Public Safety Canada | Sécurité publique Canada

Deputy Minister | Sous-ministre

Ottawa, Canada
K1A 0P8

PROTECTED B // CABINET CONFIDENCE

DATE: AUG 2 3 2023

File No.: PS-040909
GCDOCS No.: 32894642

MEMORANDUM FOR THE MINISTER OF PUBLIC SAFETY, DEMOCRATIC INSTITUTIONS AND INTERGOVERNMENTAL AFFAIRS

CONSULTATIONS ON FOREIGN INTERFERENCE LEGISLATIVE AMENDMENTS
(Information only)

ISSUE

Public Safety Canada has been working closely with the Canadian Security Intelligence Service (CSIS) and the Department of Justice (JUS) on proposals to modernize Canada's approach to countering foreign interference (FI). This note is to inform you of the planned launch of public and stakeholder consultations that constitute a significant part of this effort.

CURRENT STATUS

The launch of FI consultations is currently planned for the week of August 28, 2023. The Privy Council Office (PCO) will be informing the Prime Minister and his Office of this intended start date, along with providing the associated consultation papers. Public Safety (PS) has developed a consultation plan and timeline (**TAB A**), as well as an overarching chapeau narrative (**TAB B**) intended for the *Consulting with Canadians* webpage to tie the various consultation initiatives into a broader Government of Canada narrative on ongoing efforts to counter FI.

PS will engage in a second consultation on the implementation of a Foreign Influence Transparency Registry (FITR) (**TAB C**) and consult on changes to the *Canadian Security Intelligence Service Act* (**TAB D**). JUS will consult on changes to the *Criminal Code*, the *Security of Information Act* (SOIA) and the *Canada Evidence Act* (CEA) (**TAB E**). Your colleague, the Honourable Arif Virani, Minister of Justice, is expected to be briefed shortly.

With respect to the FITR, the consultation paper reflects the outcomes of the first round of consultations s. 39 - Cabinet Confidence A second round of consultations will allow for further refinement, as well as additional discussion with targeted stakeholders, including with Provinces, Territories, Municipalities, and Indigenous (PTI) partners.

Canada

With respect to the *CSIS Act*, CSIS proposes to consult the Canadian public on the potential for *CSIS Act* amendments in key areas related to CSIS's core authorities, and bolstering Canada's response to countering FI, including:

- Enhancing CSIS's ability to communicate information and advice to non-federal partners;
- Supporting CSIS's capacity to collect information to counter foreign interference in a digital age;
- Closing the gap in foreign intelligence collection created by technological evolution;
- Enhancing CSIS's capacity to capitalize on data analytics; and
- Introducing a periodic review of the *CSIS Act* to better keep pace with the evolving threat.

BACKGROUND

PS has been working closely with CSIS and JUS to advance commitments from the *Modernizing Canada's Approach to Countering Hostile Activities by State Actors Memorandum to Cabinet* (HASA MC), s. 39 - Cabinet s. 39 - This includes consulting Canadians on enhancements to the Government of Canada's counter-FI legislative toolkit.

As a first step, on March 10, 2023, the then Minister of Public Safety launched a 60-day public and stakeholder consultations on the creation of a FITR to bolster defences against non-transparent foreign influence activities in Canada. While online consultations formally closed on May 9, 2023, discussions with targeted stakeholders remain ongoing, including PTIs.

Almost 1,000 online responses were received from Canadians, and PS engaged with over 80 stakeholders from various organizations, communities, advocacy groups, professional associations, religious groups, and representatives from provincial and territorial governments. Several key themes emerged during these consultations:

- There is broad support for FITR, on the grounds that it will enhance transparency, protect vulnerable communities, and help deter malign foreign influence.
- A FITR must be consistent with *The Canadian Charter of Rights and Freedoms*. It must not be used to create a "blacklist", or to stigmatize or further marginalize certain Canadian communities.
- A FITR is not a universal tool to counter FI; rather, it is only one of many tools needed to counter FI.

s. 39 - Cabinet Confidence

s. 39 - Cabinet Confidence

CONSIDERATIONS

These papers have been developed by departments and reviewed and approved by Deputies led by the Clerk. They have also been reviewed through a 4 corners discussion. The current plan is to return to Cabinet as soon as possible in the Fall Session. This timing is subject to the launch of consultations the week of August 28, 2023.

The execution of the consultations is intended to be two-fold:

Public Consultations
Public consultations will be undertaken via an online portal. The FITR and *CSIS Act* consultation papers, supported by web content drawn from the overarching chapeau narrative, will be hosted on the PS website. The *Criminal Code*, SOIA, and CEA consultation paper will be hosted on the JUS website. The overarching chapeau narrative will also bring these consultations together under the *Consulting with Canadians* web domain with weblinks to the respective papers.

Stakeholder Consultations
Stakeholder consultations will be undertaken via roundtable and bilateral meeting formats with select stakeholders (evergreen list **TAB G**). A diverse number of stakeholders and groups, including Indigenous groups, diaspora community groups, academics, advocacy groups, industry, etc., are being considered for roundtable consultations by JUS and CSIS. JUS has indicated a preference for conducting its roundtables separately due to sensitivities regarding CSIS interactions with certain groups. However, there is noted overlap between stakeholders and groups that CSIS and JUS are seeking to consult. Partners are working together to determine where engagements can be combined to avoid consultation fatigue.

With respect to FITR, the primary intent is to engage PTIs. These discussions will be combined, where possible, with *CSIS Act*, *Criminal Code*, SOIA, and CEA.

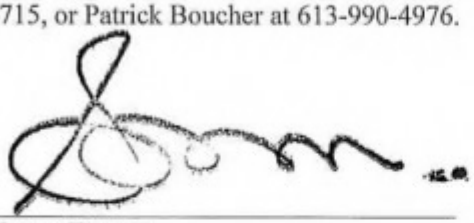
A communications plan for the consultations is attached (**TAB H**).

A draft of the What We Heard So Far (WWHSF) Report from the first round of FITR consultations, with an accompanying Memo (PS-040703), was sent for your approval in early August. It is recommended that the FITR WWHSF Report be released prior or concurrently to the launch of the second round of consultations. It is included under **TAB F** for reference.

NEXT STEPS

Work is underway to finalize the documents for release and to be ready to go live the week of August 28, 2023.

Should you require any additional information, please do not hesitate to contact me at 613-614-4715, or Patrick Boucher at 613-990-4976.



Shawn Tupper
Deputy Minister

Attachment(s) (8):
Tab A: Consultation Placemat and Timeline
Tab B: Countering Foreign Interference (Chapeau Piece)
Tab C: Foreign Influence Transparency Registry: Updated Public Consultation Paper
Tab D: Enhancing Measures To Counter Foreign Interference Public Consultation Paper – Whether To Amend The Canadian Security Intelligence Service Act
Tab E: Public Consultations on Potential Amendments to the Security of Information Act, Criminal Code and Canada Evidence Act
Tab F: What We've Heard So Far – Foreign Influence Transparency Registry Consultation Summary
Tab G: Tentative Consolidated Stakeholders List
Tab H: Launch of the Government of Canada Consultations on Foreign Interference Communications Approach

Prepared by: *NCSB*
Consulted*: CSIS*

TAB A

LAST UPDATED: August 18, 2023

Protected B | Protégé B

CONSULTATIONS AND ENGAGEMENT ON FOREIGN INTERFERENCE

- Consultations on potential legislative amendments to the *Canadian Security and Intelligence Service Act* (CSIS Act), the *Criminal Code*, the *Security of Information Act* (SOIA), and the *Canada Evidence Act* (CEA) are planned for the summer of 2023. Consultations will gauge a wide range of views on the proposed reforms, including potential impacts on Charter rights and freedoms, and seek to foster public and stakeholder buy-in.
- Broad-based consultations will engage both the Canadian public, through an online consultation paper, and targeted stakeholders, through roundtable discussions (or bilateral as necessary), from academia, law, industry, media, advocacy and diverse communities and historically marginalized groups.
- An overarching narrative will tie in the various consultations to the broader challenges posed by foreign interference (FI) which impacts all areas of Canadian society, and demonstrate how legislative amendments could bolster Canada's response. A strategic public communications approach will present the consultations as a continuation of the Public Safety-led consultations on the Foreign Influence Transparency Registry (FITR), as part of a broader effort of the Government of Canada to modernize Canada's toolkit to counter FI.
- This narrative will be featured on the Consulting Canadians webpage as well as the Public Safety and Department of Justice (DOJ) websites where the online consultation papers will be housed.
- To minimize stakeholder fatigue or frustration, Public Safety, DOJ, and the Canadian Security Intelligence Service (CSIS) will coordinate engagements, and hold joint sessions where possible.

FITR

Desired outcome: Considered an international best practice, a Foreign Influence Transparency Registry (FITR) would strengthen transparency and accountability on foreign influence in Canada through disclosure requirements.

Status:

- PS launched public and stakeholder consultations to guide the development of the FITR on March 10, 2023.
- PS received nearly 1,000 responses and engaged with more than 80 stakeholders.
- While the online component of the consultations closed on May 9, the proposed sub-national application of FITR will require more in-depth discussions with Provinces, Territories, Municipalities and Indigenous partners.
- s. 39 - Cabinet Confidence

Way Forward:

- PS intends to conduct targeted consultations with specific stakeholders s. 39 - Cabinet s. 39 - Cabinet in order to further develop the proposed legislation.

