes de 18 à 34 ans à 38 % des répondants de 55 ans et plus). Elle est en outre plus élevée en Ontario (41 %) et dans les Prairies (40 %) et plus faible au Québec (20 %).

5. Équilibre entre la sécurité et les libertés civiles

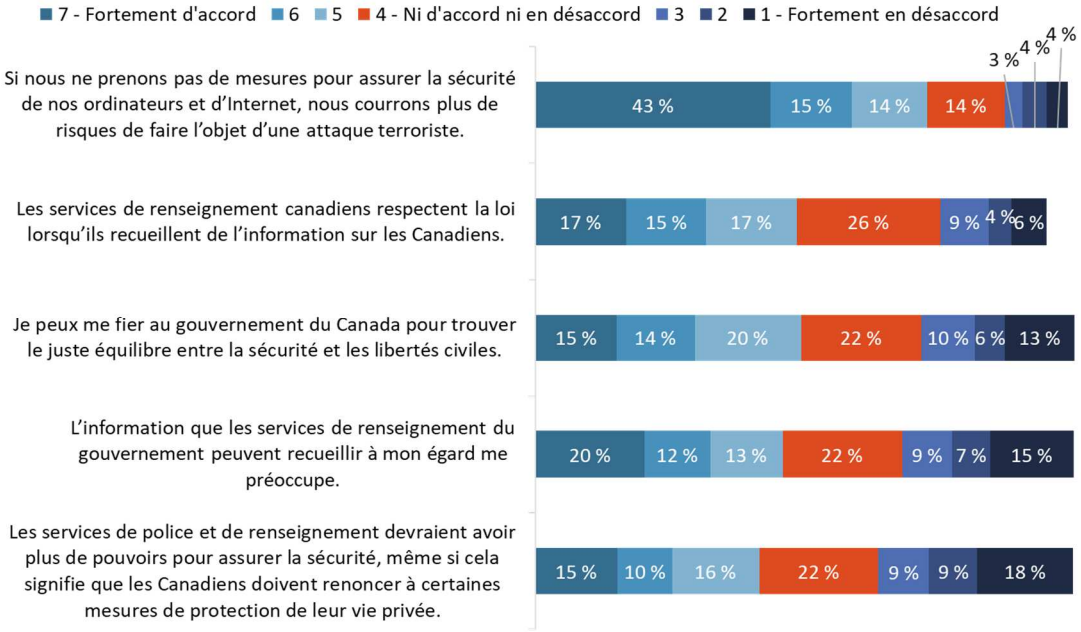
Environ la moitié des répondants sont d'accord avec tous les énoncés concernant l'équilibre entre la sécurité et les libertés civiles.

En utilisant une échelle de sept points où 1 signifie « fortement en désaccord », 7, « fortement d'accord » et 4, « ni d'accord ni en désaccord », les répondants devaient exprimer dans quelle mesure ils étaient d'accord ou en désaccord avec les énoncés suivants concernant l'équilibre entre la sécurité et les libertés civiles :

- Je peux me fier au gouvernement du Canada pour trouver le juste équilibre entre la sécurité et les libertés civiles.
- Les services de police et de renseignement devraient avoir plus de pouvoirs pour assurer la sécurité, même si cela signifie que les Canadiens doivent renoncer à certaines mesures de protection de leur vie privée.
- Les services de renseignement canadiens respectent la loi lorsqu'ils recueillent de l'information sur les Canadiens.
- L'information que les services de renseignement du gouvernement peuvent recueillir à mon égard me préoccupe.
- Si nous ne prenons pas de mesures pour assurer la sécurité de nos ordinateurs et d'Internet, nous courrons plus de risques de faire l'objet d'une attaque terroriste.

Bien que les répondants soient plus susceptibles d'être d'accord qu'en désaccord avec chacun de ces énoncés, la mesure dans laquelle ils sont d'accord varie. L'énoncé avec lequel le plus grand nombre de répondants se montrent d'accord, et le seul qui a reçu une réponse favorable de la majorité des répondants, est le suivant : « Si nous ne prenons pas de mesures pour assurer la sécurité de nos ordinateurs et d'Internet, nous courrons plus de risques de faire l'objet d'une attaque terroriste ». Près des trois quarts (72 %) sont d'accord dans une certaine mesure avec cet énoncé, et 43 % sont *fortement* d'accord.

Diagramme 9 : Équilibre entre la sécurité et les libertés civiles



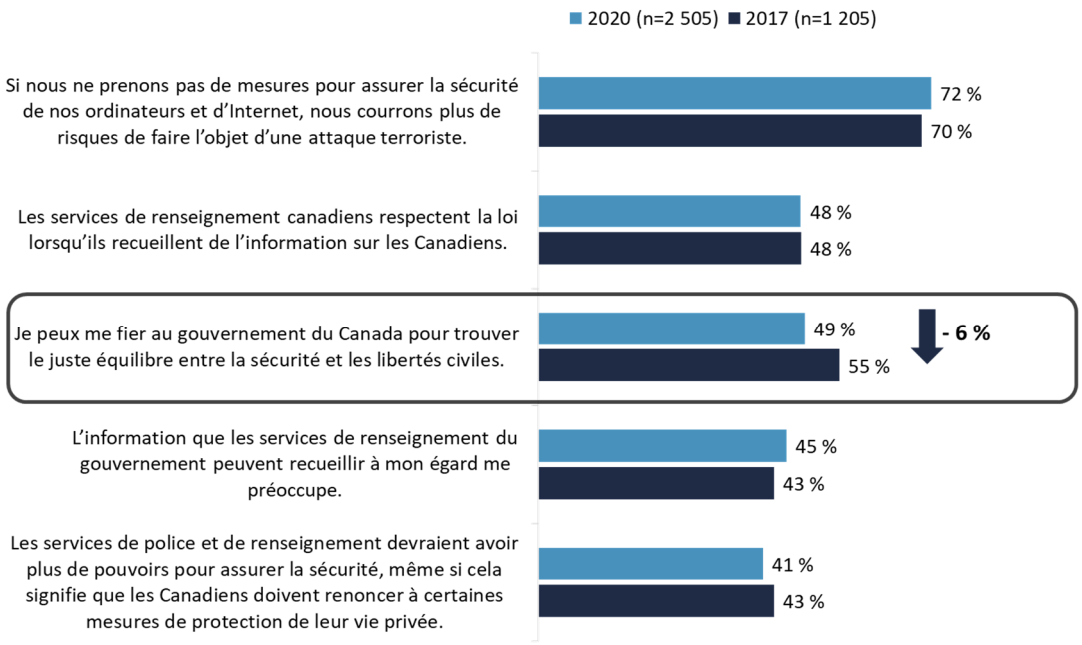
Base de référence : n=2 505; tous les répondants
Q3. À quel point êtes-vous d'accord ou en désaccord avec chacun des énoncés suivants?

