Government of Canada | Gouvernement du Canada

Attitudes towards the Communications Security Establishment – Tracking Study

Final Report

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
Final Report

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

Table of Contents

Table of Figures

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).

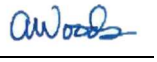
Preparedness for a Cyberattack

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).

Introduction

Phoenix Strategic Perspectives (Phoenix SPI) is pleased to provide the Communications Security Establishment (CSE) with this research report outlining the results of a national quantitative public opinion research study undertaken to inform the Agency's communications strategies.

1. Background and Objectives

CSE is Canada's national cryptologic agency. Unique within Canada's security and intelligence community, CSE employs code-makers and code-breakers to provide the Government of Canada with information technology security (IT Security) and foreign signals intelligence (SIGINT) services. CSE also provides technical and operational assistance to federal law enforcement and security agencies.

CSE's mandate and authorities are defined in the *Communications Security Establishment Act* (Part 3 of Bill C-59: An Act respecting national security matter) which authorizes CSE:

1. to acquire, covertly or otherwise, information from or through the global information infrastructure, including by engaging or interacting with foreign entities located outside Canada or by using any other method of acquiring information, and to use, analyze and disseminate the information for the purpose of providing foreign intelligence, in accordance with the Government of Canada's intelligence priorities.
2. to provide advice, guidance and services to help protect federal institutions' electronic information and information infrastructures; and electronic information and information infrastructures designated under subsection 21(1) as being of importance to the Government of Canada; and to acquire, use and analyze information from the global information infrastructure or from other sources in order to provide such advice, guidance and services.
3. to carry out activities on or through the global information infrastructure to help protect
    a) federal institutions' electronic information and information infrastructures; and
    b) electronic information and information infrastructures designated under subsection 21(1) as being of importance to the Government of Canada.
4. to carry out activities on or through the global information infrastructure to degrade, disrupt, influence, respond to or interfere with the capabilities, intentions or activities of a foreign individual, state, organization or terrorist group as they relate to international affairs, defence or security.
5. to provide technical and operational assistance to federal law enforcement and security agencies, the Canadian Forces and the Department of National Defence.

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 to communicate.

2. Methodology

A 12-minute random digit dialling (RDD) telephone survey was administered to 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. 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. 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). The margin of error is greater for results pertaining to subgroups of the total sample. More information on the methodology can be found in the Appendix of this report: Technical Specifications of Research.

3. Notes to Readers

- All results are expressed as percentages unless otherwise noted.
- Percentages may not always add to 100 due to rounding.
- Demographic differences are identified in the report. Only differences that are significant at the 95% confidence level and pertain to a sub-group sample size of more than n=30 are discussed in the report.
- The tabulated data is available under separate cover.

Detailed Findings

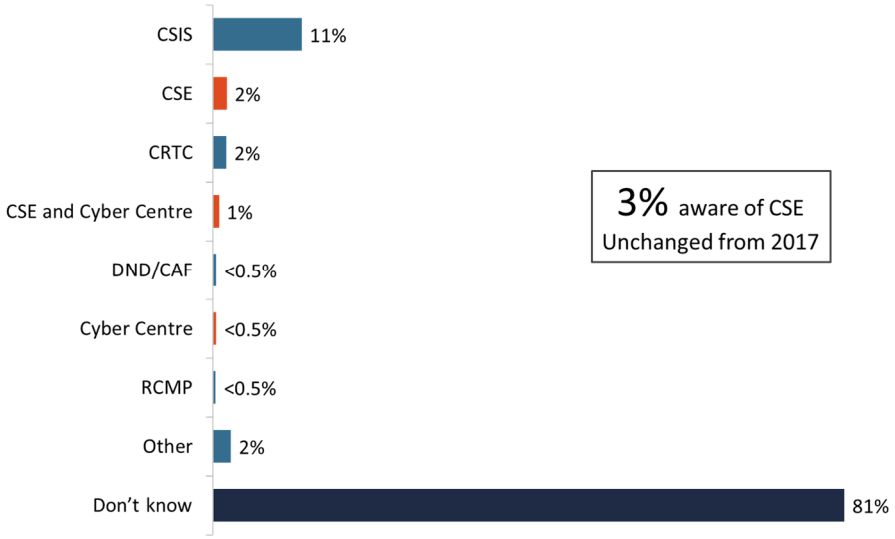
1. Awareness of CSE

Low unaided awareness of CSE

Asked if they were aware that there is a government agency responsible for intercepting and analyzing foreign communications and helping protect the government's computer networks, a large majority (81%) of Canadians indicated that they could not identify such an agency. As the accompanying graph shows, the only agency identified with any frequency was the Canadian Security Intelligence Service (CSIS) (11%). Only three percent identified CSE (2% naming CSE, and 1% naming CSE and the Cyber Centre).

Results are unchanged compared to 2017.

Figure 1: Unaided Awareness of CSE



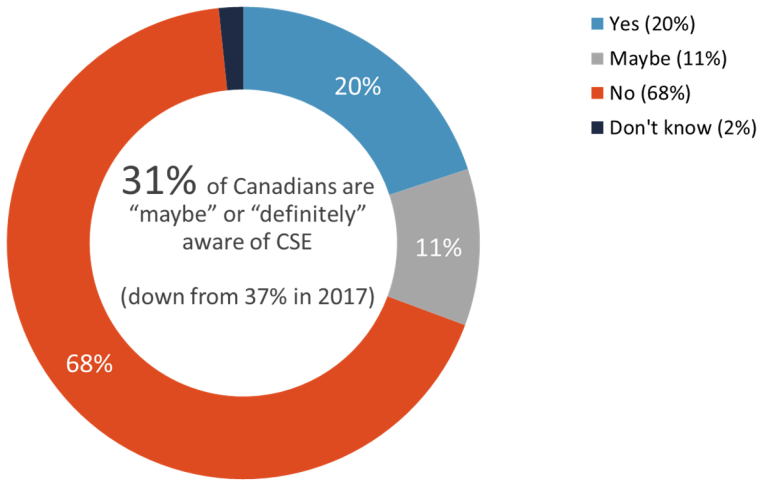
Base: n=2,505; all respondents
Q1. As you may be aware, there is a government agency that is responsible for intercepting and analyzing foreign communications and helping protect the government's computer networks. Can you name this agency?

Roughly three in 10 aware of CSE

After being informed that the government agency responsible for intercepting and analyzing foreign communications and helping protect the government's computer networks is the Communications Security Establishment, respondents were asked if they had ever heard, seen or read anything about CSE. In response, just over two-thirds (68%) of Canadians said they had not. One in five (20%) indicated that they *definitely* had, while approximately one in 10 (11%) indicated that they *maybe* had heard, seen or read about CSE.

Aided awareness has decreased over time (31% vs. 37% in 2017).

Figure 2: Aided Awareness of CSE



Base: n=2,505; all respondents
Q4. Would you say that you have ever heard, seen or read anything about the Communications Security Establishment, or CSE?