CSIS ACT

Desired outcome: Address *CSIS Act* challenges with legislative amendments in key areas impacting CSIS' ability to counter FI.

Consultation objectives:

- Inform and educate stakeholders on CSIS' mandate, including *CSIS Act* challenges;
- Listen to stakeholder's experiences to better understand unknown impacts of *CSIS Act* challenges on society;
- Broach areas where changes to the *CSIS Act* could help CSIS better address modern FI threats;
- Obtain feedback on ways to balance modern tools with privacy concerns;
- Develop and/or maintain trusted relationships with stakeholders (especially communities targeted by FI);
- Demonstrate CSIS' commitment to national security transparency; and
- Garner support to pass *CSIS Act* amendments.

Way Forward:

- Led by Public Safety and CSIS
- Hybrid (online public consultations and targeted stakeholder consultations)
- Documents will include:
  - Consultation paper with discussion questions to be hosted on PS webpage.
  - PowerPoint presentation to facilitate roundtable discussions.
- Feedback received to be evaluated by Public Safety and CSIS and summarized in a broader What We Heard Report on FI consultations, or other summary.

SOIA AND CRIMINAL CODE

Desired outcome: Canada's criminal law framework, including FI related offences in the SOIA and Criminal Code, is responsive to the evolving threat environment and the seriousness of FI.

Consultation objectives:

- To foster transparency on potential development of legislative measures, policies and programs targeting FI;
- To gather information on key issues, priorities and concerns regarding FI threats and how to counter them; and,
- To ensure that, in cooperation and consultation with Indigenous peoples, the proposed measures are consistent with the *United Nations Declaration on the Rights of Indigenous Peoples Act*.

Way Forward:

- Led by DOJ
- Hybrid (online public consultation and targeted stakeholder consultations)
- Documents will include:
  - Consultation paper to discuss proposed Criminal Code and SOIA amendments to be hosted on Department of Justice webpage.
  - PowerPoint presentation to facilitate roundtable discussions.
- Feedback received to be evaluated by DOJ and summarized in a broader What We Heard Report on FI consultations, or other summary.

CEA AND CRIMINAL CODE

Desired outcome: Canada's legislative scheme for the protection and use of national security information in administrative and criminal proceedings is responsive to the evolving threat environment and the seriousness of FI.

Consultation objectives:

- To foster transparency on potential development of legislative measures, policies and programs targeting FI;
- To gather information on key issues, priorities and concerns regarding FI threats and how to counter them; and,
- To ensure that, in cooperation and consultation with Indigenous peoples, the proposed measures are consistent with the *United Nations Declaration on the Rights of Indigenous Peoples Act*.

Way Forward:

- Led by DOJ
- Hybrid (online public consultations and targeted stakeholder consultations)
- Documents will include:
  - Consultation paper to discuss CEA and Criminal Code amendments to be hosted on Department of Justice webpage.
  - PowerPoint presentation to facilitate roundtable discussions.
- Feedback received to be evaluated by DOJ and summarized in a broader What We Heard Report on FI consultations, or other summary.

s. 39 - Cabinet Confidence

TAB B

UNCLASSIFIED
LAST UPDATED: August 21, 2023

Countering-Foreign Interference *(Chapeau Piece)*

Canada is a country open to the world. We are an advanced trading economy and an open democracy with positive relations with a great number of nations. We also believe in collective security, and we have built durable security and military partnerships with like-minded states around the world.

Foreign partners regularly seek to influence the decisions we make as a country, just as Canada seeks to influence the decisions of others. Foreign partners generally use legitimate and transparent means to advocate their interests, such as lobbying, political dialogue, trade negotiations and diplomacy.

Some foreign states use covert, deceptive and sometimes threatening means to interfere in our political system and our economy. They do so to advance their own strategic objectives, to the detriment of Canada's national interests.

The threat of foreign interference is not new, but has increased in recent years as the world becomes more competitive, the digital world has created more ways for people and governments to have far reaching impact, and some states are willing to use all means available to them to challenge our democratic way of life. These interference activities are not acceptable and Canada will never tolerate them.

Foreign interference can affect all individuals in Canada: government officials, civil society, communities, businesses, academia, and the media. Examples of interference by foreign states, or those acting on their behalf, include:

- Threatening, harassing or intimidating people in Canada or their family and friends abroad because of their political opinions or to shape behaviour;
- Attempting to interfere in Canada's democratic institutions and processes, such as elections, to advance their interests;
- Stealing our intellectual property, know-how or imposing market conditions to gain an economic advantage against Canada;
- Targeting officials at all levels of government to influence public policy and decision-making in a way that is clandestine, deceptive or threatening, and to the detriment of Canadian interests.

Foreign interference poses one of the greatest threats to Canada's national security, our way of life, and our economic prosperity and sovereignty. We must shine a light on these threats, and come together as a country to defend our nation from those who attempt to harm us. These examples underscore the urgency needed to hold those who would threaten individuals in Canada and Canada's sovereignty accountable for their actions by strengthening the consequences of engaging in interference activities in Canada.

Modernizing Canada's Toolkit to Counter Foreign Interference

Foreign states, or their proxies, are known to target certain vulnerable groups within Canada – often based on their ethno-religious background. They do this in an effort to sew divisions, fear, and suspicion within Canadian communities. They can threaten the basic rights of individuals in Canada, including personal security, religious and cultural freedoms, freedom of speech, movement and the right to earn a livelihood without interference. Furthermore, these interference activities can result in increased stigmatization of certain groups in Canada.

As the threat of foreign interference evolves, Canada's response needs to adapt. Domestic and international experts have noted that Canada needs to modernize its tools to counter the threat of foreign interference. Canada's closest allies and like-minded partners have also brought forward legislative initiatives to modernize their counter-foreign interference toolkits.

Consulting with Canadians is an important step in this effort to modernize our toolkit to counter foreign interference, so that potential solutions are aligned with our national values, capture a wide range of expertise, perspectives, views and opinions, and respect Canadian fundamental rights and freedoms. The Canadian public have expressed interest in greater transparency, as well as deeper engagement with the Government of Canada on national security issues, including foreign interference.

This is why on March 10, 2023, Public Safety Canada launched public and stakeholder consultations to guide the development of a Foreign Influence Transparency Registry (FITR). The initial phase of public consultations closed on May 9. The FITR consultations yielded a large number of responses from across Canada and included engagements with a wide range of groups, such as community organizations, academia and the private sector. The consultations demonstrated broad support for the introduction of a FITR in Canada, but one of the main themes that emerged from the consultations is that a Registry is not a universal solution, and should be accompanied by other legislative amendments to address other aspects of foreign interference. You can access the "What We've Heard So Far" report here [insert hyperlink], and are invited to review the proposed frame here [insert hyperlink], as we continue consultations, including with Provinces, Territories, Municipalities and Indigenous partners.

What we know, and what has been reinforced through the consultations, is that Canada's toolkit needs to adapt as the threats emanating from foreign interference evolve. To address these gaps Canada must consider:

- Modernizing the criminal law, including by introducing new foreign interference-related offences to better capture the evolving threat.
- Providing the Government of Canada with better tools to address certain types of activities that foreign states use to covertly shape public opinion and exert undue influence in Canada (e.g., Introducing a FITR in Canada).
- Providing Canada's national security agencies with the legal ability to share threat information with a wider set of Canadian partners than the federal government (e.g., Sharing of information with Canada's private stakeholders to protect Canada's critical infrastructure).
- Improving the ways that the legal system deals with intelligence information in administrative and criminal proceedings.
- Making sure that the Canadian Security Intelligence Service has modernized authorities to be able to adequately protect Canadians and Canadian institutions in a digital world (e.g., Amending intelligence collection authorities which are currently limited to information located within Canada).

In recognition of this, and of the above challenges, in addition to FITR consultations, the Government of Canada is launching consultations on the *Canadian Security Intelligence Service Act*, the *Criminal Code*, the *Security of Information Act* and the *Canada Evidence Act*. The purpose of these consultations is to assess potential amendments to these laws to bolster Canada's counter-foreign interference toolkit.

UNCLASSIFIED
LAST UPDATED: August 21, 2023

Together, we can protect Canadian values, principles, rights and freedoms from those who seek to harm our way of life.

[Chapeau to act as an intro piece to the Foreign Influence Transparency Registry, Criminal Code/Security of Information Act/Canada Evidence Act and CSIS Act amendments]

Foreign Influence Transparency Registry

Foreign governments regularly seek to influence the Government of Canada and public opinion in Canada, and often do so through established, legitimate, and transparent channels. When individuals or entities seek to exert influence on behalf of a foreign government in non-transparent ways, this can have serious consequences on democratic process in Canada or result in policy or legislative outcomes unduly favourable to foreign interests. For this reason, Canada's closest allies and like-minded partners have brought forward additional measures to enhance foreign influence transparency in their respective countries.

Canada has existing tools to ensure transparency and address conflicts of interest, such as the Lobbying Act, Conflict of Interest Act and the Canada Elections Act, however these legislative tools were not designed specifically to address this type of foreign interference. A foreign influence transparency registry could address existing gaps and increase transparency and general public awareness of non-transparent foreign influence activities in Canada by imposing registration and information disclosure obligations on individuals and entities engaged in foreign influence activities. Additionally, a foreign influence transparency registry would help deter non-transparent foreign influence activities by increasing the risk to individuals who would seek to avoid registration obligations by designing appropriate compliance measures and penalties.