Près de la moitié des personnes se disent d'accord dans une certaine mesure avec les énoncés « Les services de renseignement canadiens respectent la loi lorsqu'ils recueillent de l'information sur les Canadiens » (49 %) et « Je peux me fier au gouvernement du Canada pour trouver le juste équilibre entre la sécurité et les libertés civiles » (49 %), alors qu'une proportion légèrement moins élevée (45 %) des répondants sont d'accord avec l'énoncé « L'information que les services de renseignement du gouvernement peuvent recueillir à mon égard me préoccupe ».

Les répondants sont moins susceptibles d'être d'accord avec l'énoncé suivant : « Les services de police et de renseignement devraient avoir plus de pouvoirs pour assurer la sécurité, même si cela signifie que les Canadiens doivent renoncer à certaines mesures de protection de leur vie privée ». Quatre personnes sur 10 (41 %) sont d'accord avec le compromis, c'est-à-dire de renoncer à certaines mesures de protection de la vie privée pour assurer la sécurité, alors que plus du tiers des répondants (36 %) ne sont pas du même avis (18 % sont *fortement* en désaccord).

Comparativement à 2017, la différence suivante est la plus évidente dans les perceptions : un nombre moins important de Canadiens estiment qu'ils peuvent se fier au gouvernement du Canada pour trouver le juste équilibre entre la sécurité et les libertés civiles (49 % comparativement à 55 % en 2017).

Diagramme 10 : Équilibre entre la sécurité et les libertés civiles : 2020 comparativement à 2017



Q3. À quel point êtes-vous d'accord ou en désaccord avec chacun des énoncés suivants?

En ce qui a trait à ces énoncés, les différences suivantes entre les sous-groupes sont dignes de mention :

- Les Canadiens plus âgés ont plus tendance que les plus jeunes à croire que si l'on ne prend pas de mesures pour assurer la sécurité de nos ordinateurs et d'Internet, on court plus de risques de subir une attaque terroriste (75 % des répondants de 55 ans et plus comparativement à 67 % des personnes âgées entre 18 et 34 ans).

- Les femmes (52 % comparativement à 45 % des hommes) ainsi que les titulaires d'un diplôme universitaire (56 % comparativement à 44 % des personnes ayant un niveau de scolarité moins élevé) sont plus susceptibles de croire que l'on peut se fier au gouvernement pour trouver un juste équilibre entre la sécurité et les libertés civiles.

- Les femmes (44 % comparativement à 38 % des hommes) et les Canadiens de 35 ans et plus (46 % comparativement à 28 % des répondants âgés entre 18 et 34 ans) sont plus enclins à être d'avis que les services de police et les organismes de renseignement devraient avoir plus de pouvoirs pour assurer la sécurité même si cela signifie que les Canadiens doivent renoncer à certaines mesures de protection de leur vie privée.

- Les résidents du Québec (51 %) sont plus susceptibles que ceux des Prairies (42 %), de l'Alberta (41 %) et de la Colombie-Britannique (41 %) à se préoccuper de la collecte de renseignements personnels par des organismes gouvernementaux de renseignement. En revanche, les titulaires d'un diplôme universitaire (35 %) sont plus nombreux que les personnes ayant au plus un diplôme d'études secondaires (25 %) à ne pas s'en préoccuper.

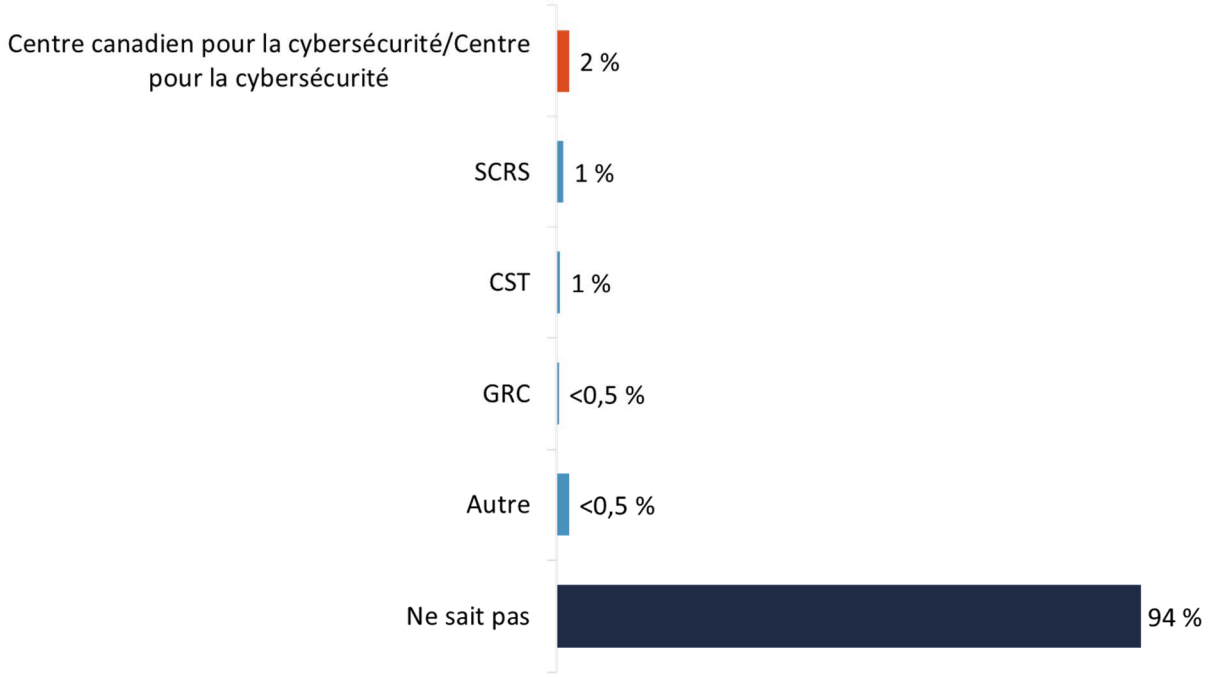
- Finalement, les Canadiens de moins de 35 ans (25 % comparativement à 17 % des répondants de 35 ans et plus) sont plus susceptibles d'être en désaccord avec l'énoncé selon lequel les organismes canadiens de renseignement respectent la loi lorsqu'ils recueillent des renseignements au sujet des Canadiens. Les résidents de l'Alberta (25 %) et des Prairies (24 %) avaient également plus tendance à manifester leur désaccord que les répondants du Québec (16 %).