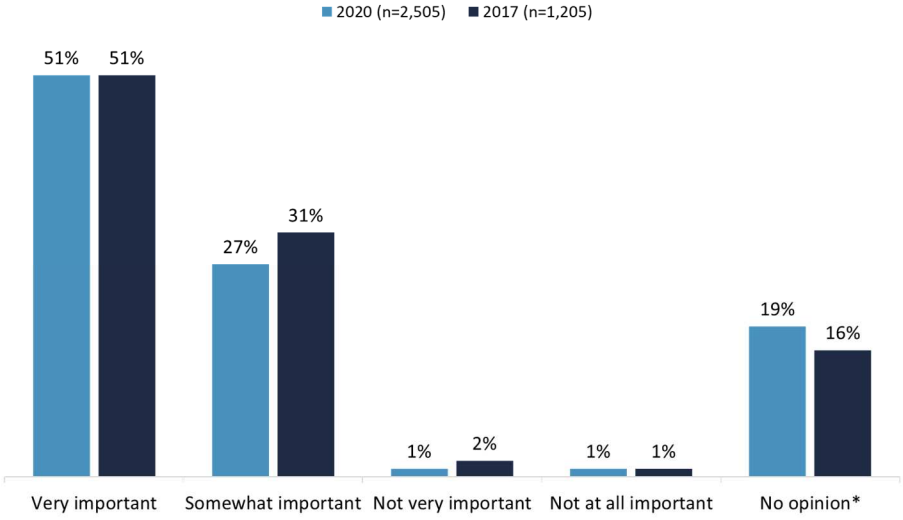
Definite awareness of the CSE *on an aided basis* was higher among men (23% vs. 17% of women) and among those with more formal education (24% of those with a university degree vs. 14% of those with a high school diploma or less). Definite awareness *on an aided basis* also increased with age (from 16% of 18-34 year olds to 23% of those 55 and older), and regionally it ranged from a high of 25% in British Columbia to a low of 15% in Quebec.

2. Perceptions of CSE's Mission and Activities

Half rate CSE's mission as very important to national security

Over three-quarters of Canadians assigned importance to CSE's mission in relation to Canada's national security: 51% said CSE's mission is very important and 27% said it is somewhat important to Canada's national security. These results differ slightly from those of 2017, as a result of a smaller proportion assigning moderate importance to the CSE's mission.

Figure 3: Importance of CSE's Mission to National Security



Q5. Would you say that the Communications Security Establishment's mission is very important, somewhat important, not very important or not at all important to Canada's national security? *Includes "don't know" responses.

Attributions of importance to CSE's mission were more likely among older than younger Canadians (81% of those 55 and older vs. 74% of 18-34 year olds), and among those with a university degree (83% vs. 78% of those with college or trade-related education, and 73% of those with a high school diploma or less).

Nearly everyone assigned importance to protecting Canada's computer networks but disrupting foreign cyber threats viewed as most important

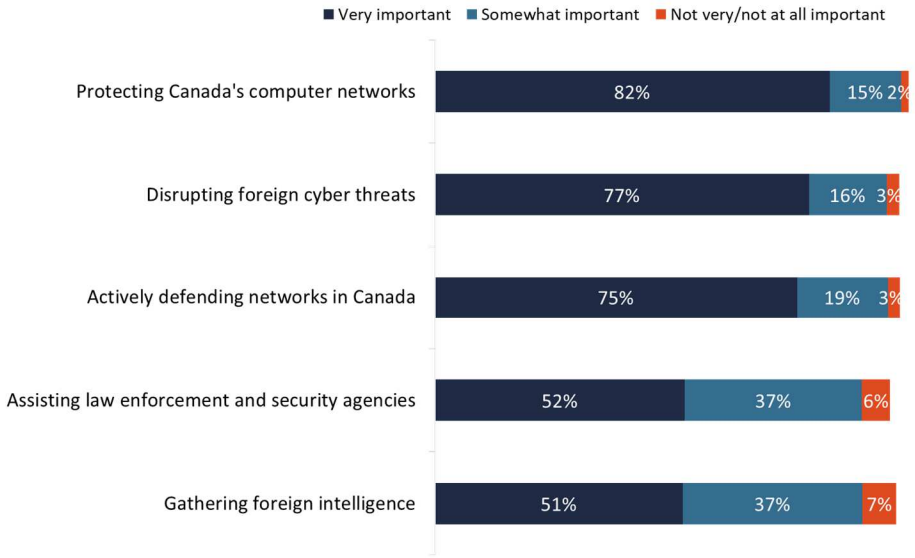
Respondents were asked to rate the importance of the following CSE's activities related to national security:

- Gathering foreign intelligence which involves intercepting and analyzing foreign communications
- Protecting the computer networks that are important to the country from cyber-attacks
- Assisting law enforcement and security agencies by helping collect and analyze communications
- Actively defending networks in Canada from foreign cyber threats
- Disrupting foreign cyber threats before they affect Canada or Canadians

The vast majority of Canadians assigned importance to each of these CSE activities, with half or more rating all of these activities as *very* important. Leading the way was protecting Canada's computer networks, with nearly everyone (97%) assigning this importance, including 82% who rated 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).

Figure 4: Importance of CSE's Activities to National Security



Base: n=2,505; all respondents
Q6. Now, I will read a list of the main things that the Communications Security Establishment, or CSE, does. For each, I would like to know if you think it is very important, somewhat important, not very important or not at all important to Canada's national security?

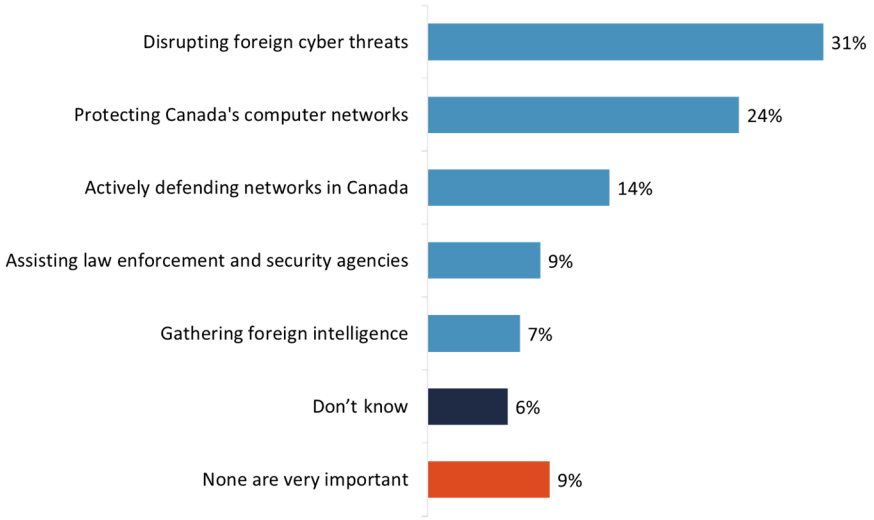
Sub-group variations regarding the perceived importance of these activities were limited, and included the following:

- Disrupting foreign cyber threats was more likely to be considered somewhat or very important among Canadians over 35 years of age (95% vs. 91% of those aged 18-35).

- Gathering foreign intelligence was more likely to be considered somewhat or very important among older than younger Canadians (90% of those 55 and older vs. 85% of those aged 18-34). The perceived importance of this also increased with education (from 85% of those with a high school diploma or less to 91% of those with a university degree).

More than eight in 10 (85%) Canadians said at least one of these CSE activities is very important to Canada's national security. To understand the relative importance of these activities, respondents were asked to select the most important activity from among the activities they rated as *very* important. Three in 10 (31%) identified disrupting foreign cyber threats as the most important activity, while nearly one-quarter (24%) said that protecting Canada's computer networks was most important. Following this, in descending order, came actively defending networks in Canada (14%), assisting law enforcement and security agencies (9%), and gathering foreign intelligence (7%).

Figure 5: Most Important CSE Activity vis-à-vis National Security



Base: n=2,505; all respondents
Q7. Which one of the following activities is most important when it comes to Canada's national security?