About the Consultation

On March 10, 2023, the Minister of Public Safety launched public and stakeholder consultations on a foreign influence transparency registry. While public consultations closed on May 9, 2023, some stakeholder consultations extended beyond this date. Preliminary public and stakeholder feedback has indicated broad support for a registry in Canada, and respondents have provided meaningful feedback to government officials to inform the design of a built-for-Canada foreign influence transparency registry.

Since the close of public consultations, the Government has worked on developing a registry proposal that is responsive to the views provided by the public and stakeholders. As policy refinement and development continues, the government intends to undertake additional engagements with select stakeholders, as well as seek additional views from the public.

The purpose of this additional public consultation period is therefore to solicit additional feedback on the creation of a Foreign Influence Transparency Registry as a tool for greater transparency over foreign influence activities and a deterrent to malign and covert interference by foreign states.

How to Participate

Visit our consultation page [insert hyperlink]. Consultations will be open for 45 days.

Next steps

Feedback from consultation with the public and stakeholders will inform the Government's decision on what measures to bring forward, and what they could look like.

Related information

- Consultation Paper [insert hyperlink]
- Foreign Interference

Contact us

Public Safety Canada
269 Laurier Avenue West
Ottawa, ON K1A 0P8
Email: TBC

Criminal Code/Security of Information Act/Canada Evidence Act

Justice Canada is seeking to initiate a meaningful dialogue on whether to amend the *Security of Information Act* (SOIA) and modernize certain *Criminal Code* offences, whether to amend the *Criminal Code* to reform how national security information is protected and used in criminal proceedings, and to introduce a review mechanism in the *Canada Evidence Act* (CEA) to manage sensitive information.

An Overview of Existing Measures

The Government currently uses various measures to counter foreign interference, including investigating and laying criminal charges in accordance with Canadian laws. These laws include Canada's SOIA, which criminalizes information-related conduct that may be harmful to Canada, such as unauthorized disclosure of information, spying, economic espionage and foreign-influenced threats or violence. There are *Criminal Code* offences that address different types of conduct in connection with foreign interference, such as sabotage, intimidation, computer hacking and bribery, amongst others. And, there are offences and other provisions in the *Canada Elections Act* which address foreign involvement in our federal electoral processes.

In recent years, however, many experts have called on Canada to modernize these laws to address new and evolving foreign interference threats and to ensure consistency with allied countries. The SOIA, for example, has not had a substantial revision since 2001 and may benefit from updates to better respond to modern threats. Australia, the U.S. and the U.K. have all recently taken steps to enhance their ability to identify and counter foreign interference.

About the Consultation

Justice Canada is examining whether to

- amend the SOIA by introducing new foreign interference offences that will improve protections for people in Canada and our democratic processes;
- improve on SOIA provisions that protect against unauthorized disclosures of information that could harm Canada's interests;
- modernize the sabotage offence in the *Criminal Code*;

- introduce a general review mechanism in the CEA to manage sensitive information in judicial reviews and statutory appeal of federal administrative decisions; and
- other potential *Criminal Code* and CEA amendments to deal with how national security information is handled in criminal proceedings.

Furthermore, Justice Canada will consult on measures that could be taken to provide an overall legislative scheme for the protection and use of national security information in judicial reviews and statutory appeals of federal governmental decision making. Finally, it will gauge views on potential reforms relating to intelligence and evidence in criminal proceedings.

How to Participate

Visit our consultation page [insert hyperlink]. Consultations will be open for 60 days.

Next steps

Feedback from consultation with the public and stakeholders will inform the Government's decision on what measures to bring forward, and what they could look like.

Related information

- Consultation Paper [insert hyperlink]
- Foreign Interference

Contact us

Department of Justice
284 Wellington Ave
Ottawa, ON K1A 0H8
Email: TBC

CSIS Act

The Canadian Security Intelligence Service (CSIS) is seeking to initiate a meaningful dialogue on potential amendments to the *Canadian Security Intelligence Service Act* (*CSIS Act*) to more effectively counter modern-day threats, including foreign interference.

An Overview of CSIS Act Challenges Impacting ability to Counter Foreign Interference

Canada is witnessing aggressive foreign interference from highly-capable state actors who exploit technology and other means to advance their national interests to the detriment of Canada's. To counter this sophisticated threat requires CSIS to have the right tools and authorities.

The objective in amending the *CSIS Act* is to ensure CSIS can continue to protect Canada and Canadians in an increasingly digital world. In the face of sophisticated foreign interference threats, *CSIS Act* amendments will:

- Enable CSIS to help Canadian society build resilience against foreign interference;
- Support CSIS' capacity to collect information to counter foreign interference in a digital age; and
- Ensure that national security legislation keeps pace with evolving threats.

UNCLASSIFIED
LAST UPDATED: August 21, 2023

About the Consultation

CSIS will consult the Canadian public on the potential for *CSIS Act* amendments in key areas including: (1) enhancing CSIS' ability to communicate information and advice to non-federal partners; (2) supporting CSIS' capacity to collect information to counter foreign interference in a digital age; (3) closing the gap in foreign intelligence collection created by technological evolution; (4) enhancing CSIS' capacity to capitalize on data analytics; and (5) introducing a periodic review of the *CSIS Act* to better keep pace with the evolving threat. As a complement to public consultations, CSIS will also engage with a broad array of stakeholders in round table discussions, including those from community advocacy organizations, businesses, critical infrastructure, academia, and legal, privacy and transparency experts.

The consultations will allow Canadians to participate in a full and informed discussion about national security tools and authorities. CSIS recognizes that the authorities in the *CSIS Act* must reflect the values and ideals of those it seeks to protect. Engaging in a dialogue with Canadians on maintaining the right balance between protecting national security and respecting Canadians' expectations of privacy is a prerequisite to achieving this objective.

How to Participate

Visit our consultation page [insert hyperlink]. Consultations will be open for 60 days.

Next steps

Feedback from consultation with the public and stakeholders will inform the Government's decision on what measures to bring forward, and what they could look like.

Related information

- Consultation Paper [insert hyperlink]
- Foreign Interference

Contact us

Public Safety Canada
269 Laurier Avenue West
Ottawa, ON K1A 0P8
Email: TBC

French Version

NON CLASSIFIÉ
DERNIÈRE VERSION : 21 AOUT 2023

Lutte contre l'ingérence étrangère *(aperçu général)*

Le Canada est un pays ouvert sur le monde. Nous avons une économie commerciale avancée et une démocratie ouverte et entretenons des relations positives avec un grand nombre de nations. Nous croyons également à la sécurité collective et nous avons établi des partenariats militaires et de sécurité durables avec des États du monde entier partageant les mêmes points de vue.

Les partenaires étrangers cherchent souvent à influencer les décisions que nous prenons en tant que pays, tout comme le Canada cherche à influencer les décisions des autres. Les partenaires étrangers utilisent généralement des moyens légitimes et transparents pour défendre leurs intérêts, tels que le lobbying, le dialogue politique, les négociations commerciales et la diplomatie.

Certains États étrangers utilisent des moyens clandestins, trompeurs et parfois menaçants pour s'immiscer dans notre système politique et notre économie. Ils le font pour promouvoir leurs propres objectifs stratégiques, au détriment des intérêts nationaux du Canada.

La menace d'ingérence étrangère n'est pas nouvelle, mais elle s'accroît depuis les dernières années à mesure que le monde devient de plus en plus compétitif, que le monde numérique multiplie les moyens pour les particuliers et les gouvernements d'avoir un impact considérable et que certains États sont prêts à utiliser tous les moyens à leur disposition pour remettre en cause notre mode de vie démocratique. Ces activités d'ingérence sont inacceptables, et le Canada ne les tolérera jamais.

L'ingérence étrangère peut toucher tout le monde au Canada : les fonctionnaires, la société civile, les communautés, les entreprises, les universités et les médias. Voici quelques exemples d'ingérence par des États étrangers ou des personnes agissant en leur nom :

- Menacer, harceler ou intimider des personnes au Canada ou leur famille et leurs amis à l'étranger en raison de leurs opinions politiques ou pour modeler leur comportement;
- Tenter de s'ingérer dans les institutions et les processus démocratiques du Canada, comme les élections, pour promouvoir leurs intérêts;
- Voler notre propriété intellectuelle, notre savoir-faire ou imposer des conditions de marché pour obtenir un avantage économique sur le Canada;
- Cibler des fonctionnaires à tous les ordres de gouvernement pour influencer les politiques publiques et la prise de décision d'une manière clandestine, trompeuse ou menaçante, et au détriment des intérêts canadiens.

L'ingérence étrangère constitue l'une des plus grandes menaces pour la sécurité nationale, le mode de vie, la prospérité économique et la souveraineté du Canada. Nous devons faire la lumière sur ces menaces et nous unir en tant que pays pour défendre notre nation contre ceux qui tentent de nous nuire. Ces exemples soulignent l'urgence qu'il y a à tenir pour responsables de leurs actes ceux qui menacent des personnes au Canada et la souveraineté du pays, en renforçant les conséquences de la participation à des activités d'ingérence au Canada.