6. Connaissance et perceptions du Centre pour la cybersécurité

La connaissance spontanée du Centre pour la cybersécurité est pratiquement nulle.

Lorsqu'on a demandé aux répondants de nommer l'organisation qui fait partie du CST et qui a pour principale responsabilité de fournir des conseils, des avis, des services et du soutien en matière de cybersécurité, plus de neuf répondants sur 10 (94 %) ont dit qu'ils ne connaissaient pas le nom de cette organisation. Seulement 2 % ont nommé correctement le Centre canadien pour la cybersécurité ou le Centre pour la cybersécurité.

Diagramme 11 : Connaissance spontanée du Centre pour la cybersécurité



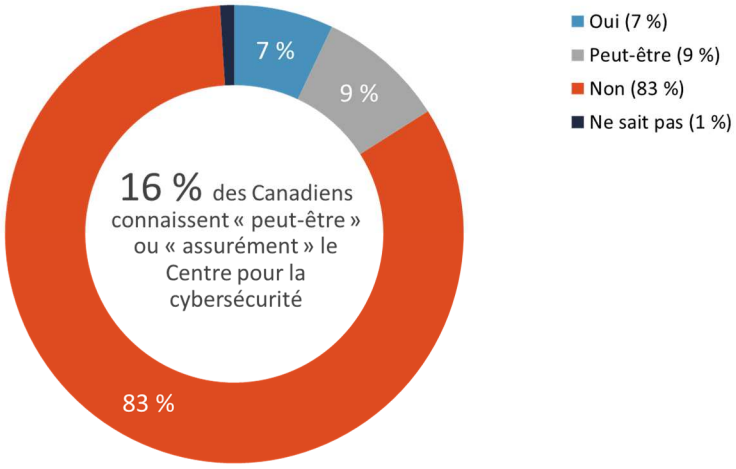
Base de référence : n=2 505; tous les répondants
Q10. Un organisme au sein du Centre de la sécurité des télécommunications du Canada (CST) assume principalement la responsabilité de fournir des avis, des conseils, des services et du soutien concernant la cybersécurité. Pouvez-vous nommer cet organisme?

La plupart des répondants ne connaissent pas le Centre pour la cybersécurité.

Lorsqu'on a demandé directement aux répondants s'ils avaient entendu, vu ou lu quelque chose au sujet du Centre canadien pour la cybersécurité ou le Centre pour la cybersécurité, la grande majorité (83 %) ont répondu par la négative. Seulement 16 % des participants ont dit qu'ils avaient *peut-être* ou *assurément* entendu, vu ou lu quelque chose au sujet du Centre pour la cybersécurité; 9 % ont répondu *peut-être* et 7 % ont dit *oui*. Ces résultats ont été obtenus en posant la question suivante :

> Le Centre canadien pour la cybersécurité, ou le Centre pour la cybersécurité, a été créé en 2018. Réunissant l'expertise opérationnelle ayant trait à la cybersécurité de plusieurs unités au gouvernement du Canada, le Centre pour la cybersécurité est une source importante qui fournit des avis, des conseils, des services et du soutien en matière de cybersécurité au gouvernement, au secteur privé et à la population canadienne. Avez-vous entendu, vu ou lu quelque chose au sujet du Centre canadien pour la cybersécurité ou du Centre pour la cybersécurité?

Diagramme 12 : Connaissance assistée du Centre pour la cybersécurité



Base de référence : n=2 505; tous les répondants
Q11. Avez-vous entendu, vu ou lu quelque chose au sujet du Centre canadien pour la cybersécurité ou du Centre pour la cybersécurité?

Au moins un tiers des répondants estiment que les activités du Centre pour la cybersécurité ont un grand effet sur le Canada.

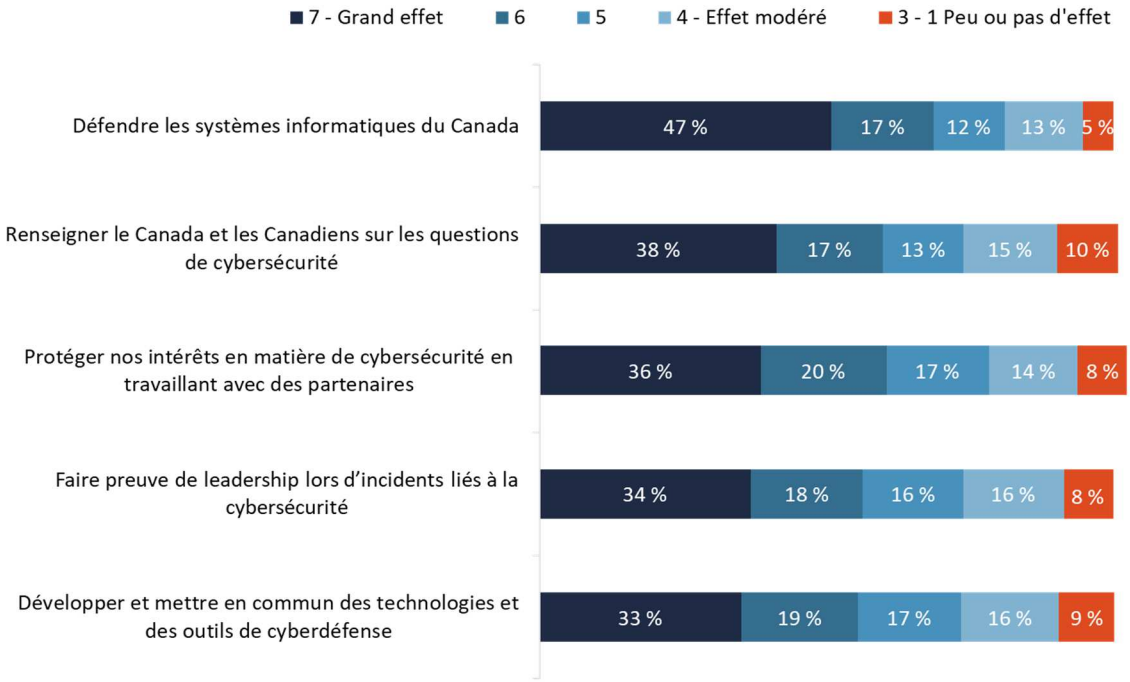
On a lu aux répondants une liste des activités du Centre pour la cybersécurité et on leur a demandé d'indiquer dans quelle mesure ils croyaient que ces activités ont un effet sur le Canada, en utilisant une échelle de sept points, où 1 signifie « aucun effet », 7, un « grand effet », et 4, un « effet modéré ». Les activités étaient les suivantes :

- Renseigner le Canada et les Canadiens sur les questions de cybersécurité.
- Protéger nos intérêts en matière de cybersécurité en travaillant avec des entreprises et des partenaires gouvernementaux.
- Développer et mettre en commun des technologies et des outils de cyberdéfense.
- Défendre les systèmes informatiques du Canada.
- Faire preuve de leadership lors d'incidents liés à la cybersécurité.