The following sub-group variations were notable:

- Disrupting foreign cyber threats was more likely to be considered most important among younger Canadians (37% of 18-34 year olds vs. 26% of 35-54 year olds).

- Protecting computer networks was more likely to be considered most important in Quebec (31% vs. 19% to 24% of Canadians residing elsewhere in the country) and among those with a university degree than among those with a high school diploma or less (27% vs. 21%).

- Actively defending networks in Canada from foreign cyber threats was more likely to be considered most important among 35-54 year olds (17% vs. 12% of 18-34 year olds, and 13% of those aged 55 and older), and in Alberta (18%) and Ontario (17%) than in Quebec (11%) and British Columbia (11%).

- Gathering foreign intelligence was more likely to be considered most important by older Canadians (9% of those aged 55 and older vs. 5% of 18-34 year olds).

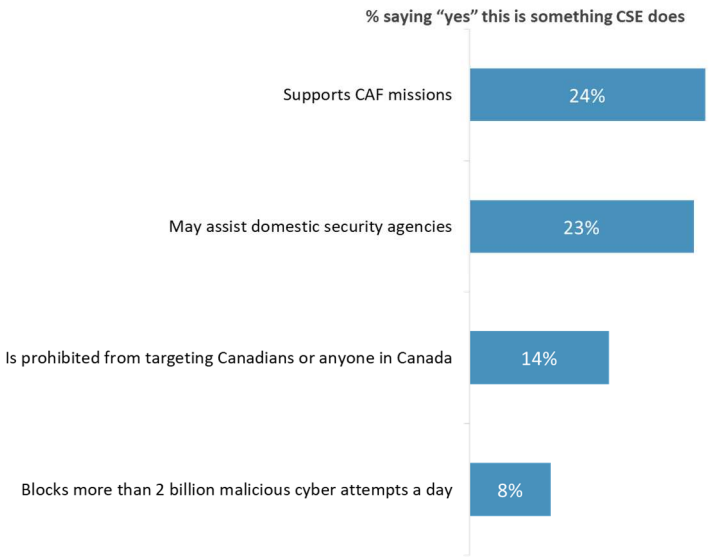
Low knowledge of CSE's mandate

Respondents were asked if they were aware of the following activities in relation to the CSE:

- CSE is prohibited by law from targeting Canadians anywhere, or anyone in Canada.
- CSE may assist domestic security agencies.
- Across the government, CSE blocks more than two billion malicious cyber attempts a day.
- CSE supports Canadian Armed Forces missions, including in cases of Canadians kidnapped abroad.

Less than one-quarter of Canadians are aware of any of these 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'.

Figure 6: Knowledge of CSE's Mandate



Base: n=2,505; all respondents
Q8. Are you aware that.... Don't know: range from 3% to 4%

Men were more likely to claim to be aware that CSE is prohibited by law from targeting Canadians anywhere, or anyone in Canada (17% vs. 12% of women), and that CSE may assist domestic security agencies (27% vs. 19% of women).

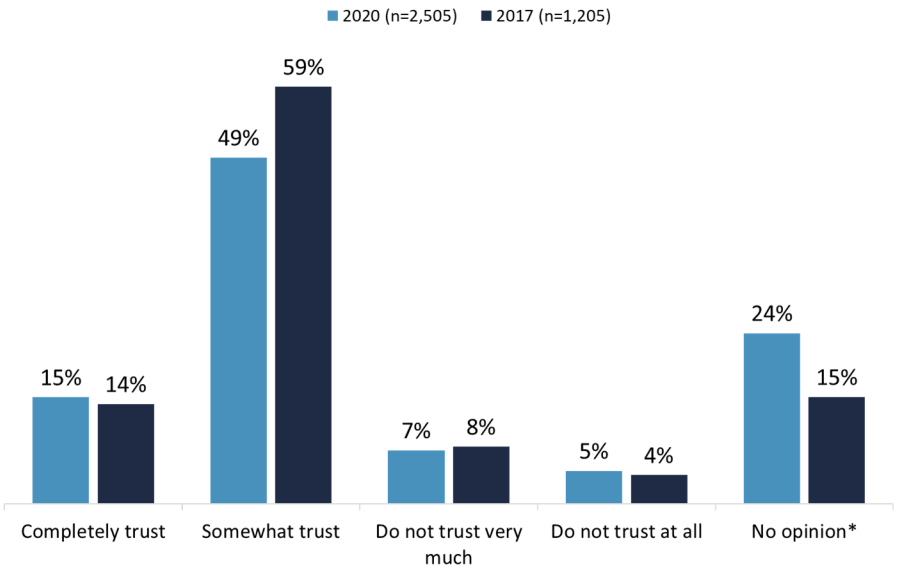
3. Trust in CSE

Almost two-thirds trust CSE to act ethically and legally

Nearly two-thirds of Canadians 'somewhat' (49%) or 'completely' (15%) trust CSE to act ethically and legally. Conversely, 12% do not trust CSE 'at all' or 'very much'. Nearly one-quarter (24%) said they had no opinion on this.

Trust of 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 over time (24% vs. 15% in 2017).

Figure 7: Trust in CSE: 2020 vs. 2017



Q9. To what extent would you say that you trust the Communications Security Establishment to act both ethically and legally in fulfilling its mandate? *Includes "don't know" responses.

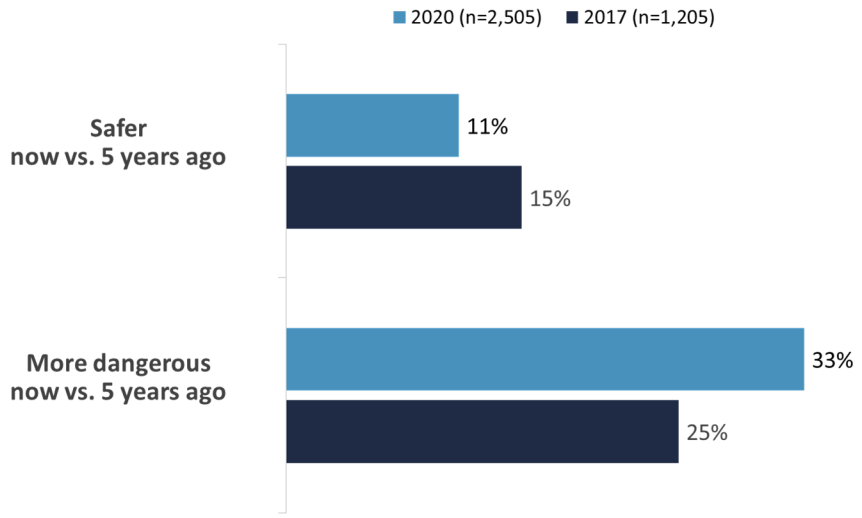
Trust that CSE would act ethically and legally at least to some extent was higher among those with a university degree (68%) than those with a high school diploma or less (58%). Distrust of CSE in this regard was higher among men (16% vs. 9% of women).

4. Views on National Security

Roughly one in 10 feel Canada is safer now than five years ago

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, a majority at 51%, feel that, overall, Canada is about the same as it was five years ago. The proportion of Canadians who feel Canada is safer has declined slightly (11% vs. 15% in 2017), while the proportion who feel Canada is more dangerous has increased over time (33% vs. 25% in 2017).

Figure 8: Perceptions of Canada's Safety: 2020 vs. 2017



Q2. From your point of view, do you feel that – overall – Canada is safer, more dangerous or about the same as it was five years ago?