Moderniser la boîte à outils du Canada pour lutter contre l'ingérence étrangère

Nous savons que certains États étrangers, ou leurs mandataires, ciblent certains groupes vulnérables au Canada, souvent en se fondant sur leur appartenance ethnoreligieuse. Ils agissent ainsi dans le but de semer la division, la peur et la suspicion au sein des communautés canadiennes. Ils peuvent menacer les

droits fondamentaux d'individus au Canada, notamment leur sécurité personnelle, leurs libertés religieuses et culturelles, leur liberté d'expression, leur liberté de mouvement et leur droit de gagner leur vie sans ingérence. En outre, ces activités d'ingérence peuvent entraîner une stigmatisation accrue de certains groupes au Canada.

La menace d'ingérence étrangère évolue, et le Canada doit adapter ses mesures. Des experts nationaux et internationaux ont fait remarquer que le Canada doit moderniser ses outils pour lutter contre cette menace. Certains des alliés les plus proches du Canada et de ses partenaires aux vues similaires ont introduit des mesures législatives pour moderniser leurs outils de lutte contre l'ingérence étrangère.

La consultation des Canadiens est une étape importante de la modernisation de notre boîte à outils pour lutter contre l'ingérence étrangère. Elle fera en sorte que les solutions soient alignées sur nos valeurs nationales, tiennent compte d'un large éventail d'expertises, de perspectives, de points de vue et d'opinions, et respectent les droits fondamentaux et les libertés des Canadiens. Le public canadien a exprimé son intérêt pour une plus grande transparence, ainsi que pour une collaboration approfondie avec le gouvernement du Canada sur les questions de sécurité nationale, dont l'ingérence étrangère.

C'est pourquoi, le 10 mars 2023, Sécurité publique Canada a lancé des consultations auprès du public et des intervenants afin d'orienter l'élaboration d'un registre pour la transparence en matière d'influence étrangère (RTMIE). La phase initiale des consultations publiques s'est achevée le 9 mai dernier. Les consultations sur le RTMIE ont donné lieu à un grand nombre de réponses à l'échelle du Canada et à des discussions avec un large éventail de groupes, comme des organisations communautaires, le monde universitaire et le secteur privé. Elles ont démontré qu'il y a un vaste soutien à l'introduction d'un RTMIE au Canada, mais l'un des principaux thèmes qui en sont ressortis est qu'un registre n'est pas une solution universelle et que celui-ci devrait être accompagné d'autres changements législatifs qui traiteraient d'autres aspects de l'ingérence étrangère. Vous pouvez consulter le « Rapport sur ce que nous avons entendu » [insérer l'hyperlien] et examiner le cadre proposé [insérer l'hyperlien] pendant que nous poursuivons les consultations, notamment avec les provinces, les territoires, les municipalités et les partenaires autochtones.

Ce que nous savons, et ce qui a été confirmé par les consultations, c'est que la boîte à outils du Canada doit s'adapter à l'évolution des menaces émanant de l'ingérence étrangère. Pour combler les lacunes, le Canada doit envisager ce qui suit :

- Moderniser le droit pénal, y compris en introduisant de nouvelles infractions liées à ingérence étrangère afin de mieux saisir la menace en constante évolution.
- Fournir au gouvernement du Canada de meilleurs outils pour contrer certains types d'activités que les États étrangers utilisent pour façonner secrètement l'opinion publique et exercer une influence indue au Canada (p. ex., l'introduction d'un RTMIE au Canada).
- Donner aux organismes de sécurité nationale du Canada la possibilité légale d'échanger des renseignements sur les menaces avec des partenaires canadiens ne faisant pas parti du gouvernement fédéral (p. ex., la communication de renseignements à des intervenants du secteur privé canadien pour protéger les infrastructures essentielles du pays).
- Améliorer la façon dont le système judiciaire traite les renseignements dans les poursuites administratives et criminelles.
- Veiller à ce que le Service canadien du renseignement de sécurité dispose de pouvoirs modernisés afin d'être en mesure de protéger adéquatement les Canadiens et les institutions

canadiennes dans un monde numérique (p. ex., modifier les pouvoirs de collecte de renseignements qui sont actuellement limités aux informations situées à l'intérieur du Canada).

Compte tenu de la situation et des difficultés susmentionnées, le gouvernement du Canada lance, en plus des consultations sur le RTMIE, des consultations sur la *Loi sur le Service canadien du renseignement de sécurité*, le *Code criminel*, la *Loi sur la protection de l'information* et la *Loi sur la preuve au Canada*. Ces consultations ont pour objectif d'évaluer les modifications qui pourraient être apportées à ces lois dans le but de renforcer les outils de lutte contre l'ingérence étrangère dont dispose le Canada.

Ensemble, nous pouvons protéger les valeurs, les principes, les droits et les libertés des Canadiens contre ceux qui cherchent à nuire à notre mode de vie.

[Aperçu général qui servira d'introduction au registre pour la transparence en matière d'influence étrangère et aux modifications du Code criminel, *de la* Loi sur la protection de l'information, *de la* Loi sur la preuve au Canada *et de la* Loi sur le Service canadien du renseignement de sécurité*].*

Registre pour la transparence en matière d'influence étrangère

Les gouvernements étrangers cherchent souvent à influencer le gouvernement du Canada et l'opinion publique au Canada, et le font fréquemment par des voies établies, légitimes et transparentes. Toutefois, lorsque des personnes ou des entités cherchent à exercer une influence au nom d'un gouvernement étranger de manière non transparente ou de façon malveillante, les conséquences peuvent être graves. Ces activités pourraient interférer avec les processus démocratiques du Canada ou entraîner des résultats politiques ou législatifs indûment favorables aux intérêts étrangers. C'est pourquoi certains des alliés les plus proches du Canada et de ses partenaires aux vues similaires ont proposé des mesures supplémentaires qui visent expressément à améliorer la transparence en matière d'influence étrangère dans leurs pays respectifs.

Le Canada dispose de certains outils pour garantir la transparence et traiter les conflits d'intérêts, tels que la *Loi sur le lobbying*, la *Loi sur les conflits d'intérêts* et la *Loi électorale du Canada*, mais ces outils législatifs n'ont pas été conçus précisément pour répondre à la menace complexe que constitue l'influence étrangère malveillante. Un registre pour la transparence en matière d'influence étrangère pourrait combler les lacunes existantes et accroître la transparence et la sensibilisation du grand public aux activités d'influence étrangère malveillante au Canada en imposant des obligations liées à l'inscription et la divulgation de renseignements pour les individus et les entités se livrant à des activités d'influence étrangère. En outre, un registre pour la transparence en matière d'influence étrangère supporté par des mesures de conformité et des sanctions contribuerait à dissuader les activités d'influence étrangère malveillante en augmentant le risque pour les personnes qui chercheraient à se soustraire aux obligations d'inscription en concevant des mesures de conformité et des sanctions.

À propos des consultations

Le 10 mars 2023, le ministre de la Sécurité publique a lancé des consultations auprès du public et des intervenants au sujet d'un registre pour la transparence en matière d'influence étrangère. Les consultations publiques ont pris fin le 9 mai 2023, mais certaines consultations auprès des intervenants se sont prolongées au-delà de cette date. Selon les premiers commentaires recueillis, le public et les intervenants appuient largement l'établissement d'un registre au Canada. Les répondants ont fourni aux

représentants du gouvernement des commentaires significatifs qui leur permettront d'orienter la conception d'un registre pour le Canada.

Depuis la clôture des consultations publiques, le gouvernement travaille à l'élaboration d'une proposition de registre tenant compte des avis exprimés par le public et les intervenants. Au fur et à mesure que l'élaboration et le perfectionnement des politiques se poursuivra, le gouvernement a l'intention de mobiliser encore une fois certains intervenants et de solliciter d'autres avis de la part du public.

L'objectif de cette période supplémentaire de consultation publique est donc d'obtenir des commentaires supplémentaires sur l'établissement d'un registre pour la transparence en matière d'influence étrangère dans le but d'accroître la transparence des activités d'influence étrangère et de dissuader les États étrangers de se livrer à des activités d'ingérence malveillante et secrète.

Comment participer

Rendez-vous sur notre page sur les consultations [insérer l'hyperlien]. Les consultations se tiendront pendant 45 jours.

Prochaines étapes

Les commentaires issus des consultations auprès du public et des intervenants éclaireront la décision du gouvernement quant aux mesures à mettre en œuvre et à leur forme.

Renseignements connexes

- Document de consultation [insérer l'hyperlien]
- Interférence étrangère

Nous joindre

Sécurité publique Canada
269, avenue Laurier Ouest
Ottawa (Ontario) K1A 0P8
Courriel : À confirmer

Code criminel/Loi sur la protection de l'information/Loi sur la preuve au Canada

Justice Canada souhaite entamer un dialogue constructif pour savoir s'il convient de modifier la *Loi sur la sécurité de l'information* et de moderniser certaines infractions prévues dans le *Code criminel*, s'il y a lieu de modifier le *Code criminel* pour réformer la façon dont les renseignements relatifs à la sécurité nationale sont protégés et utilisés dans les procédures pénales, et s'il faut introduire un mécanisme d'examen dans la *Loi sur la preuve au Canada* afin de gérer les renseignements de nature délicate.

Aperçu des mesures actuelles

Le gouvernement applique actuellement diverses mesures pour contrer l'ingérence étrangère, dont mener des enquêtes et porter des accusations criminelles conformément aux lois canadiennes. Ces lois comprennent la *Loi sur la protection de l'information*, qui criminalise les comportements liés à l'information susceptibles de nuire au Canada, comme la communication non autorisée, l'espionnage, l'espionnage économique et les menaces ou les actes violents pour le compte d'une entité étrangère. Il existe des infractions au *Code criminel* qui concernent différents types de comportements liés à

l'ingérence étrangère, comme le sabotage, l'intimidation, le piratage informatique et la corruption. Enfin, la *Loi électorale du Canada* prévoit des infractions et d'autres dispositions relatives à l'ingérence étrangère dans nos processus électoraux fédéraux.