Plus des deux tiers des Canadiens ont accordé une cote équivalente ou supérieure à 5 pour chacune de ces activités; selon eux, chaque activité a un effet plus que modéré sur le Canada. En outre, au moins deux tiers des répondants estiment que chaque activité a un grand effet.

L'activité qui, aux yeux des participants, entraîne le plus grand effet (cote de 5 ou plus) représente la défense des systèmes informatiques du Canada (76 %), suivie de la protection de nos intérêts en matière de cybersécurité en travaillant avec des partenaires (73 %), du développement et de la mise en commun des technologies et des outils de cyberdéfense (69 %) et de l'information fournie au Canada et aux Canadiens sur des questions de cybersécurité et du leadership lors d'incidents liés à la cybersécurité (68 % chacun).

Diagramme 13 : Perception de l'effet des activités du Centre pour la cybersécurité sur le Canada



Base de référence : n=2 505; tous les répondants
Q12. Je vais maintenant vous lire une liste des principales choses que fait le Centre pour la cybersécurité. Pour chacune d'elles, j'aimerais que vous me disiez dans quelle mesure, selon vous, cette activité a ou aura un effet sur le Canada.

Les différences suivantes entre les sous-groupes sont dignes de mention :

- Les groupes suivants sont plus susceptibles de trouver que l'activité de renseigner le Canada et les Canadiens au sujet des questions de cybersécurité entraîne un effet perceptible (cote de 5 ou plus) : les plus jeunes répondants (74 % des personnes âgées entre 18 et 34 ans comparativement à 65 % des répondants de 55 ans et plus), les répondants ayant un niveau de scolarité plus élevé (77 % des titulaires d'un diplôme universitaire comparativement à 64 % des participants ayant un diplôme d'études secondaires ou moins) et les répondants de l'Ontario et du Québec (71 % dans chacune de ces provinces comparativement aux résidents de la Colombie-Britannique (63 %)).
- Les répondants ayant un niveau de scolarité plus élevé (77 % des titulaires d'un diplôme universitaire comparativement à 68 % des personnes ayant au plus un diplôme d'études secondaires) ont plus tendance à attribuer un effet perceptible à l'activité de protéger les intérêts en matière de cybersécurité en travaillant avec des entreprises et des partenaires gouvernementaux. Au niveau régional, c'est au Québec (77 %) que les répondants sont les plus enclins à croire que cette activité porte fruit et c'est en Colombie-Britannique qu'ils le sont le moins (65 %).
- La probabilité d'attribuer un effet perceptible au développement et à la mise en commun des technologies et des outils de cyberdéfense augmente avec le niveau de scolarité (61 % des personnes ayant au plus un diplôme d'études secondaires et 74 % des titulaires d'un diplôme universitaire). Elle diminue avec l'âge (75 % des personnes âgées entre 18 et 34 ans et 64 % des répondants de 55 ans et plus) et s'avère la plus élevée au Québec (76 % comparativement à la proportion totalisant entre 62 % et 68 % ailleurs).
- Les groupes suivants sont plus susceptibles d'attribuer un effet perceptible à la défense des systèmes informatiques au Canada : les titulaires d'un diplôme universitaire (79 % comparativement à 73 % des personnes ayant une formation collégiale ou professionnelle et à 74 % des personnes ayant au plus un diplôme d'études secondaires) et les répondants de 54 ans et moins (79 % des participants âgés

entre 18 et 34 ans et 77 % des personnes de 35 à 54 ans comparativement à 72 % des gens de 55 ans et plus).

- La probabilité d'attribuer un effet perceptible au leadership lors d'incidents liés à la cybersécurité augmente avec le niveau de scolarité (61 % des personnes ayant au plus un diplôme d'études secondaires et 74 % des titulaires d'un diplôme universitaire) et varie au niveau régional; elle s'établit à 73 % au Québec et à 62 % en Colombie-Britannique.

7. État de préparation en vue d'une cyberattaque

Le gouvernement canadien semble le plus préparé pour lutter contre une menace de cyberattaque.

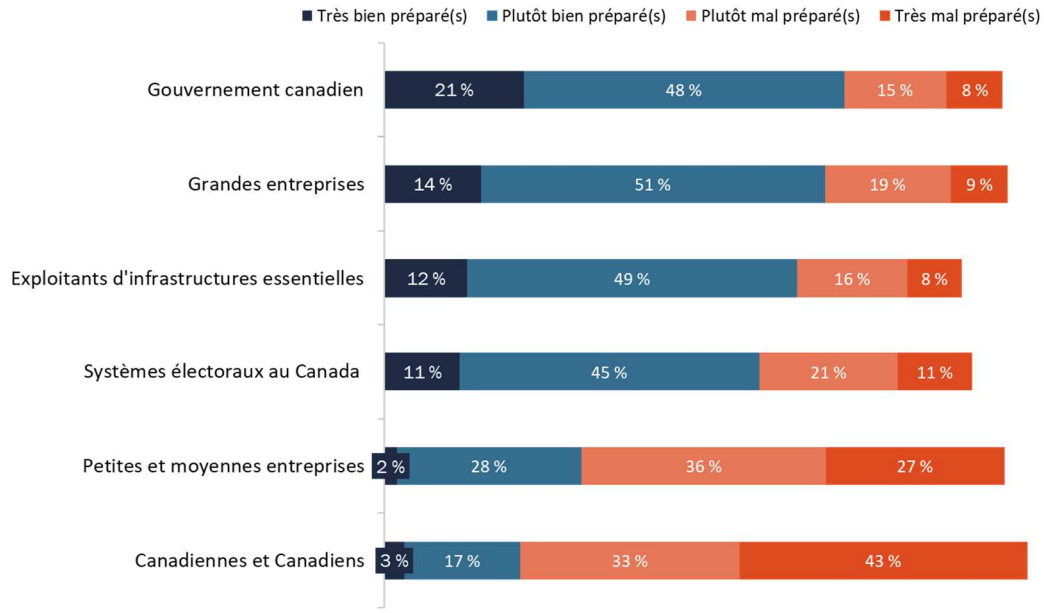
Finalement, on a demandé aux répondants d'indiquer dans quelle mesure chacune de ces entités est préparée, selon eux, à lutter contre une menace de cyberattaque :

- le gouvernement canadien;
- les systèmes électoraux dans l'ensemble du Canada;
- les Canadiennes et les Canadiens;
- les grandes entreprises;
- les petites et moyennes entreprises;
- les exploitants d'infrastructures essentielles.