The perception that Canada is safer now than it was five years ago declines with age (from 17% of 18-34 year olds to 8% of those 55 and older), and ranges from 13% in Ontario to 8% in Alberta. The perception that Canada is more dangerous increases with age (from 26% of 18-34 year olds to 38% of those 55 and older), and is highest in Ontario (41%) and the Prairies (40%), and lowest in Quebec (20%).

5. Balancing Security and Civil Liberties

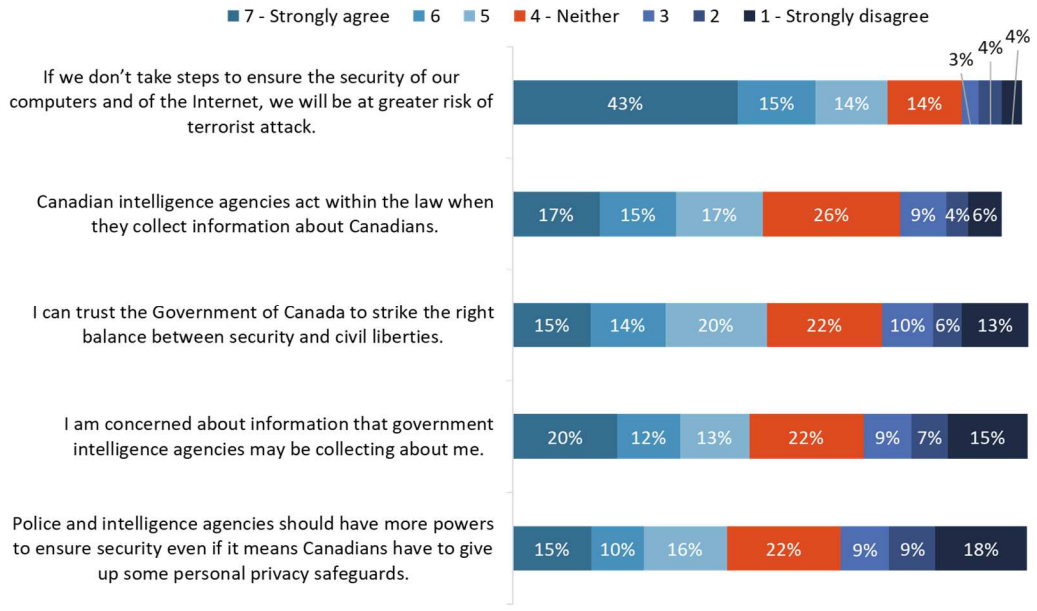
Roughly half agree with all balancing security with civil liberties statements

Using a 7-point scale where 1 means 'strongly disagree', 7 means 'strongly agree', and 4 means 'neither agree nor disagree', respondents were asked to express their level of agreement of disagreement with the following statements about balancing security with civil liberties:

- I can trust the Government of Canada to strike the right balance between security and civil liberties.
- Police and intelligence agencies should have more powers to ensure security even if it means Canadians have to give up some personal privacy safeguards.
- Canadian intelligence agencies act within the law when they collect information about Canadians.
- I am concerned about information that government intelligence agencies may be collecting about me.
- 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.

While respondents were more likely to agree than disagree with each of these statements, the level of agreement varied. The statement most likely to elicit agreement, and the only one to elicit agreement from a majority of respondents, 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". Nearly three-quarters (72%) agreed with this statement to some degree, including 43% who *strongly* agreed.

Figure 9: Balancing Security with Civil Liberties



Base: n=2,505; all respondents
Q3. To what extent do you agree or disagree with each of the following statements

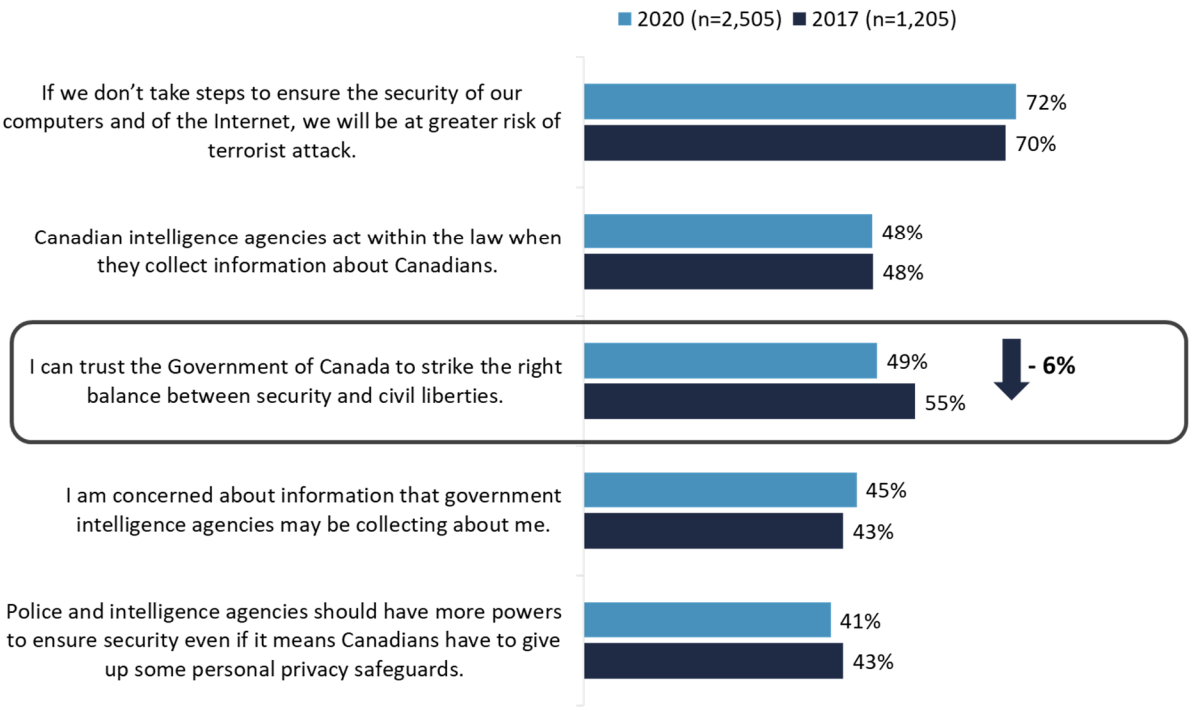
Nearly half expressed some degree of agreement that "Canadian intelligence agencies act within the law when they collect information about Canadians" (49%) and "I can trust the Government of Canada to

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 in perceptions is that fewer Canadians feel they trust the Government of Canada to strike the right balance between security and civil liberties (49% vs. 55% in 2017).

Figure 10: Balancing Security with Civil Liberties: 2020 vs. 2017



Q3. To what extent do you agree or disagree with each of the following statements.

The following subgroup differences in relation to these statements are noteworthy:

- Agreement that not taking steps to ensure the security of our computers and of the Internet will result in greater risk of terrorist attack was more likely among older than younger Canadians (75% of respondents 55 and older vs. 67% of 18-34 year olds).

- Agreement that the Government of Canada can be trusted to strike the right balance between security and civil liberties was more likely among women (52% vs. 45% of men), and among those with a university degree (56% vs. 44% of those with less formal education).

- Agreement 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 was more likely among women (44% vs. 38% of men), and among Canadians 35 and older (46% vs. 28% of 18-34 year olds).

- Concern about personal information that government intelligence agencies may be collecting was more likely in Quebec (51%) than in the Prairies (42%), Alberta (41%), and B.C. (41%). Conversely, lack of concern about this was more likely among those with a university degree (35%) than those with a high school diploma or less (25%).