Ces dernières années, cependant, de nombreux experts ont appelé le Canada à moderniser ces lois pour faire face aux nouvelles menaces d'ingérence étrangère et à leur évolution, et pour assurer la cohérence avec les pays alliés. La *Loi sur la protection de l'information*, par exemple, n'a pas fait l'objet d'un remaniement important depuis 2001 et pourrait bénéficier d'une mise à jour pour qu'elle réponde mieux aux menaces modernes. L'Australie, les États-Unis et le Royaume-Uni ont tous pris récemment des mesures pour renforcer leur capacité à déceler et à contrer les activités d'ingérence étrangère.

À propos des consultations

Justice Canada étudie les possibilités suivantes :

- Modifier la *Loi sur la protection de l'information* en introduisant de nouvelles infractions d'ingérence étrangère, ce qui protégerait davantage les citoyens canadiens et nos processus démocratiques;
- Améliorer les dispositions de la *Loi sur la protection de l'information* contre les communications non autorisées d'information susceptibles de nuire aux intérêts du Canada;
- Moderniser l'infraction de sabotage prévue dans le *Code criminel*;
- Introduire un mécanisme général d'examen dans la *Loi sur la preuve au Canada* qui permettra de gérer les renseignements de nature délicate dans le cadre des contrôles judiciaires et des appels prévus par la loi en ce qui a trait à des décisions administratives fédérales;
- Apporter d'autres modifications au *Code criminel* et à la *Loi sur la preuve au Canada* sur la question du traitement des renseignements relatifs à la sécurité nationale utilisés dans le cadre des procédures pénales.

En outre, Justice Canada consultera sur les mesures qui pourraient être prises pour fournir un cadre législatif global sur la protection et l'utilisation des renseignements relatifs à la sécurité nationale dans les contrôles judiciaires et les appels prévus par la loi des décisions du gouvernement fédéral. Enfin, Justice Canada recueillera des avis sur les réformes éventuelles concernant les renseignements et les éléments de preuve dans les procédures pénales.

Comment participer

Rendez-vous sur notre page sur les consultations [insérer l'hyperlien]. Les consultations se tiendront pendant 60 jours.

Prochaines étapes

Les commentaires issus des consultations auprès du public et des intervenants éclaireront la décision du gouvernement quant aux mesures à mettre en œuvre et à leur forme.

Renseignements connexes

- Document de consultation [insérer l'hyperlien]
- Interférence étrangère

Nous joindre

NON CLASSIFIÉ
DERNIÈRE VERSION : 21 AOUT 2023

Ministère de la Justice
284, avenue Wellington
Ottawa (Ontario) K1A 0H8
Courriel : À confirmer

Loi sur le SCRS

Le Service canadien du renseignement de sécurité (SCRS) souhaite entamer un dialogue constructif sur les modifications possibles à la *Loi sur le Service canadien du renseignement de sécurité* (*Loi sur le SCRS*) afin de pouvoir lutter plus efficacement contre les menaces contemporaines, dont l'ingérence étrangère.

Aperçu des aspects de la *Loi sur le SCRS* qui freinent la lutte contre l'ingérence étrangère

Le Canada est témoin d'une ingérence étrangère agressive de la part d'acteurs étatiques très compétents qui exploitent la technologie et d'autres moyens pour promouvoir leurs intérêts nationaux au détriment de ceux du Canada. Pour contrer cette menace sophistiquée, le SCRS doit disposer des outils et des pouvoirs appropriés.

Les modifications à la *Loi sur le SCRS* auraient pour but de permettre au SCRS de continuer à protéger le Canada et les Canadiens dans un monde de plus en plus numérique. Face aux menaces sophistiquées d'ingérence étrangère, les modifications à la *Loi sur le SCRS* auraient les effets suivants :

- Permettre au SCRS d'aider la société canadienne à se prémunir contre l'ingérence étrangère;
- Soutenir le SCRS dans sa capacité à recueillir de l'information pour contrer l'ingérence étrangère à l'ère numérique;
- Veiller à ce que la législation en matière de sécurité nationale suive l'évolution des menaces.

À propos des consultations

Le SCRS consultera le public canadien sur la possibilité d'apporter des modifications à la *Loi sur le SCRS* dans des domaines clés, notamment : (1) améliorer la capacité du SCRS à communiquer des renseignements et des conseils à des partenaires non fédéraux; (2) soutenir le SCRS dans sa capacité à recueillir de l'information pour contrer l'ingérence étrangère à l'ère numérique; (3) combler l'écart dans la collecte de renseignements étrangers créé par l'évolution technologique; (4) améliorer la capacité du SCRS à tirer parti de l'analyse des données; et (5) introduire un examen périodique de la *Loi sur le SCRS* afin de mieux suivre l'évolution de la menace. En complément des consultations publiques, le SCRS participera également à des tables rondes avec un large éventail d'intervenants, notamment des organisations de défense des intérêts des communautés, des entreprises, des infrastructures essentielles, des universitaires et des experts en matière de droit, de protection de la vie privée et de transparence.

Les consultations permettront aux Canadiens de participer à une discussion complète et informée sur les outils et les pouvoirs en matière de sécurité nationale. Le SCRS reconnaît que les pouvoirs conférés par la *Loi sur le SCRS* doivent rendre compte des valeurs et des idéaux de ceux qu'il cherche à protéger. Un dialogue avec les Canadiens sur le maintien d'un juste équilibre entre la protection de la sécurité nationale et le respect des attentes des Canadiens en matière de protection de la vie privée est une condition préalable à la réalisation de cet objectif.

Comment participer

Rendez-vous sur notre page sur les consultations [insérer l'hyperlien]. Les consultations se tiendront pendant 60 jours.

Prochaines étapes

Les commentaires issus des consultations auprès du public et des intervenants éclaireront la décision du gouvernement quant aux mesures à mettre en œuvre et à leur forme.

Renseignements connexes

- Document de consultation [insérer l'hyperlien]
- Interférence étrangère

Nous joindre

Sécurité publique Canada
269, avenue Laurier Ouest
Ottawa (Ontario) K1A 0P8
Courriel : À confirmer

TAB C

ENHANCING MEASURES TO COUNTER FOREIGN INTERFERENCE

Foreign Influence Transparency Registry

Updated Public Consultation Paper

Overview / Background

Foreign governments regularly seek to influence the Government of Canada and public opinion in Canada, and often do so through traditional and lawful diplomatic activities. Influence activities undertaken by a foreign principal, when sufficiently transparent, may not pose a significant harm to Canada or Canadians. However, some foreign governments — or their proxies — may leverage individuals or entities to engage in non-transparent, malign foreign influence activities intended to shape Canadian government policy, outcomes, or public opinion, without disclosure of the foreign government ties. These activities could interfere with democratic processes in Canada or result in policy or legislative outcomes unfairly favourable to foreign interests. While Canada has a number of existing tools to support transparency, new measures are being considered, specifically a Foreign Influence Transparency Registry (FITR).

In March 2023, the Prime Minister announced the latest steps in the Government of Canada's plan to address foreign interference. These included establishing a new National Counter Foreign Interference Coordinator at Public Safety Canada to provide sustained central leadership and coordinate efforts to combat foreign interference, and announcing the intent to consult the public to guide the creation of a FITR. Public Safety's consultation paper was published on March 10, 2023, and the public consultation portal closed to new responses on May 9, 2023.

A FITR would increase transparency and general public awareness of foreign influence activities in Canada through, among other provisions, enhanced public disclosure requirements for individuals or entities acting on behalf of foreign principals to influence Canada and Canadians. Additionally, a FITR would help deter malign foreign influence activities by increasing the risk to individuals who would try to avoid registration obligations by designing compliance measures and penalties.

Public and stakeholder feedback indicated broad support for a registry in Canada. Respondents provided meaningful feedback to inform the design of a FITR for Canada, and the Government has taken steps to ensure that a proposal is taking into account the views of the public and stakeholders. A summary of "What We Heard So Far" *[insert hyperlink]* is now available.

The following provides an overview of the Government's approach to a FITR in Canada, currently under consideration and informed by the input from public and stakeholder consultations undertaken to date. We invite reactions and/or comments to help us refine the final form of FITR.

Scope and Obligations

A FITR would need to, at a minimum, impose registration and information disclosure requirements on a number of foreign influence activities. Relevant information provided during the registration process would be made publicly available for Canadians to consult freely.

To trigger a registration requirement, three elements should be present:

1) Foreign Influence Arrangement

Any arrangement between an individual or entity and a foreign principal, where the individual or entity acts at the direction of or in association with a foreign principal to engage in foreign influence activities in relation to a government or political process would be registrable.

A foreign principal would include a foreign power, foreign state, and foreign economic entity as defined in the Security of Information Act.

The foreign influence arrangement itself would be registrable, and disclosure requirements could include providing information on any activities undertaken pursuant to that arrangement. The disclosure obligation is on the individual or entity carrying out the activity, not on the foreign principal.