Une majorité de répondants estiment que la plupart de ces entités sont au moins quelque peu préparées à réagir en cas de menace de cyberattaque. Cela dit, la taille de la majorité varie selon l'entité et les répondants sont beaucoup plus susceptibles de les considérer « plutôt bien » préparées plutôt que « très bien » préparées. En réalité, pas plus d'une personne sur cinq (21 %) juge que l'une ou l'autre de ces entités est très bien préparée pour réagir à une cyberattaque.

Le gouvernement canadien est plus susceptible d'être considéré, au minimum, comme plutôt bien préparé à cet égard (69 %), suivi des grandes entreprises (65 %), des exploitants d'infrastructures essentielles (61 %) et des systèmes électoraux dans l'ensemble du Canada (56 %). À titre de comparaison, seulement 30 % des répondants estiment que les petites et moyennes entreprises sont préparées à réagir à une menace de cyberattaque, et seulement un participant sur cinq (20 %) croit que les Canadiennes et les Canadiens y sont préparés. Près des deux tiers jugent que les petites et moyennes entreprises sont plutôt mal (36 %) ou très mal préparées (27 %), alors que plus des trois quarts sont d'avis que les Canadiennes et les Canadiens sont plutôt mal (33 %) ou très mal préparés (43 %).

Diagramme 14 : État de préparation des différentes entités pour réagir à une cybermenace



Base de référence : n=2 505; tous les répondants

Q13. À votre avis, dans quelle mesure croyez-vous que chacun des éléments suivants est prêt à faire face à une cyberattaque? Diriez-vous que [INSÉRER LE CHOIX DE RÉPONSE] [EST/SONT] très bien préparé(s), plutôt préparé(s), plutôt mal préparé(s) ou très mal préparé(s) à affronter une cybermenace?

Plus les répondants sont âgés (78 % des personnes âgées entre 18 et 34 ans et 63 % des gens de 55 ans et plus), moins ils ont l'impression que le gouvernement canadien est prêt à faire face à une cybermenace. On note la même tendance pour ce qui est des perceptions des répondants concernant le système électoral (65 % des personnes âgées entre 18 et 34 ans et 51 % des gens de 55 ans et plus) et les exploitants d'infrastructures essentielles (67 % des personnes âgées entre 18 et 34 ans et 58 % des répondants de 55 ans et plus). Les plus jeunes participants (72 %), soit ceux ayant entre 18 et 34 ans, et les répondants de 35 à 54 ans (72 %) sont aussi plus susceptibles que les gens de 55 ans et plus (58 %) de croire que les grandes entreprises sont préparées à une telle éventualité.

Les groupes suivants ont plus l'impression que les Canadiennes et les Canadiens sont mal préparés pour réagir à une cybermenace :

- les répondants âgés entre 35 et 54 ans (80 % comparativement à 73 % des personnes de 18 à 34 ans et à 75 % des participants de 55 ans et plus);
- les personnes ayant une formation collégiale ou professionnelle (80 %) et un diplôme universitaire (79 %) comparativement aux répondants ayant au plus un diplôme d'études secondaires (66 %).

Finalement, les répondants du Québec sont plus susceptibles de croire que les entités suivantes sont mal préparées pour réagir à une cybermenace : le gouvernement canadien, les grandes entreprises, les petites et moyennes entreprises, ainsi que les exploitants d'infrastructures essentielles.

Annexes

1. Caractéristiques techniques

Les caractéristiques suivantes s'appliquent à l'enquête :

- Un sondage téléphonique à composition aléatoire de 12 minutes a été administré à 2 505 Canadiens de 18 ans et plus.
- Nous avons eu recours à un échantillonnage aléatoire afin d'extrapoler les résultats à l'ensemble de la population de Canadiens de 18 ans et plus.
- Les entrevues ont été réalisées par Elemental Data Collection Inc. (EDCI) au moyen de l'interview téléphonique assistée par ordinateur (ITAO).
- Conformément aux pratiques exemplaires en matière de sondage, le questionnaire a fait l'objet d'un prétest au préalable afin de s'assurer qu'il mesurait ce qu'il devait mesurer.
    - Les répondants avaient le choix de participer dans la langue officielle de leur choix.
    - Les entrevues du prétest ont été enregistrées en mode numérique et examinées par des membres de l'équipe de Phoenix SPI.
    - Dix entrevues ont été réalisées dans chacune des langues officielles.
    - De manière générale, le questionnaire était bien élaboré. Aucun problème important n'est ressorti en ce qui a trait à la conception du questionnaire ou à la compréhension qu'avaient les répondants des questions. La longueur du questionnaire représentait le seul enjeu; il était trop long. Par conséquent, la taille de l'échantillon a été réduite pour pouvoir mener une plus longue entrevue.
- Une base d'échantillonnage double avec chevauchement (utilisateurs de téléphone fixe et de cellulaire) a été utilisée pour réduire au minimum les erreurs de couverture. En tout, 1 721 entrevues (ou 69 % du nombre total) ont été réalisées à partir de l'échantillon de participants joints par ligne terrestre et 784 entrevues (ou 31 % du nombre total) ont été effectuées avec des participants joints au cellulaire.
    - On a indiqué à tous les répondants que leur participation était volontaire et que les renseignements recueillis seraient protégés en vertu de la *Loi sur la protection des renseignements personnels*.
    - Les appels ont été faits à différents moments de la journée et de la semaine pour optimiser la possibilité d'établir un contact.
    - Dans le groupe de l'échantillon de répondants joints par ligne terrestre, un minimum de huit rappels ont été effectués avant de retirer le numéro de la liste. Pour l'échantillon de répondants joints au cellulaire, un minimum de cinq rappels ont été faits.
- L'échantillon était disproportionné sur le plan géographique afin d'améliorer l'exactitude des résultats provinciaux. La répartition des entrevues complétées est comme suit :

Strate	Entrevues complétées
Terre-Neuve-et-Labrador	150
Île-du-Prince-Édouard	150
Nouvelle-Écosse	150
Nouveau-Brunswick	150
Québec	450
Ontario	600

Manitoba	175
Saskatchewan	178
Alberta	225
Colombie-Britannique	272
Territoires	5

- L'échantillon de 2 505 Canadiens est jugé exact avec une marge d'erreur de plus ou moins 2,2 %, 19 fois sur 20 (rajustée pour refléter l'échantillon disproportionné sur le plan géographique).
- Le travail sur le terrain a été réalisé entre le 11 février et le 7 mars 2020.
- Le taux de réponse global[1] est de 7 % (9 % pour l'échantillon de répondants joints par ligne terrestre et 4 % pour l'échantillon de répondants joints par cellulaire). Le tableau ci-dessous présente de l'information au sujet des dispositions du dernier appel réparties selon le type d'échantillon.