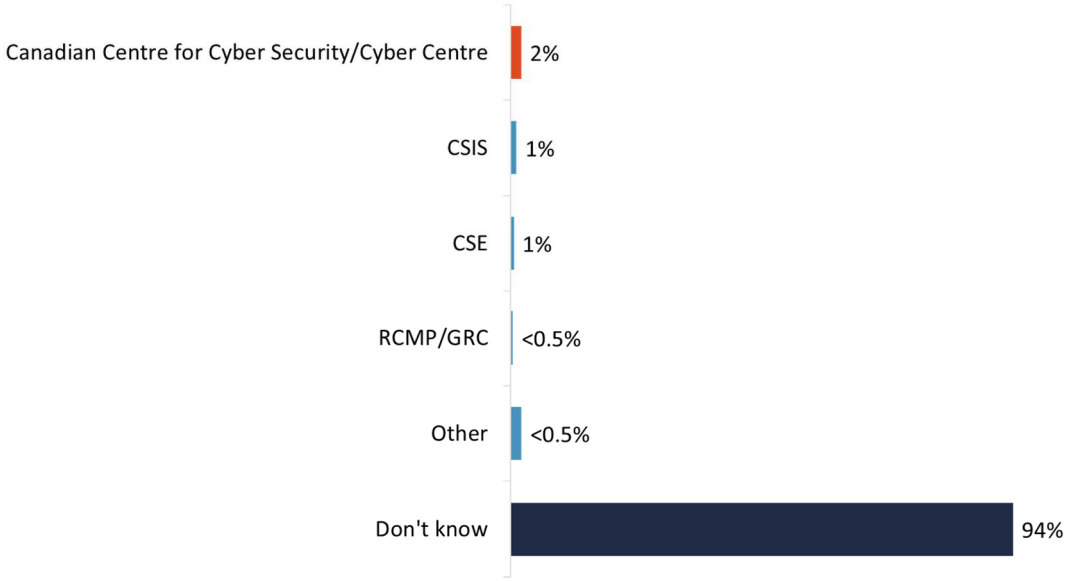
- Finally, disagreement that Canadian intelligence agencies act within the law when they collect information about Canadians was most likely among Canadians under 35 years of age (25% vs. 17% of respondents 35 and older). Disagreement was also more likely in Alberta (25%) and the Prairies (24%) than in Quebec (16%).

6. Awareness and Perceptions of the Cyber Centre

Virtually no unaided awareness of Cyber Centre

When respondents were asked to name the organization that is part of CSE with primary responsibility for providing advice, guidance, services, and support on cyber security, more than nine in 10 (94%) said they did not know the name of this organization. Only 2% correctly named the Canadian Centre for Cyber Security or the Cyber Centre.

Figure 11: Unaided Awareness of the Cyber Centre



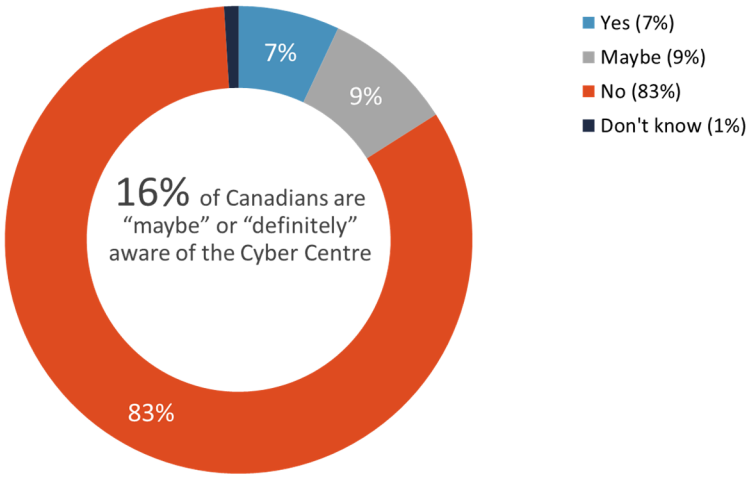
Base: n=2,505; all respondents
Q10. There is an agency that is part of the Communications Security Establishment, or CSE, with primary responsibility for providing advice, guidance, services and support on cyber security. Can you name this organization?

Most not aware of Cyber Centre

When respondents were asked directly if they had heard, seen, or read anything about the Canadian Centre for Cyber Security or Cyber Centre, the large majority (83%) said they had not. Only 16% said they had *maybe* or *definitely* heard, seen, or read anything about the Cyber Centre - 9% saying *maybe* and 7% saying *yes*. These results were in response to the following question:

> The Canadian Centre for Cyber Security, or Cyber Centre, launched in 2018. Uniting operational cyber security expertise from several units within the Government of Canada, the Cyber Centre is a key source of advice, guidance, services and support on cyber security for government, the private sector and the Canadian public. Have you heard, seen or read anything about the Canadian Centre for Cyber Security, or Cyber Centre?

Figure 12: Aided Awareness of the Cyber Centre



Base: n=2,505; all respondents
Q11. Have you heard, seen or read anything about the Canadian Centre for Cyber Security, or Cyber Centre?

At least one-third perceive Cyber Centre's activities as high impact on Canada

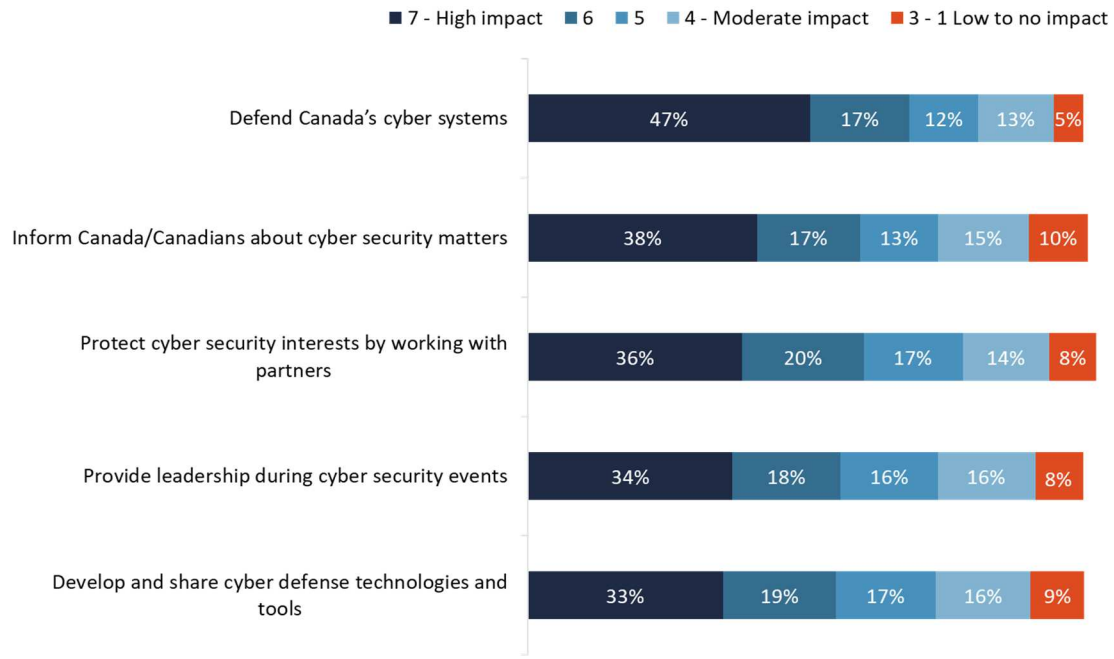
Respondents were read a list of Cyber Centre activities and asked to rate how much of an impact they think those activities have on Canada using a 7-point scale, where 1 means "no impact," 7 means "high impact," and 4 means "moderate impact. The list of activities included the following:

- Inform Canada and Canadians about cyber security matters.
- Protect our cyber security interests by working with business and government partners.
- Develop and share cyber defense technologies and tools.
- Defend Canada's cyber systems.
- Provide leadership during cyber security events.