2) Foreign Influence Activities

The Government is considering three types of activities that may constitute a "foreign influence activity" where undertaken in an arrangement with a foreign principal:

- Communication with a public office holder
- Communication or distribution of information to the public
- Disbursement of money or thing of value

3) Political or governmental processes

The activity that is undertaken pursuant to the foreign influence arrangement would have to be in relation to a political or government process at the federal level or other levels of jurisdiction for the registering obligation to trigger. A political or government process could include:

- Any proceeding of a legislative body;
- The development of any legislative proposal;
- The development or amendment of any policy or program;
- The making of a decision by a public office holder or government body, including the awarding of a contract;
- The holding of an election or referendum; and
- The nomination of a candidate or the development of an electoral platform by a political party.

Exemptions

A limited number of exemptions would be required for the registry to ensure that certain lawful arrangements are not captured. Based on feedback gained during consultations, the Government is considering a smaller number of exemptions as opposed to a larger list. Fewer exemptions would reduce the risk of hostile actors, and their proxies, avoiding registration requirements by finding loopholes in exemptions.

The obligation to register would not apply in these circumstances:

- Foreign nationals who hold passports that contain a valid diplomatic, consular, official or special representative acceptance issued by the Chief of Protocol for the Department of Foreign Affairs, Trade and Development;
- Employees of a foreign principal who are acting openly and in their official capacity; and,
- Arrangements to which His Majesty in Right of Canada is a party.

The Government would also provide that the Governor-in-Council (GIC) may, by regulations, make provision for further exemptions to which registration obligations would not apply.

Application to Provincial, Territorial, Municipal governments and Indigenous organizations

Malign foreign influence is problematic at all levels of society. A Foreign Influence Transparency Registry (FITR) should therefore apply to influence activities directed at all levels of jurisdiction in Canada, including municipal, provincial, and territorial governments, as well as Indigenous groups. This is something that was a clear recommendation throughout the consultation process from both stakeholders and the public. To provide time to properly consult with these other levels of government and indigenous partners, prospective legislation would propose to only bring into force the application of the legislation to the other levels of jurisdiction and indigenous partners at a date to be fixed by the GIC.

Administration

Many respondents in the consultation process were in favour of the FITR being administered by an independent entity to increase trust in the regime, and reduce the risk of political interference. Based on this feedback, the Government is considering designing the registry to be administered by an independent Commissioner appointed for up to seven years by the Governor-in-Council following consultations with the opposition parties in the House of Commons and recognized groups in the Senate.

Compliance

One of the key objectives of the FITR is to promote transparency for foreign influence activities in Canada. To promote compliance with the registration obligations contemplated pursuant to the proposed legislation and to deter non-compliance, certain compliance tools may be proposed. Modern compliance frameworks typically include both civil and criminal sanctions. A FITR would rely primarily on civil sanctions, notably through the use of administrative monetary penalties (AMPs), and reserve criminal sanction for more serious breaches.

First, registrants would be required to update their registration information on a regular basis to ensure the registry presents the most up to date information.

Second, the Government is considering four contraventions that could be included in the statute:

- Failing to register an arrangement with the prescribed timeframe;
- Failing to update arrangement information pursuant to the prescribed timeframe;

- Knowingly providing false or misleading information to the Commissioner; and,
- Obstructing the operation of the registry.

Where it is determined that a violation has occurred, the Commissioner may issue a Notice of Violation noting various information, such as the violation of the legislation, the name of the individual or entity in violation, the proposed penalty, the right to pay the penalty or make representations about the violation and penalty, and if no such action is taken that the individual or entity will be deemed to have committed the violation. In that case, a Notice of Violation and the administrative monetary penalty would be published, including the name of the person or entity found to be in violation of the legislation. Recipients of Notices of Violation would be able to seek a Judicial Review before the Federal Court of Canada.

Notices of violation would need to be codified in legislation as a tool available to the Commissioner to enforce the act, but other notices could be utilized by the Commissioner in the conduct of his or her duties. These would not necessarily need to be written in legislation. For example, the Commissioner may decide to issue compliance notices, which would not necessarily need to be made public, for instances where an individual may be in a registrable arrangement but has yet to register. The purposes of these notices would be to encourage potential registrants to bring themselves into compliance with their obligations.

For more serious contraventions of the FITR, the Commissioner would be able to refer the matter to a law enforcement entity of jurisdiction, who would be able to independently conduct a criminal investigation and refer the matter to the Public Prosecution Service of Canada to take appropriate actions.

Investigative Tools and Information Sharing

The Commissioner would be able to receive complaints or information signaling possible contraventions of the legislation and would exercise its discretion on whether to investigate or to refuse to conduct an investigation. To support its investigations, the Commissioner would rely on a number of tools, including informal investigative approaches and more formal tools, such as the ability to summon and enforce the attendance of persons before the Commissioner and compel them to give oral or written evidence on oath; and, compel persons to produce any documents or other things that the Commissioner considers relevant for the investigation.

Reporting and Oversight

FITR would almost certainly impose a number of reporting and oversight mechanisms to support its proper administration, including an annual reporting requirement by the Commissioner, the content of which would be set out in regulations. Furthermore, the Commissioner's activities would be reviewable by two bodies: the National Security and Intelligence Review Agency (NSIRA) and the National Security and Intelligence Committee of Parliamentarians (NSICOP). Finally, the FITR regime could be reviewable by Parliament every five years.

Ongoing policy refinement: What do you think?

Policy refinement and engagement efforts are ongoing on some aspects of FITR. Below are areas where the Government is seeking additional input from stakeholders.

Application to other levels of jurisdiction

1. Are there specific considerations in extending registration obligations to individuals or entities engaging in foreign influence activities at other levels of jurisdiction or those involving indigenous governance?

Exemptions

2. What is the extent to which legal activities and solicitor-client privilege information should be exempt from registration obligations?

3. Given the scope of the registration obligations, are there other activities that should be exempt from registration obligations?

General:

4. Are there any specific aspects of the proposed model, built on what we've heard to date, that require further refinement?

French Version

AMÉLIORER LES MESURES POUR CONTRER L'INGÉRENCE ÉTRANGÈRE

Registre pour la transparence en matière d'influence étrangère

Document de consultation publique actualisé

Vue d'ensemble et contexte

Les gouvernements étrangers cherchent régulièrement à influencer le gouvernement du Canada et l'opinion publique au Canada, et le font souvent au moyen d'activités diplomatiques traditionnelles et légitimes. Les activités d'influence exercées par un commettant étranger qui, lorsqu'elles sont suffisamment transparentes, peuvent ne pas causer de préjudice important au Canada ou aux Canadiens. Toutefois, certains gouvernements étrangers, ou leurs mandataires, peuvent inciter des personnes physiques ou des entités à participer à des activités d'influence étrangère non transparentes et de nature malveillante visant à façonner la politique du gouvernement canadien, les résultats ou l'opinion publique, sans divulguer leurs liens avec le gouvernement étranger. Ces activités pourraient interférer avec les processus démocratiques du Canada ou entraîner des résultats politiques ou législatifs injustement favorables aux intérêts étrangers. Même si le Canada dispose d'un certain nombre d'outils pour favoriser la transparence, de nouvelles mesures sont à l'étude, en particulier un registre pour la transparence en matière d'influence étrangère (RTMIE).

En mars 2023, le premier ministre a annoncé les dernières mesures définies dans le plan du gouvernement du Canada pour lutter contre l'ingérence étrangère. Ces mesures comprennent notamment la création d'un nouveau poste de coordinateur national de la lutte contre l'ingérence étrangère à Sécurité publique Canada pour assurer un leadership central durable et coordonner les efforts de lutte contre l'ingérence étrangère, et l'annonce de l'intention de consulter le public pour orienter l'établissement d'un RTMIE. Le document de consultation de Sécurité publique Canada a été publié le 10 mars 2023 et le portail de consultation publique a été fermé à la réception des nouvelles réponses le 9 mai 2023.

Un RTMIE accroîtrait la transparence et la sensibilisation du grand public aux activités d'influence étrangère au Canada grâce, entre autres, à des exigences renforcées en matière de communication publique pour les personnes ou entités agissant au nom de commettants étrangers en vue d'influencer le Canada et les Canadiens. En outre, un RTMIE contribuerait à dissuader les activités d'influence étrangère malveillante en augmentant le risque pour les personnes qui essaieraient de contourner les obligations liées à l'inscription en concevant des mesures de conformité et des sanctions.

De façon générale, le public et les intervenants étaient en faveur de la création d'un registre au Canada. Les répondants ont fourni des commentaires utiles pour la conception d'un RTMIE au Canada, et le gouvernement a pris des mesures pour s'assurer qu'une proposition prend en compte les opinions du public et des intervenants. Un résumé du Rapport sur ce que nous avons entendu *[insérer le lien]* est maintenant disponible.

Les paragraphes qui suivent donnent un aperçu de l'approche du gouvernement concernant la création d'un RTMIE au Canada, actuellement à l'étude et éclairée par les commentaires formulés par le public et les intervenants au cours des consultations entreprises à ce jour. Nous vous invitons à nous faire part de vos réactions ou de vos commentaires pour nous aider à mettre au point les derniers détails du RTMIE.

Champ d'application et obligations

Un RTMIE devrait, à tout le moins, imposer des exigences en matière d'inscription au registre et de communication de renseignements pour un certain nombre d'activités d'influence étrangère. Les renseignements pertinents fournis au cours de la procédure d'inscription au registre seraient mis à la disposition du public afin que les Canadiens puissent les consulter librement.

