Government of Canada | Gouvernement du Canada

Attitudes towards the Communications Security Establishment – Tracking Study

Executive Summary

Prepared for the Communications Security Establishment

Supplier Name: Phoenix SPI
Contract Number: 2L165-200494-001-CY
Contract Value: $84,978.57
Award Date: 2020-01-09
Delivery Date: 2020-04-30

Registration Number: 063-19
For more information on this report, please contact CSE at: media@cse-cst.gc.ca

Ce rapport est aussi disponible en français.

Canada

Attitudes towards the Communications Security Establishment: Tracking Study Executive Summary

Prepared for the Communications Security Establishment
Supplier name: Phoenix Strategic Perspectives Inc.
April 2020

This public opinion research report presents the results of a telephone survey of 2,505 Canadians, aged 18+, conducted by Phoenix SPI on behalf of the Communications Security Establishment (CSE) between February 11 and March 7, 2020.

Cette publication est aussi disponible en français sous le titre : Attitudes envers le Centre de la sécurité des télécommunications – Étude de suivi.

media@cse-cst.gc.ca

Catalogue number:
D96-16/2020E-PDF

International Standard Book Number (ISBN):
978-0-660-34497-3

Related publications (registration number: POR 063-19):

Catalogue number (Final report, French) D96-16/2020F-PDF
ISBN 978-0-660-34496-6

Executive Summary

Phoenix Strategic Perspectives (Phoenix SPI) was commissioned by the Communications Security Establishment (CSE) to conduct a national telephone survey to inform the Agency's communications strategies.

1. Research Purpose and Objectives

One of CSE's organizational objectives is to work to strengthen the trust and confidence of the public and its stakeholders through the delivery of valuable results, and continued lawfulness and privacy protection. To support this organizational objective, CSE conducted public opinion research in 2017. The 2017 results provide a baseline against which to measure changes over time. The specific objectives of the current research were: 1) track views towards intelligence agencies in Canada and CSE, and 2) explore awareness and views of the Canadian Centre for Cyber Security which launched in October 2018 to consolidate key cyber security operational units within the Government of Canada into a single cyber security centre. The findings from this research will help CSE in its efforts to build and maintain the public trust and will be used to help shape communications strategies.

2. Methodology

A 12-minute random digit dialling (RDD) telephone survey was conducted with 2,505 Canadians, 18 years of age or older, between February 11 and March 7, 2020. Interviewing was conducted using Computer Aided Telephone Interviewing (CATI) technology. Probability sampling was used; as such, the results can be extrapolated to the full population of Canadians aged 18 and older. An overlapping dual-frame (landline and cell phone) sample was used to minimize coverage error. The sample frame was geographically disproportionate so as to improve the accuracy of regional results. The data were weighted to ensure they accurately represent the distribution of the adult Canadian population in terms of age, gender and province/ territory, using Statistics Canada 2016 Census data. Based on a sample of this size, the overall results can be considered accurate to within ±2.2%, 19 times out of 20 (adjusted to reflect the geographically disproportionate sampling).

3. Key Findings

Awareness of CSE

Awareness of CSE is not high, and aided awareness is lower now than it was in 2017.

Very few Canadians are aware on an unaided basis that there is a government agency responsible for intercepting and analyzing foreign communications and helping protect the government's computer networks. Two percent correctly named CSE, while an additional 1% named CSE and the Cyber Centre. In contrast, nearly one-third claimed awareness of CSE on an aided basis (20% indicated that they had *definitely* heard, seen or read something about it, and 11% that they *maybe* had). Top-of-mind, or unaided awareness of CSE remains unchanged from 2017 while aided awareness is lower now than it was in 2017 (31% vs. 37% in 2017).

Perceptions of CSE's Mission and Activities

The majority of Canadians attribute importance to CSE's mission and consider CSE's national security-related activities to be very important, but many are not aware of CSE's specific activities in support of national security.

Over three-quarters of respondents assigned importance to CSE's mission in relation to Canada's national security (51% saying it was *very* important and 27% that it was *somewhat* important). These results differ

slightly from those of 2017, as a result of a smaller proportion assigning moderate importance to the CSE's mission.

The vast majority of respondents assigned importance to each of five CSE activities related to national security, with half or more rating all of these activities as *very* important. Leading the way was protecting Canada's computer networks (97% assigning this importance, and 82% rating it as *very* important). Almost as many assigned importance to actively defending networks in Canada (94%) and disrupting foreign cyber threats (93%), with three-quarters assigning strong importance to each of these activities. Finally, 89% assigned importance to assisting law enforcement and security agencies and 88% assigned importance to gathering foreign intelligence (over half assigning strong importance to each).

When it came to awareness of CSE activities, nearly one-quarter said that they are aware that CSE supports CAF missions (24%) and that CSE may assist domestic security agencies (23%). Fourteen percent said they are aware CSE is prohibited from targeting Canadians or anyone in Canada, while only 8% said they are aware that CSE blocks more than 2 billion malicious cyber attempts a day.