Over two-thirds of Canadians attributed scores of 5 or more to each of these activities, indicating that, in their minds, each activity has a more than moderate impact on Canada. Moreover, at least one-third rated each activity as having a high impact.

The top rated activity 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).

Figure 13: Perceived Impact of the Cyber Centre's Activities on Canada



Base: n=2,505; all respondents
Q12. Now I will read a list of the main things that the Cyber Centre does, and for each one, I'd like you to tell me how much of an impact you think the activity has, or will have, on Canada.

The following sub-group variations were notable:

- The following were more likely to attribute a noticeable impact (scores of 5 or more) to informing Canada and Canadians about cyber security matters: younger respondents compared to older ones (74% of 18-34 year olds vs. 65% of those aged 55 and older), respondents with more formal education compared to those with less (77% of those with a university degree vs. 64% of those with a high school diploma or less), and respondents in Ontario and Quebec (71% each) compared to respondents in B.C. (63%).
- Respondents with more formal education were more likely than those with less formal education to attribute a noticeable impact to protecting our cyber security interests by working with business and government partners (77% of those with a university degree vs. 68% of those with a high school degree or less). Regionally, respondents in Quebec were most likely to attribute an impact to this activity (77%) while those in B.C. were least likely to (65%).
- The likelihood of attributing a noticeable impact to developing and sharing cyber defense technologies and tools increased with education (from 61% of those with a high school degree or less to 74% of those with a university degree), decreased with age (from 75% of 18-34 year olds to 64% of those aged 55 and older), and was highest in Quebec (76% vs. 62-68% elsewhere).
- The following were more likely to attribute a noticeable impact to defending Canada's cyber systems: those with a university degree (79% vs. 73% of those with college or trade-related education and 74% of those with a high school diploma or less) and those 54 and younger (79% of 18-34 year olds and 77% of 35-54 year olds vs. 72% of those aged 55 and older).
- The likelihood of attributing a noticeable impact to providing leadership during cyber security events increased with education (from 61% of those with a high school diploma or less to 74% of those with a university degree), and ranged regionally from 73% in Quebec to 62% in B.C.

7. Preparedness for a Cyberattack

Canadian government perceived as most prepared to meet threat of cyberattack

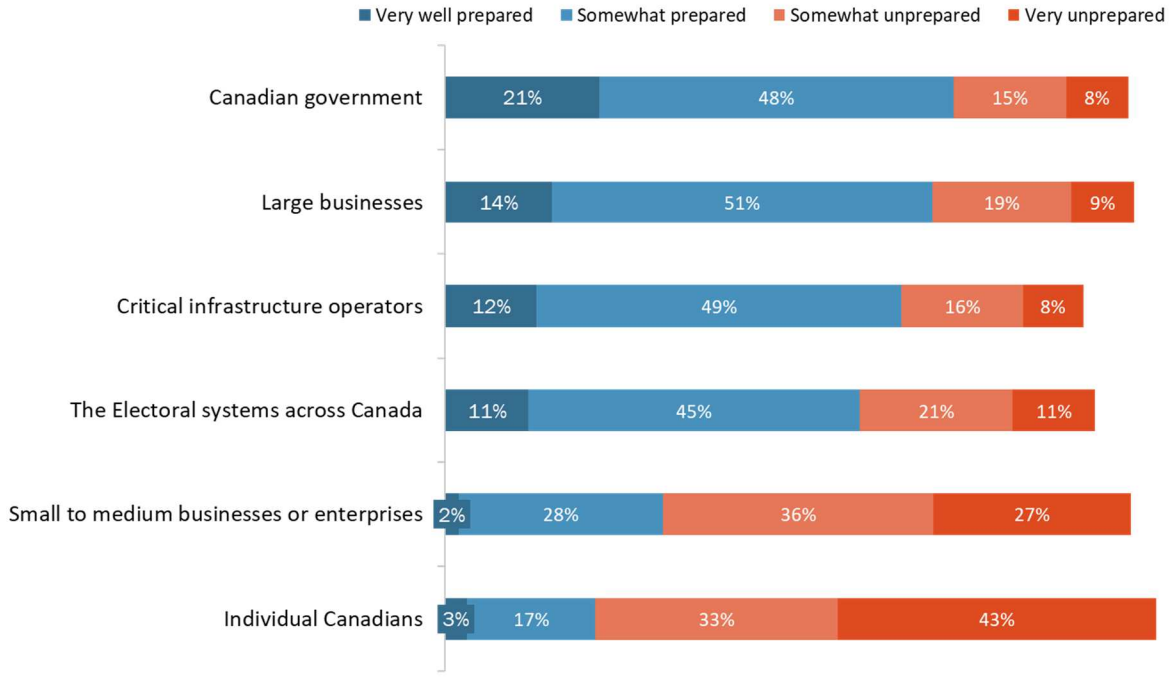
Finally, respondents were asked how well prepared they think each of the following are to meet the threat of a cyberattack:

- The Canadian government
- The Electoral systems across Canada
- Individual Canadians
- Large businesses or enterprises
- Small to medium businesses or enterprises
- Critical infrastructure operators

A majority of respondents judged that most of these are at least somewhat prepared to meet the threat of a cyberattack. That said, the size of the majority varied, and respondents were much more likely to view them as 'somewhat' as opposed to 'very well' prepared. Indeed, no more than one in five (21%) judged any of these as very well prepared to meet a cyberattack.

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, only 30% said small to medium businesses or enterprises are prepared to meet the threat of a cyberattack, and only one in five (20%) felt that individual Canadians are prepared for this. Nearly two-thirds felt that small to medium businesses were somewhat (36%) or very unprepared (27%), while just over three-quarters felt that individual Canadians were somewhat (33%) or very unprepared (43%).

Figure 14: Preparedness of Different Entities to Meet the Threat of a Cyberattack



Base: n=2,505; all respondents
Q13. In your opinion, how well prepared do you think each of the following are to meet the threat of a cyberattack? Would you say [INSERT LIST ITEM] [IS/ARE] very well prepared, somewhat prepared, somewhat unprepared or very unprepared to face a cyber threat?

Impressions that the Canadian government is prepared to meet the threat of a cyberattack declined with age (from 78% of 18-34 year olds to 63% of those aged 55 and older), as did such perceptions regarding the electoral system (from 65% of 18-34 year olds to 51% of those aged 55 and older), and critical infrastructure operators (from 67% of 18-34 year olds to 58% of those aged 55 and older). Impressions that large businesses are prepared for this was more likely among 18-34 year olds (72%) and 35-54 year olds (70%) than among those aged 55 and older (58%).

Impressions that individual Canadians are unprepared to meet the threat of a cyberattack were more likely among the following:

- 35-54 year olds (80% vs. 73% of 18-34 year olds and 75% of those aged 55 and older);
- those with college or trade-related education (80%) and a university degree (79%) compared to those with a high school diploma or less (66%).

Finally, respondents in Quebec were most likely think that the following were unprepared to meet the threat of a cyberattack: the Canadian government, large business and enterprises, small to medium businesses or enterprises, and critical infrastructure operators.