Une obligation d'inscription au registre prendrait forme lorsque trois éléments sont réunis :

1) Entente visant une influence étrangère

Toute entente entre une personne ou entité et un commettant étranger, dans le cadre de laquelle la personne ou l'entité agit sous la direction d'un commettant étranger ou en association avec lui pour se livrer à des activités d'influence étrangère en rapport avec un gouvernement ou un processus politique, serait inscrite au registre.

Un commettant étranger comprendrait une puissance étrangère, un État étranger et une entité économique étrangère, conformément à la définition énoncée dans la *Loi sur la protection de l'information*.

L'entente visant une influence étrangère elle-même devrait être inscrite au registre, et les exigences en matière de divulgation pourraient comprendre la prestation de renseignements sur toutes les activités entreprises dans le cadre de cette entente. L'obligation de divulgation incombe à la personne ou à l'entité qui exerce l'activité, et non au commettant étranger.

2) Activités d'influence étrangère

Le gouvernement envisage trois types d'activités susceptibles de constituer une « activité d'influence étrangère » lorsqu'elles sont entreprises dans le cadre d'une entente avec un commettant étranger :

- la communication avec un titulaire de charge publique;
- la communication ou la diffusion de renseignements au public;
- le versement de sommes d'argent ou le don d'objets de valeur.

3) Processus politiques ou gouvernementaux

L'activité entreprise dans le cadre de l'entente visant une influence étrangère doit être liée à un processus politique ou gouvernemental au niveau fédéral ou à un autre niveau de compétence pour que l'obligation de s'inscrire au registre prenne forme. Un processus politique ou gouvernemental peut comprendre :

- toute procédure d'un organe législatif;
- l'élaboration d'une proposition législative;
- l'élaboration ou la modification d'une politique ou d'un programme;
- la prise de décision par un titulaire de charge publique ou un organisme gouvernemental, y compris l'attribution d'un contrat;
- l'organisation d'une élection ou d'un référendum;

- la nomination d'un candidat ou l'élaboration d'un programme électoral par un parti politique.

Exemptions

Pour garantir que certaines ententes légales ne sont pas prises en compte, le registre devrait compter un nombre limité d'exemptions. D'après les commentaires recueillis dans le cadre du processus de consultation, le gouvernement envisage de réduire le nombre d'exemptions plutôt que d'en dresser une liste plus longue. Un nombre limité d'exemptions réduirait le risque que des acteurs hostiles, et leurs mandataires, se soustraient aux exigences d'inscription au registre en trouvant des failles dans les exemptions.

Les exemptions pourraient comprendre :

- l'étranger titulaire d'un passeport contenant une acceptation valide qui l'autorise à occuper un poste en tant qu'agent diplomatique ou consulaire, ou en tant que représentant officiel ou spécial, délivrée par le chef du protocole du ministère des Affaires étrangères, du Commerce et du Développement;
- les employés d'un commettant étranger qui agissent ouvertement et en leur qualité officielle; et
- les ententes auxquelles Sa Majesté du chef du Canada est partie.

Le gouvernement prévoit également que le gouverneur en conseil peut, par voie réglementaire, prévoir d'autres exemptions auxquelles les obligations liées à l'inscription au registre ne s'appliqueraient pas.

Application aux gouvernements provinciaux et territoriaux, aux administrations municipales et aux organisations autochtones

L'influence étrangère malveillante est inquiétante dans toutes les sphères de la société. Un registre pour la transparence en matière d'influence étrangère (RTMIE) devrait donc s'appliquer aux activités d'influence dirigées vers tous les ordres d'administration au Canada, y compris les gouvernements provinciaux et territoriaux, les administrations municipales et les groupes autochtones. Il s'agit là d'une recommandation claire formulée par les intervenants et le public tout au long du processus de consultation. Afin de disposer du temps nécessaire pour consulter comme il se doit ces ordres de gouvernement et ces partenaires autochtones, le projet de loi proposerait l'entrée en vigueur de l'application de la loi aux autres administrations et aux partenaires autochtones à une date fixée par le gouverneur en conseil.

Administration

De nombreuses personnes interrogées dans le cadre du processus de consultation se sont dites en faveur de l'administration du RTMIE par une entité indépendante afin d'accroître la confiance dans le régime et de réduire le risque d'ingérence politique. Sur la base de ces commentaires, le gouvernement envisage de concevoir un registre qui serait administré par un commissaire indépendant nommé par le gouverneur en conseil pour une période maximale de sept ans, après consultation des partis d'opposition à la Chambre des communes et des groupes reconnus au Sénat.

Conformité

L'un des principaux objectifs du RTMIE est de promouvoir la transparence des activités d'influence étrangère au Canada. Afin de promouvoir le respect des obligations en matière d'inscription au registre prévues dans le projet de loi et de décourager l'inobservation de ces obligations, certains outils de conformité peuvent être proposés. Les cadres de conformité modernes prévoient généralement des sanctions civiles et pénales. Un RTMIE s'appuierait principalement sur des sanctions civiles, notamment par le biais de sanctions administratives pécuniaires (SAP), et réserverait les sanctions pénales aux infractions les plus graves.

Premièrement, les déclarants seraient tenus de mettre à jour régulièrement les renseignements sur leur inscription au registre afin de garantir que le registre présente les renseignements les plus récents.

Deuxièmement, le gouvernement envisage d'inclure quatre infractions dans la loi :

- le défaut d'inscrire une entente au registre dans les délais prescrits;
- le défaut de mettre à jour les renseignements relatifs à l'entente dans les délais prescrits;
- le fait de fournir sciemment des renseignements faux ou trompeurs au commissaire;
- le fait d'entraver le fonctionnement du registre.

Lorsqu'il est établi qu'une violation a été commise, le commissaire peut dresser un procès-verbal de violation dans lequel il consigne divers renseignements, tels que la violation de la loi, le nom de la personne ou de l'entité en infraction, la sanction proposée, le droit de payer la sanction ou de présenter des observations sur la violation et la sanction; si aucune de ces mesures n'est prise, la personne ou l'entité sera réputée avoir commis la violation. Dans ce cas, un avis de violation et la sanction administrative pécuniaire seraient publiés, y compris le nom de la personne ou de l'entité en infraction avec la loi. Les destinataires des avis de violation pourraient présenter une demande de contrôle judiciaire devant la Cour fédérale du Canada.

L'émission d'un avis de violation devrait être codifié dans la loi en tant qu'outil d'application de la loi mis à la disposition du commissaire; cependant, d'autres avis pourraient être utilisés par le commissaire dans l'exercice de ses fonctions. De tels avis ne devraient pas nécessairement être indiqués dans la loi. Par exemple, le commissaire peut décider d'émettre des avis de conformité, qui n'auraient pas nécessairement besoin d'être rendus publics, dans les cas où une personne pourrait être partie à une entente à inscrire au registre dont l'inscription n'a pas encore été faite. Ces avis auraient pour but d'encourager les déclarants potentiels à se conformer à leurs obligations.

En cas d'infractions plus graves relatives au RTMIE, le commissaire aurait le pouvoir de renvoyer l'affaire à une entité d'application de la loi compétente qui serait en mesure de mener une enquête criminelle indépendante et de renvoyer l'affaire au Service des poursuites pénales du Canada afin qu'il prenne les mesures appropriées.

Outils d'enquête et partage des renseignements

Le commissaire pourrait recevoir des plaintes ou des renseignements signalant d'éventuelles infractions à la loi et il exercerait son pouvoir discrétionnaire pour enquêter ou refuser d'enquêter. Pour soutenir ses enquêtes, le commissaire s'appuierait sur un certain nombre d'outils, y compris des techniques d'enquête informelles et des outils officiels, comme la capacité d'assigner et de contraindre des personnes à comparaître devant lui, de les enjoindre à déposer oralement ou par écrit sous la foi du

serment, et de produire les documents et autres pièces qu'il juge nécessaires en vue de mener l'enquête.

Établissement de rapports et mécanismes de surveillance

La mise en place d'un RTMIE serait très certainement accompagnée d'un certain nombre de mécanismes de surveillance obligatoires afin de soutenir sa bonne administration, y compris une exigence de produire un rapport annuel par le commissaire, dont le contenu serait défini par règlement. En outre, les activités du commissaire pourraient être examinées par l'Office de surveillance des activités en matière de sécurité nationale et de renseignement (OSSNR) et le Secrétariat du Comité des parlementaires sur la sécurité nationale et le renseignement (CPSNR). Enfin, le RTMIE pourrait être examiné par le Parlement tous les cinq ans.

Raffinement continu des politiques : Qu'en pensez-vous?

Des efforts de raffinement des politiques et d'engagement sur certains aspects du RTMIE sont en cours. Vous trouverez ci-dessous les domaines dans lesquels le gouvernement souhaite obtenir une contribution additionnelle des intervenants.

Application à d'autres ordres d'administration

1. Existe-t-il des considérations particulières concernant l'élargissement des obligations en matière d'inscription au registre aux personnes ou aux entités exerçant des activités d'influence étrangère à d'autres ordres d'administration ou des activités concernant la gouvernance autochtone?

Exemptions

2. Dans quelle mesure les activités légales et les renseignements protégés par le secret professionnel liant l'avocat à son client devaient-ils être exemptés des obligations liées à l'inscription au registre?

3. Compte tenu de la portée des obligations liées à l'inscription au registre, existe-t-il d'autres activités qui devraient être exemptées de ces obligations?