	Total	Téléphone fixe	Cellulaire
Nombre total de numéros, au départ	**104 396**	**32 963**	**71 433**
Hors du champ de l'étude – non valides	**62 639**	**12 661**	**49 978**
Cas non résolus (U)	**26 404**	**11 993**	**14 411**
Pas de réponse/répondeur	26 404	11 993	14 411
Admissibles - Non-réponse (IS)	**1 392**	**548**	**844**
Problème de langue	457	285	172
Incapable de répondre (malade/décès)	119	67	52
Rappel (répondant non disponible)	2 060	799	1 261
Refus	9 586	5 071	4 515
Raccroché	418	265	153
Admissibles - Réponses (R)	**12 640**	**6 487**	**6 153**
Quota atteint	16	15	1
Entrevue complétée	2 505	1 721	784
Non admissible – Refus de mentionner sa province	35	25	10
Non admissible – Exclusions liées à l'industrie	111	61	50
Non admissible – Âge	46	0	46

- Les données du sondage ont été pondérées selon la région, l'âge et le sexe au moyen des données démographiques tirées du Recensement de 2016 de Statistique Canada.
- Le potentiel de biais de non-réponse a été évalué en comparant les caractéristiques des répondants au moyen de données non pondérées et pondérées. Comme c'est généralement le cas pour les sondages téléphoniques visant l'ensemble de la population, les Canadiens plus âgés (55 ans et plus) sont surreprésentés et les Canadiens plus jeunes (moins de 35 ans) sont sous-représentés dans l'échantillon du sondage. Cela a été corrigé par la pondération.

[1] La formule du taux de réponse est la suivante : [R=R/(U+IS+R)]. Autrement dit, pour obtenir le taux de réponse, il faut diviser le nombre d'unité ayant répondu [R] par le nombre de cas non résolus [U] plus le nombre de ménages et de personnes admissibles n'ayant pas répondu [IS] plus le nombre d'unités ayant répondu [R].

2. Questionnaire de sondage

INTRODUCTION

Bonjour. Je m'appelle [nom de l'intervieweur]. Je vous téléphone au nom de Phoenix SPI qui mène, pour le compte du gouvernement du Canada, une enquête sur des questions d'intérêt pour la population canadienne. Préférez-vous continuer en français ou en anglais? / Would you prefer to continue in English or French?

NOTE DE L'INTERVIEWEUR : Si le répondant préfère répondre en anglais, l'intervieweur doit être en mesure de continuer l'entrevue en anglais ou lire ce qui suit : « Thank you. Someone will call you back soon to complete the survey in English. »

Il faut environ sept minutes pour répondre au sondage et vous êtes libre d'y participer ou non. Vos réponses demeureront entièrement confidentielles et anonymes.

[ÉCHANTILLON DE RÉPONDANTS JOINTS PAR LIGNE TERRESTRE]

A. Nous aimerions parler à la personne de votre foyer qui a 18 ans ou plus et qui a célébré son anniversaire de naissance le plus récemment? Est-ce que ce serait vous?

*[INTERVIEWEUR : AU BESOIN : Nous choisissons des numéros de téléphone au hasard, puis une personne de chaque foyer à interviewer.]

01. Oui	PASSER À LA QR. 1
02. Non	DEMANDER DE PARLER À LA PERSONNE ADMISSIBLE; RÉPÉTER L'INTRODUCTION

[ÉCHANTILLON DE RÉPONDANTS JOINTS PAR CELLULAIRE]

B. Avez-vous 18 ans ou plus?

01. Oui	CONTINUER
02. Non	REMERCIER/METTRE FIN

C. Vous trouvez-vous à un endroit où vous pouvez parler au téléphone en sécurité et répondre à mes questions?

01. Oui	PASSER À LA QR. 1
02. Non	POSER LA QUESTION D

D. Nous aimerions réaliser cette entrevue lorsque ce sera sûr et pratique pour vous d'y participer. À quel moment devrais-je vous rappeler?

FIXER SI POSSIBLE UN TEMPS POUR RAPPELER (HEURE/JOUR) : _____

QUESTIONS DE RECRUTEMENT

[TOUT LE MONDE]

QR. 1 Travaillez-vous dans l'un ou l'autre des secteurs suivants? [LIRE LA LISTE]

01. La publicité, les études de marché ou les relations publiques
02. Les médias (p. ex., télévision, radio, journaux)
03. La cybersécurité

REMERCIER/ METTRE FIN SI LE RÉPONDANT DIT OUI À L'UNE DES OPTIONS CI-DESSUS
METTRE FIN SI LE RÉPONDANT DIT QU'IL NE SAIT PAS OU S'IL REFUSE DE RÉPONDRE

MESSAGE POUR REMERCIER/METTRE FIN : « Merci d'avoir accepté de répondre au présent sondage, mais vous ne répondez pas aux critères d'admissibilité de l'enquête. »

QR. 2 Quelle est l'année de votre naissance?

Inscrire l'année : _____
99. [NE PAS LIRE] Je ne sais pas/je refuse de répondre

[DEMANDER QR. 3 SI QR. 2 = 99]

QR. 3 Seriez-vous disposé à me dire à quelle catégorie d'âge vous appartenez?

[LIRE LA LISTE]

01. 18 à 24 ans
02. 25 à 34 ans
03. 35 à 44 ans
04. 45 à 54 ans
05. 55 à 64 ans
06. 65 ans ou plus
99. [NE PAS LIRE] Je refuse de répondre

QR. 4 Dans quelle province ou quel territoire habitez-vous?