Appendices

1. Technical Specifications

The following specifications applied to this survey:

- A 12-minute random digit dialling (RDD) telephone survey was administered to 2,505 Canadians, 18 years of age or older.
- Probability sampling was used; as such, the results can be extrapolated to the full population of Canadians aged 18 and older.
- Interviewing was conducted by Elemental Data Collection Inc. (EDCI) using Computer Aided Telephone Interviewing (CATI) technology.
- Following survey best practices, the questionnaire was pre-tested in advance of the fieldwork to ensure that it measured what it was intended to measure.
    - Respondents had the choice of participating in the official language of their choice.
    - The pre-test interviews were digitally recorded and reviewed by Phoenix SPI team members.
    - There were 10 completions in each official language.
    - Overall, the questionnaire worked well. There were no significant problems in terms of design or respondents' comprehension of the questions. The only issue was the questionnaire length; it was too long. As a result, the sample size was reduced to accommodate the longer interview.
- An overlapping dual-frame (landline and cell phone) sample was used to minimize coverage error. In total, 1,721 interviews (or 69% of the total) were completed with the landline sample and 784 interviews (or 31% of the total) were completed with the cell phone sample.
    - All survey participants were informed that their participation is voluntary, and that information collected is protected under the authority of the *Privacy Act*.
    - Calling was conducted at different times of the day and the week to maximize the opportunity to establish contact.
    - A minimum of eight call-backs were attempted to reach potential respondents in the landline sample before a sample record was retired. A minimum of five call-backs were attempted to reach potential respondents in the cell sample before a sample record was retired.
- The sample frame was geographically disproportionate to improve the accuracy of provincial results. The distribution of completed surveys was as follows:

Strata	Completed Interviews
Newfoundland and Labrador	150
Prince Edward Island	150
Nova Scotia	150
New Brunswick	150
Quebec	450
Ontario	600
Manitoba	175
Saskatchewan	178
Alberta	225

British Columbia	272
Territories	5

- The sample of 2,505 Canadians can be considered accurate to within ±2.2%, 19 times out of 20 (adjusted to reflect the geographically disproportionate sampling).
- The fieldwork took place between February 11 and March 7, 2020.
- The overall response rate[1] was 7% (9% for the landline sample and 4% for the cell phone sample). The table below presents information about the final call dispositions for this survey broken out by sample type.

	Total	Landline	Cell
Total Numbers Attempted	**104,396**	**32,963**	**71,433**
Out-of-scope - Invalid	**62,639**	**12,661**	**49,978**
Unresolved (U)	**26,404**	**11,993**	**14,411**
No answer/Answering machine	26,404	11,993	14,411
In-scope - Non-responding (IS)	**1,392**	**548**	**844**
Language barrier	457	285	172
Incapable of completing (ill/deceased)	119	67	52
Callback (respondent not available)	2,060	799	1,261
Refusal	9,586	5,071	4,515
Termination	418	265	153
In-scope - Responding units (R)	**12,640**	**6,487**	**6,153**
Quota Full	16	15	1
Completed Interview	2,505	1,721	784
Not Qualified – Refused to provide province	35	25	10
Not Qualified – Industry exclusions	111	61	50
Not Qualified – Age	46	0	46

- The survey data have been weighted by region, age and gender using population figures from Statistics Canada's 2016 census data.
- The potential for non-response bias was assessed by comparing the characteristics of respondents through unweighted and weighted data. As is typically the case for general population telephone surveys, older Canadians (those aged 55 and older) were overrepresented in the final survey sample and younger Canadians (those under 35 years of age) were underrepresented. This was corrected with weighting.

[1] The response rate formula is as follows: [R=R/(U+IS+R)]. This means that the response rate is calculated as the number of responding units [R] divided by the number of unresolved [U] numbers plus in-scope [IS] non-responding households and individuals plus responding units [R].

2. Survey questionnaire

INTRODUCTION

Hello/Bonjour, my name is [Interviewer's name]. I'm calling from Phoenix SPI on behalf of the Government of Canada to conduct a survey on issues of interest to Canadians. Would you prefer to continue in English or French? / Préférez-vous continuer en français ou en anglais?

INTERVIEWER NOTE: If the respondent prefers to respond in French, the interviewer must be able to either proceed with the interview in French or read the following statement: "Je vous remercie. Quelqu'un vous rappellera bientôt pour mener le sondage en français."

The survey takes about 7 minutes and is voluntary. Your responses will be kept entirely confidential and anonymous.

[LANDLINE SAMPLE]

A. We would like to speak to the person in your household, 18 years of age or older, who has had the most recent birthday. Would that be you?

*[INTERVIEWER: IF NEEDED: We choose telephone numbers at random and then select one person from each household to be interviewed.]

01. Yes	GO TO SCR. 1
02. No	ASK TO SPEAK TO ELIGIBLE PERSON; REPEAT INTRODUCTION

[CELL SAMPLE]

B. Are you 18 years of age or older?

01. Yes	CONTINUE
02. No	THANK/DISCONTINUE

C. Are you in a place where you can safely talk on the phone and answer my questions?

01. Yes	GO TO SCR. 1
02. No	ASK D

D. We would like to conduct this interview with you when it is safe and convenient to do so. When would it be more convenient for me to call back?

SCHEDULE CALL-BACK IF POSSIBLE (TIME/DAY): _____

SCREENING QUESTIONS

[EVERYONE]

SCR. 1 Do you work in any of the following areas? [READ LIST]

01. Advertising or Market Research or Public Relations

02. The media (i.e. TV, radio, newspapers)
03. Cybersecurity

THANK/DISCONTINUE IF ANY OF THE ABOVE
TERMINATE IF "DON'T KNOW" OR "REFUSED"

THANK/DISCONTINUE MESSAGE: "Thank you for your willingness to take part in this survey, but you do not meet the eligibility requirements of this study."

SCR. 2 In what year were you born?

Record year: _____
99. [DO NOT READ] Don't know/Refused

[ASK SCR. 3 IF SCR. 2 =99]

SCR. 3 Would you be willing to tell me in which of the following age categories you belong?

[READ LIST]

01. 18 to 24
02. 25 to 34
03. 35 to 44
04. 45 to 54
05. 55 to 64
06. 65 or older
99. [DO NOT READ] Refused

SCR. 3 In which province or territory do you live?

[DO NOT READ LIST]

01. Newfoundland and Labrador
02. Prince Edward Island
03. Nova Scotia
04. New Brunswick
05. Quebec
06. Ontario
07. Manitoba
08. Saskatchewan
09. Alberta
10. British Columbia
11. Yukon
12. Northwest Territories
13. Nunavut
TERMINATE IF "DON'T KNOW" OR "REFUSED"

SCR. 4 RECORD GENDER [BY OBSERVATION]

01. Male
02. Female

UNAIDED AWARENESS OF INTELLIGENCE AGENCIES

1. As you may be aware, there is a government agency that is responsible for intercepting and analyzing foreign communications and helping protect the government's computer networks. Can you name this agency? [TRACKING: 2017]

   [DO NOT READ LIST; ACCEPT ONE RESPONSE]

   01. The Communications Security Establishment (CSE)
   02. The Canadian Security Intelligence Service (CSIS)
   03. Department of National Defence (the Canadian Armed Forces)
   04. Global Affairs Canada (DFAIT or Foreign Affairs)
   05. Bureau of Intelligence Analysis
   06. Bureau of Economic Intelligence
   07. Canadian Centre for Cyber Security (Cyber Centre)
   08. CSE and the Cyber Centre
   09. Other (specify)
   99. [DO NOT READ] Don't know

TRUST IN GOVERNMENT INTELLIGENCE SERVICES

2. From your point of view, do you feel that – overall – Canada is safer, more dangerous or about the same as it was five years ago? [TRACKING: 2017]

   [DO NOT READ LIST]

   01. Safer
   02. More dangerous
   03. About the same
   99. [DO NOT READ] Don't know

3. To what extent do you agree or disagree with each of the following statements. Please rate your view on a scale of 1 to 7, where 1 means "strongly disagree," 7 means "strongly agree," and 4 – the mid-point – means you neither agree nor disagree. [TRACKING: 2017] [ROTATE]

   a. I can trust the Government of Canada to strike the right balance between security and civil liberties.
   b. Police and intelligence agencies should have more powers to ensure security even if it means Canadians have to give up some personal privacy safeguards.
   c. Canadian intelligence agencies act within the law when they collect information about Canadians.
   d. I am concerned about information that government intelligence agencies may be collecting about me.
   e. 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.