Trust in CSE

Trust in CSE to act ethically and legally in fulfilling its mandate has declined since 2017.

Nearly two-thirds of Canadians trust CSE 'somewhat' (49%) or 'completely' (15%) to act ethically and legally. Trust of the CSE in this regard has declined over time (64% vs. 73% in 2017) while the level of distrust remains unchanged. The proportion who said they have no opinion has increased (24% vs. 15% in 2017).

Views on National Security

The proportion of Canadians who think Canada is more dangerous now than five years ago has increased since 2017.

Asked if they feel that Canada is safer, more dangerous, or about the same compared to five years ago, approximately one in 10 (11%) said Canada is safer and one-third (33%) said Canada is more dangerous. The rest (51%) feel that, overall, Canada is about the same as it was five years ago. The proportion of respondents who feel Canada is safer has declined slightly over time (11% vs. 15% in 2017), while the proportion who feel it is more dangerous has increased (33% vs. 25% in 2017).

Balancing Security and Civil Liberties

Seven in 10 Canadians agree that if steps are not taken to secure computers and the Internet, Canada will be at greater risk of terrorist attack.

Using a 7-point scale, respondents expressed their level of agreement or disagreement with a set of statements about balancing security with civil liberties. The only statement to elicit some degree of agreement from a majority was "If we don't take steps to ensure the security of our computers and of the Internet, we will be at greater risk of terrorist attack". Seventy-two percent agreed that Canada will face a greater risk of terrorist attack if steps are not taken.

Nearly half expressed some degree of agreement that "Canadian intelligence agencies act within the law when they collect information about Canadians" (49%) and "I can trust the Government of Canada to strike the right balance between security and civil liberties" (49%), while slightly fewer (45%) agreed with the statement "I am concerned about information that government intelligence agencies may be collecting about me".

Respondents were least likely to agree that "Police and intelligence agencies should have more powers to ensure security even if it means Canadians have to give up some personal privacy safeguards". Four in 10

(41%) agreed with the trade off – giving up some privacy safeguards for security – while more than one-third (36%) disagreed, including 18% who *strongly* disagreed.

Compared to 2017, the most notable difference has been a decrease in the level of agreement that "I can trust the Government of Canada to strike the right balance between security and civil liberties" (49% vs. 55% in 2017).

Awareness and Perceptions of the Cyber Centre

Limited awareness of the Cyber Centre, but majorities believe the centre's activities are having at least a moderate impact on Canada.

More than nine in 10 (94%) respondents could not name the organization that is part of CSE with primary responsibility for providing advice, guidance, services, and support on cyber security. Only 2% correctly named the Canadian Centre for Cyber Security/Cyber Centre. Aided awareness of the Cyber Centre was somewhat higher. When asked if they had heard, seen, or read anything about the Canadian Centre for Cyber Security or Cyber Centre, 16% said they had *maybe* or *definitely* heard, seen, or read anything about it. The large majority (83%) said they had not.

Respondents rated the impact of various Cyber Centre activities on Canada using another 7-point scale. Leading the way in terms of perceived impact (scores of 5 or more) was defending Canada's cyber systems (76%), followed by protecting cyber security interests by working with partners (73%), developing and sharing cyber defense technologies and tools (69%), and informing Canada/Canadians about cyber security matters and providing leadership during cyber security events (68% each).

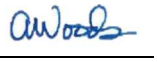
Preparedness for a Cyberattack

SMEs and individual Canadians more likely to be judged as unprepared for a cyberattack.

Finally, respondents were asked how well prepared they think various actors/institutions are to meet the threat of a cyberattack. In response, a majority judged most of them to be prepared to meet the threat, but the size of the majority varied, and respondents were much more likely to view them as 'somewhat' as opposed to 'very well' prepared. The Canadian government was most likely to be seen as at least somewhat prepared in this regard (69%), followed by large businesses or enterprises (65%), critical infrastructure operators (61%), and the electoral systems across Canada (56%). By comparison, nearly two-thirds felt that small to medium businesses were somewhat (36%) or very (27%) unprepared for this, while just over three-quarters felt that individual Canadians were somewhat (33%) or very (43%) unprepared for a cyberattack.

4. Political Neutrality Certification

I hereby certify as a Senior Officer of Phoenix Strategic Perspectives that the deliverables fully comply with the Government of Canada political neutrality requirements outlined in the Policy on Communications and Federal Identity of the Government of Canada and Procedures for Planning and Contracting Public Opinion Research. Specifically, the deliverables do not contain any reference to electoral voting intentions, political party preferences, standings with the electorate, or ratings of the performance of a political party or its leader.



Alethea Woods
President
Phoenix SPI

5. Contract Value

The contract value was $84,978.57 (including HST).