[NE PAS LIRE LA LISTE]

01. Terre-Neuve-et-Labrador
02. Île-du-Prince-Édouard
03. Nouvelle-Écosse
04. Nouveau-Brunswick
05. Québec
06. Ontario
07. Manitoba
08. Saskatchewan
09. Alberta
10. Colombie-Britannique
11. Yukon
12. Territoires du Nord-Ouest
13. Nunavut

METTRE FIN SI LE RÉPONDANT DIT QU'IL NE SAIT PAS OU S'IL REFUSE DE RÉPONDRE

QR. 5 INSCRIRE LE SEXE [SELON LA VOIX]

01. Homme
02. Femme

CONNAISSANCE SPONTANÉE DES ORGANISMES DE RENSEIGNEMENT

1. Comme vous le savez peut-être déjà, il y a un organisme gouvernemental qui est chargé d'intercepter et d'analyser des communications étrangères et de contribuer à la protection des réseaux informatiques du gouvernement. Pouvez-vous nommer cet organisme? [SUIVI : 2017]

   [NE PAS LIRE LA LISTE; ACCEPTER UNE SEULE RÉPONSE]

   01. Le Centre de la sécurité des télécommunications (CST)
   02. Le Service canadien du renseignement de sécurité (SCRS)
   03. Le ministère de la Défense nationale (les Forces armées canadiennes)
   04. Affaires mondiales Canada (MAECD ou Affaires étrangères)
   05. Le Bureau d'appréciation des renseignements
   06. Le Bureau du renseignement économique
   07. Le Centre canadien pour la cybersécurité (Centre pour la cybersécurité)
   08. Le CST et le Centre pour la cybersécurité
   09. Autre réponse (veuillez préciser)
   99. [NE PAS LIRE] Je ne sais pas

CONFIANCE DANS LES SERVICES DE RENSEIGNEMENT DU GOUVERNEMENT

2. Avez-vous l'impression que, de façon globale, le Canada est plus sûr qu'il y a cinq ans, plus dangereux ou à peu de chose près le même? [SUIVI : 2017]

   [NE PAS LIRE LA LISTE]

   01. Plus sûr
   02. Plus dangereux
   03. À peu de chose près le même
   99. [NE PAS LIRE] Je ne sais pas

3. À quel point êtes-vous d'accord ou en désaccord avec chacun des énoncés suivants? Veuillez répondre en utilisant une échelle de sept points où 1 signifie « fortement en désaccord », 7 veut dire « fortement d'accord » et le point milieu, 4, signifie que vous n'êtes ni d'accord ni en désaccord. [SUIVI : 2017]

   a. Je peux me fier au gouvernement du Canada pour trouver le juste équilibre entre la sécurité et les libertés civiles.
   b. Les services de police et de renseignement devraient avoir plus de pouvoirs pour assurer la sécurité, même si cela signifie que les Canadiens doivent renoncer à certaines mesures de protection de leur vie privée.
   c. Les services de renseignement canadiens respectent la loi lorsqu'ils recueillent de l'information sur les Canadiens.
   d. L'information que les services de renseignement du gouvernement peuvent recueillir à mon égard me préoccupe.
   e. Si nous ne prenons pas de mesures pour assurer la sécurité de nos ordinateurs et d'Internet, nous courrons plus de risques de faire l'objet d'une attaque terroriste.

CONNAISSANCES ET PERCEPTIONS RELATIVES AU CST

4. Le Centre de la sécurité des télécommunications du Canada (ou CST) est l'organisme gouvernemental canadien chargé d'intercepter et d'analyser des communications étrangères et de contribuer à protéger les réseaux informatiques importants du pays, comme les systèmes gouvernementaux et l'infrastructure essentielle. Diriez-vous que vous avez déjà lu, vu ou entendu quoi que ce soit sur le Centre de la sécurité des télécommunications du Canada (CST)? [SUIVI-MODIFIÉ : 2017]

   [LIRE LA LISTE]

   01. Oui
   02. Peut-être
   03. Non
   99. [NE PAS LIRE] Je ne sais pas

5. Selon cette description et les connaissances que vous possédez peut-être déjà sur le Centre de la sécurité des télécommunications du Canada (ou CST), diriez-vous que sa mission est très importante, plutôt importante, pas très importante ou pas du tout importante pour la sécurité nationale du Canada – ou n'avez-vous pas d'opinion? [SUIVI : 2017]

   [NE PAS LIRE LA LISTE]

   01. Très importante
   02. Plutôt importante
   03. Pas très importante
   04. Pas du tout importante
   05. Pas d'opinion
   99. [NE PAS LIRE] Je ne sais pas

6. Je vais vous lire une liste des principales choses que fait le Centre de la sécurité des télécommunications du Canada (ou CST). Pour chacune d'elles, j'aimerais que vous me disiez si vous trouvez que c'est quelque chose de très important, plutôt important, pas très important ou pas important du tout pour la sécurité nationale du Canada.

   [ALTERNER L'ORDRE DES CHOIX DE RÉPONSE]

   a. Recueillir des renseignements étrangers, ce qui comprend l'interception et l'analyse de communications étrangères.
   b. Protéger les réseaux informatiques importants du pays contre les cyberattaques.
   c. Aider les organismes d'application de la loi et de sécurité en participant à la collecte et à l'analyse de communications.
   d. Défendre activement les réseaux au Canada contre les cybermenaces étrangères.
   e. Neutraliser les cybermenaces étrangères avant qu'elles nuisent au Canada ou aux Canadiens.

   [RÉPÉTER L'ÉCHELLE AU BESOIN]

   01. Très important
   02. Plutôt important
   03. Pas très important
   04. Pas du tout important
   05. Pas d'opinion
   99. [NE PAS LIRE] Je ne sais pas

SI LE RÉPONDANT ESTIME QU'AU MOINS DEUX CHOIX DE RÉPONSE À LA Q6 SONT « TRÈS IMPORTANTS » :

7. Laquelle des activités suivantes est <u>la plus</u> importante pour ce qui est de la sécurité nationale du Canada?

   [INSÉRER LES RÉPONSES DE LA Q6]

8. Êtes-vous au courant que…

   [ALTERNER L'ORDRE DES CHOIX DE RÉPONSE]

   a. La loi interdit au CST de cibler les Canadiens, où qu'ils soient, ou quiconque se trouvant au Canada.
   b. Le CST peut offrir son aide à des organismes nationaux de sécurité.
   c. Dans l'ensemble du gouvernement, le CST bloque tous les jours plus de deux milliards de tentatives de cyberactivités malveillantes.
   d. Le CST appuie des missions des Forces armées canadiennes, notamment lorsque des Canadiens sont kidnappés à l'étranger.