AWARENESS AND PERCEPTIONS OF CSE

4. The Communications Security Establishment, or CSE, is the Canadian government agency, which is responsible for intercepting and analysing foreign communications and helping protect computer networks that are important to the country, like government systems and critical infrastructure. Would you say that you have ever heard, seen or read anything about the Communications Security Establishment, or CSE? [TRACKING-MODIFIED: 2017]

[READ LIST]

01. Yes
02. Maybe
03. No
99. [DO NOT READ] Don't know

5. Based on this description, and what you may know about the Communications Security Establishment, or CSE, would you say that its mission is very important, somewhat important, not very important or not at all important to Canada's national security – or do you not have an opinion? [TRACKING: 2017]

[DO NOT READ LIST]

01. Very important
02. Somewhat important
03. Not very important
04. Not at all important
05. No opinion
99. [DO NOT READ] Don't know

6. Now, I will read a list of the main things that the Communications Security Establishment, or CSE, does. For each, I would like to know if you think it is very important, somewhat important, not very important or not at all important to Canada's national security?

[ROTATE ITEMS]

a. Gathering foreign intelligence which involves intercepting and analyzing foreign communications
b. Protecting the computer networks that are important to the country from cyber-attacks
c. Assisting law enforcement and security agencies by helping collect and analyze communications
d. Actively defending networks in Canada from foreign cyber threats
e. Disrupting foreign cyber threats before they affect Canada or Canadians

[REPEAT SCALE IF NEEDED]

01. Very important
02. Somewhat important
03. Not very important
04. Not at all important
05. No opinion
99. [DO NOT READ] Don't know

IF RESPONDENT RATES TWO OR MORE ITEMS AT Q6 AS "VERY IMPORTANT":

7. Which one of the following activities is <u>most</u> important when it comes to Canada's national security?

[INSERT ITEMS FROM Q6]

8. Are you aware that…

[ROTATE ITEMS]

a. CSE is prohibited by law from targeting Canadians anywhere, or anyone in Canada.
b. CSE may assist domestic security agencies.

c. Across the government, CSE blocks more than two billion malicious cyber attempts a day.
d. CSE supports Canadian Armed Forces missions, including in cases of Canadians kidnapped abroad.

[READ LIST]

1. Yes
2. No
99. [DO NOT READ] Don't know

9. To what extent would you say that you trust the Communications Security Establishment to act both ethically and legally in fulfilling its mandate? Would you say you completely trust, somewhat trust, do not trust very much or do not trust the CSE at all, or do you not have an opinion either way? [TRACKING: 2017]

[DO NOT READ LIST]

01. Completely trust
02. Somewhat trust
03. Do not trust very much
04. Do not trust at all
05. No opinion
99. [DO NOT READ] Don't know

AWARENESS AND PERCEPTIONS OF THE CYBER CENTRE

10. There is an agency that is part of the Communications Security Establishment, or CSE, with primary responsibility for providing advice, guidance, services and support on cyber security. Can you name this organization?

[DO NOT READ LIST: ACCEPT ONE RESPONSE]

1. The Canadian Centre for Cyber Security
2. The Cyber Centre
3. Cyber New Brunswick or Cyber NB
4. Cybersecure Catalyst
5. Global Intelligence and Cyber Centre
6. Canadian Institute for Cyber Security
7. Other (specify)
99. [DO NOT READ] Don't know

11. The Canadian Centre for Cyber Security, or Cyber Centre, launched in 2018. Uniting operational cyber security expertise from several units within the Government of Canada, the Cyber Centre is a key source of advice, guidance, services and support on cyber security for government, the private sector and the Canadian public. Have you heard, seen or read anything about the Canadian Centre for Cyber Security, or Cyber Centre?

[READ LIST]

01. Yes
02. Maybe
03. No
99. [DO NOT READ] Don't know

12. Now I will read a list of the main things that the Cyber Centre does, and for each one, I'd like you to tell me how much of an impact you think the activity has, or will have, on Canada. To do so, please rate your view on a scale of 1 to 7, where 1 means "no impact," 7 means "high impact," and 4 – the mid-point – means "moderate impact".

    [ROTATE ITEMS]

    a. Inform Canada and Canadians about cyber security matters.
    b. **Protect** our cyber security interests by working with business and government partners.
    c. Develop and share cyber defense technologies and tools.
    d. Defend Canada's cyber systems.
    e. Provide leadership during cyber security events.

Finally,

13. In your opinion, how well prepared do you think each of the following are to meet the threat of a cyberattack? Would you say [INSERT LIST ITEM] [IS/ARE] very well prepared, somewhat prepared, somewhat unprepared or very unprepared to face a cyber threat?

    [ROTATE ITEMS]

    a. The Canadian government
    b. The Electoral systems across Canada
    c. Individual Canadians
    d. Large businesses or enterprises
    e. Small to medium businesses or enterprises
    f. Critical infrastructure operators

INTERVIEWER NOTE: IF ASKED ABOUT "CRITICAL INFRASTRUCTURE" SAY: This refers to sectors, such as energy, utilities, health and finance, among others.

DEMOGRAPHICS

We have a couple final questions for statistical classification purposes. Be assured that your responses will be held in strict confidence.

14. What is the highest level of formal education that you have completed?

    [READ LIST; STOP WHEN RESPONDENT SELECTS AN ANSWER]

    01. Grade 8 or less
    02. Some high school
    03. High School diploma or equivalent
    04. Registered Apprenticeship or other trades certificate or diploma
    05. College, CEGEP or other non-university certificate or diploma
    06. University certificate or diploma below bachelor's level
    07. Bachelor's degree
    08. Post graduate degree above bachelor's level
    99. [DO NOT READ] Prefer not to answer

15. Which of the following categories best describes your current employment status? Are you…

    [READ LIST; STOP WHEN RESPONDENT SELECTS AN ANSWER]

01. Employed full-time for pay (i.e. more than 30 hours)
02. Employed part-time for pay
03. Self-employed
04. Unemployed, and currently seeking work
05. Homemaker
06. Student
07. Disabled
08. Retired
09. Other (specify)
99. [DO NOT READ] Don't know/Refused

16. Which of the following best describes your total household income? That is, the total income of all persons in your household combined, before taxes. Is it ...?

    [READ LIST; STOP WHEN RESPONDENT SELECTS AN ANSWER]

    01. Under $20,000
    02. $20,000 to just under $40,000
    03. $40,000 to just under $60,000
    04. $60,000 to just under $80,000
    05. $80,000 to just under $100,000
    06. $100,000 to just under $150,000
    07. $150,000 and above
    08. [DO NOT READ] Refused

CONCLUSION

That concludes the survey. Thank you very much for your thoughtful feedback. It is much appreciated.