Gouvernement du Canada | Government of Canada

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

Sommaire

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
Sommaire

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

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).

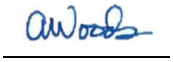
État de préparation en vue d'une cyberattaque

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).