   [LIRE LA LISTE]

   1. Oui
   2. Non
   99. [NE PAS LIRE] Je ne sais pas

9. À quel point diriez-vous que vous avez confiance que le Centre de la sécurité des télécommunications du Canada agisse de façon éthique et légale dans l'exécution de son mandat? Diriez-vous que vous vous fiez totalement, vous vous fiez quelque peu, vous ne vous fiez pas trop ou vous ne vous fiez pas du tout au CST, ou n'avez-vous pas d'opinion à ce sujet? [SUIVI : 2017]

   [NE PAS LIRE LA LISTE]

   01. Vous vous y fiez totalement
   02. Vous vous y fiez quelque peu
   03. Vous ne vous y fiez pas trop
   04. Vous ne vous y fiez pas du tout
   05. Pas d'opinion
   99. [NE PAS LIRE] Je ne sais pas

CONNAISSANCES ET PERCEPTIONS RELATIVES AU CENTRE POUR LA CYBERSÉCURITÉ

10. Un organisme au sein du Centre de la sécurité des télécommunications du Canada (CST) assume principalement la responsabilité de fournir des avis, des conseils, des services et du soutien concernant la cybersécurité. Pouvez-vous nommer cet organisme?

    [NE PAS LIRE LA LISTE : ACCEPTER UNE SEULE RÉPONSE]

    1. Le Centre canadien pour la cybersécurité
    2. Le Centre pour la cybersécurité
    3. Cyber Nouveau-Brunswick ou Cyber NB
    4. Cybersecure Catalyst
    5. Centre mondial du renseignement et de la cybersécurité
    6. Institut canadien pour la cybersécurité
    7. Autre réponse (veuillez préciser)
    99. [NE PAS LIRE] Je ne sais pas

11. Le Centre canadien pour la cybersécurité, ou le Centre pour la cybersécurité, a été créé en 2018. Réunissant l'expertise opérationnelle ayant trait à la cybersécurité de plusieurs unités au gouvernement du Canada, le Centre pour la cybersécurité est une source importante qui fournit des avis, des conseils, des services et du soutien en matière de cybersécurité au gouvernement, au secteur privé et à la population canadienne. Avez-vous entendu, vu ou lu quelque chose au sujet du Centre canadien pour la cybersécurité ou du Centre pour la cybersécurité?

    [LIRE LA LISTE]

    01. Oui
    02. Peut-être
    03. Non
    99. [NE PAS LIRE] Je ne sais pas

12. Je vais maintenant vous lire une liste des principales choses que fait le Centre pour la cybersécurité. Pour chacune d'elles, j'aimerais que vous me disiez dans quelle mesure, selon vous, cette activité a ou aura un effet sur le Canada. Veuillez utiliser une échelle de sept points où 1 signifie « aucun effet », 7 veut dire « un grand effet » et le point milieu, 4, signifie « un effet modéré ».

    [ALTERNER L'ORDRE DES CHOIX DE RÉPONSE]

    a. Renseigner le Canada et les Canadiens sur les questions de cybersécurité.
    b. Protéger nos intérêts en matière de cybersécurité en travaillant avec des entreprises et des partenaires gouvernementaux.
    c. Développer et mettre en commun des technologies et des outils de cyberdéfense.
    d. Défendre les systèmes informatiques du Canada.
    e. Faire preuve de leadership lors d'incidents liés à la cybersécurité.

Finalement,

13. À votre avis, dans quelle mesure croyez-vous que chacun des éléments suivants est prêt à faire face à une cyberattaque? Diriez-vous que [INSÉRER LE CHOIX DE RÉPONSE] [EST/SONT] très bien préparé(s), plutôt préparé(s), plutôt mal préparé(s) ou très mal préparé(s) à affronter une cybermenace?

    [ALTERNER L'ORDRE DES CHOIX DE RÉPONSE]

    a. Le gouvernement canadien
    b. Les systèmes électoraux dans l'ensemble du Canada
    c. Les Canadiennes et les Canadiens
    d. Les grandes entreprises
    e. Les petites et moyennes entreprises
    f. Les exploitants d'infrastructures essentielles

NOTE À L'INTERVIEWEUR : SI LE RÉPONDANT POSE UNE QUESTION AU SUJET DES « INFRASTRUCTURES ESSENTIELLES », DIRE : On veut dire des secteurs, comme l'énergie, les services publics, les soins de santé et les finances, entre autres.

RENSEIGNEMENTS DÉMOGRAPHIQUES

Finalement, nous avons quelques questions à vous poser à des fins statistiques seulement. Soyez assuré(e) que vos réponses demeureront entièrement confidentielles.

14. Quel est le plus haut niveau de scolarité que vous avez atteint?

    [LIRE LA LISTE; ARRÊTER LORSQUE LA PERSONNE FOURNIT UNE RÉPONSE]

    01. Études primaires ou moins
    02. Études secondaires partielles
    03. Diplôme d'études secondaires ou équivalent
    04. Diplôme d'apprenti ou autre certificat ou diplôme d'une école de métiers
    05. Certificat ou diplôme d'un collège, d'un cégep ou d'un établissement d'enseignement autre qu'une université
    06. Certificat ou diplôme universitaire inférieur à un baccalauréat
    07. Baccalauréat
    08. Diplôme d'études supérieures
    99. [NE PAS LIRE] Je préfère ne pas répondre

15. Laquelle des catégories suivantes décrit le mieux votre situation d'emploi actuelle?

    [LIRE LA LISTE; ARRÊTER LORSQUE LA PERSONNE FOURNIT UNE RÉPONSE]

    01. Salarié(e) à temps plein (plus de 30 heures)
    02. Salarié(e) à temps partiel
    03. Travailleur(euse) autonome
    04. Sans emploi et en recherche d'emploi
    05. Personne au foyer
    06. Étudiant(e)
    07. Personne handicapée
    08. Retraité(e)
    09. Autre réponse (veuillez préciser)
    99. [NE PAS LIRE] Je ne sais pas/Je refuse de répondre

16. Laquelle des catégories suivantes décrit le mieux le revenu total de votre ménage? Il s'agit du revenu total combiné de toutes les personnes de votre foyer, avant impôts.

    [LIRE LA LISTE; ARRÊTER LORSQUE LA PERSONNE FOURNIT UNE RÉPONSE]

    01. Moins de 20 000 $
    02. De 20 000 $ à moins de 40 000 $
    03. De 40 000 $ à moins de 60 000 $
    04. De 60 000 $ à moins de 80 000 $
    05. De 80 000 $ à moins de 100 000 $
    06. De 100 000 $ à moins de 150 000 $
    07. 150 000 $ et plus
    08. [NE PAS LIRE] Je refuse de répondre

CONCLUSION

Le sondage est maintenant terminé. Merci beaucoup pour vos précieuses réponses. Nous vous en sommes très reconnaissants.