Généralités :

4. Compte tenu de ce que nous avons entendu jusqu'à présent, existe-t-il des aspects particuliers du modèle proposé qui devraient être affinés?

TAB D

ENHANCING MEASURES TO COUNTER FOREIGN INTERFERENCE PUBLIC CONSULTATION PAPER

WHETHER TO AMEND THE *CANADIAN SECURITY INTELLIGENCE SERVICE ACT*

Today's Evolving Threat Landscape

As an advanced economy and open democracy, Canada is targeted by foreign states, or those acting on their behalf, who seek to advance their strategic objectives. While foreign states may advance their interests in legitimate and transparent ways, some also act in ways that threaten or intimidate people in Canada, their families elsewhere, or are covert and deceptive, and harmful to Canada's national interests.

Canadian human rights activists and dissidents exercising their constitutionally-protected freedom of expression are prime targets of state-backed threats of intimidation. Influence and harassment are used to pressure diverse Canadian communities to act in the interests of foreign states. State actors target and obtain the personal information of Canadians to enable their foreign interference activities across all sectors. State actors also attempt to target provincial, territorial, municipal, and Indigenous governments, who have limited access to federal intelligence assessments.

Technology enables and accelerates these threats, especially in the online space, where widely available secure applications and tools like virtual private networks (VPNs) and end-to-end encryption, which help to protect the privacy of Canadians and Canadian companies, make threat actors difficult to detect and identify. Not only has technology changed, but Canadians expectation of privacy relating to data and technology has also changed. CSIS' authorities were, however, written in 1984, at a time when the prolific use and expansion of digital technology could not have been foreseen; and since then the *CSIS Act* has only seen targeted amendments.

To investigate the aggressive and corrosive foreign interference that Canada faces today requires that CSIS has a toolkit appropriate for modern technology and modern day threats. Amendments to the *CSIS Act* would better equip CSIS to carry out its mandate to investigate, advise the Government of Canada, and take measures to reduce threats to the security of Canada.

CSIS' Role in Protecting Canada's National Security

CSIS is mandated to:

- Investigate activities suspected of constituting threats to the security of Canada (espionage/sabotage, foreign interference, terrorism, subversion of Canadian democracy) and reports on these to the Government of Canada;
- Take measures to reduce these threats;

- Provide security assessments on individuals who require access to sensitive government information or sensitive sites;
- Provide security advice relevant to the *Citizenship Act* or the *Immigration and Refugee Protection Act*; and
- Collect foreign intelligence within Canada at the request of the Minister of Foreign Affairs or the Minister of National Defence.

CSIS intelligence is used to advise the Government of Canada. For example, espionage and foreign interference intelligence informs best practices in safeguarding critical infrastructure, federally-funded science, and Canadian innovation. Information from CSIS' investigations can also be directed to the Royal Canadian Mounted Police to inform national security criminal investigations.

While CSIS provides critical intelligence to the Government of Canada to respond to foreign interference, there are limitations to CSIS' authorities, which hinder Canada's ability to face the sophisticated and aggressive tactics seen today.

Principles Guiding *CSIS Act* Amendments

The authorities in the *CSIS Act* must reflect the values and ideals of Canadians, whom CSIS seeks to protect. A pre-requisite to amending the *CSIS Act* is an informed conversation with Canadians about what role CSIS should play as a modern civilian intelligence service.

CSIS wants to hear your views on how CSIS should continue to protect Canada's national security, while also continuing to protect the rights and freedoms of people in Canada.

The proposals for amendments seek to enhance CSIS' authorities to better counter foreign interference and protect Canada's national security in a digital world. *CSIS Act* amendments would help to:

- Enable CSIS to disclose information to those outside the Government of Canada for the purpose of increasing awareness and resiliency against foreign interference;
- Create new judicial authorization authorities tailored to the level of intrusiveness of the techniques;
- Close the gap created by technological evolution, and regain the ability for CSIS to collect, from within Canada, foreign intelligence about foreign states and foreign individuals in Canada;
- Enhance CSIS' capacity to capitalize on data analytics to investigate threats; and
- Ensure that national security legislation keeps pace with evolving threats and Canadians evolving expectation of privacy.

Safeguards

CSIS is committed to increasing transparency to ensure that the Canadian public has trust in their security intelligence service. Maintaining systems of review, oversight, and transparency will remain primary objectives with any *CSIS Act* amendments. The rights and freedoms of people in Canada are a cornerstone of Canadian democracy and a principal consideration in CSIS' work. CSIS has multiple layers of protections to ensure respect for the rights of people in Canada, which are protected under the *Canadian Charter of Rights and Freedoms* (the *Charter*). For instance, CSIS is required to seek a Federal Court warrant before undertaking activities that are more than minimally intrusive, and undergoes non-judicial rigorous external review. The National Security and Intelligence Review Agency, and the National Security and Intelligence Committee of Parliamentarians provide a review function for CSIS' activities. Other CSIS activities are subject to the review and approval of the Intelligence Commissioner, who acts as a quasi-judicial oversight body.

The following key principles would guide any possible *CSIS Act* amendments:

Trusted: Protect individuals' rights and freedoms in line with the *Charter* and Canadians' expectations.

Accountable: Comply with the rule of law and judicial oversight; ensuring accountability to the Government of Canada and the Canadian public.

Reliable: Support the Government of Canada in protecting Canada's national security, and remain a reliable and trusted partner both domestically and internationally.

Responsible steward: Use Government resources effectively to advance CSIS operations in a technologically advanced world.

Prepared: Equipped to respond to the threats of tomorrow.

Issue #1: Whether to enable CSIS to disclose information to those outside the Government of Canada for the purpose of increasing awareness and resiliency against foreign interference

Context

At the time of enacting the *CSIS Act*, national security was strictly the purview of the federal government, where espionage and foreign interference targeted military technology and federal government institutions. For that reason, CSIS is authorized to collect, retain, and provide necessary intelligence to the Government of Canada to make decisions to protect Canada's national security. Today, foreign interference impacts every level of government and all sectors of society, including Canadian communities, academia, the media, and private enterprises. CSIS' expertise and intelligence are increasingly relevant to those outside of the federal government, and these partners turn to CSIS more than ever for information. While national security remains a federal responsibility, it is clear that countering foreign interference requires a whole-of-society effort.

What is the issue?

The *CSIS Act* does not provide CSIS with sufficient authority to disclose classified intelligence to domestic partners outside the Government of Canada. This means that CSIS generally cannot share relevant information with provinces, territories, Indigenous governments, or municipalities, except in limited situations, such as for the purposes of law enforcement or when they can take action that would reduce a specific threat further to CSIS' threat reduction mandate (TRM). CSIS uses its TRM mandate to communicate information with partners outside of the Government of Canada in an effort to reduce specific threats, when other means are not available. However, the TRM mandate is meant for reducing specific threats, and not for disclosing information for the purpose of building awareness.

Prohibitions on disclosure also limit how CSIS can share relevant information with private sector and academic institutions. Such limitations prevent CSIS from directly sharing information that could help these partners build resilience to foreign interference and espionage threats.

Given the rise in threats facing Canada, CSIS has made significant efforts to increase outreach and awareness of threats. However, as the *CSIS Act* limits the disclosure of threat-related information, CSIS provides high-level, unclassified, and general threat briefings to those who are the target of foreign interference, but are outside of the Government of Canada. CSIS' inability to communicate more specific and tangible information prevents a full and frank discussion of threats, limiting partners' ability to develop informed mitigation measures or build resiliency.

With *CSIS Act* amendments, CSIS' information could help partners be more aware of the threats they face, be able to better identify specific foreign interference techniques, and take protective measures to withstand foreign interference.

Potential area for legislative change

CSIS would be authorized to disclose information to other entities or persons, in addition to the Government of Canada, on threats to the security of Canada, for the purpose of increasing awareness and resiliency against threats to the security of Canada. With a broader disclosure authority, CSIS would also implement safeguards recognizing the need to maintain privacy protections, as well as protect CSIS' investigative techniques and sources.

What Do You Think?

1) Should CSIS be authorized to disclose information to those outside of the Government of Canada to build resiliency against threats, such as foreign interference?
2) In your view, what considerations should apply to the sharing of information with those outside of the Government of Canada about the threats they face? What type of limits should there be on when and with whom CSIS can share information?

Issue #2: Whether to implement new judicial authorization authorities tailored to the level of intrusiveness of the techniques

Context

CSIS collects minimally intrusive information under its section 12 or 16 mandate. When the collection is more than minimally intrusive, CSIS uses its section 21 authority to obtain warrants from the Federal Court. Prior to applying for warrants, CSIS must consult the Deputy Minister of Public Safety, and the Minister of Public Safety must authorize the making of the application to the Federal Court. Section 21 has always required all warrant applications to satisfy the same requirements, even though investigative techniques can vary greatly in their relative degree of intrusiveness. Section 21 provides for a single warrant authority, featuring requirements that are appropriate for the most intrusive investigative techniques. Performing a single collection activity (e.g., a single examination of a USB) would require CSIS to meet the same requirements as obtaining a warrant authorizing more extensive warrant powers (e.g., authorizing the ongoing interception of private communications) that can be executed repeatedly for a year.

What is the issue?

CSIS' warrant authority requires that regardless of the type of warranted techniques CSIS wants to employ, the warrant application must demonstrate that non-warranted investigative techniques have been tried and failed, or why they are unlikely to succeed or impracticable in urgent circumstances, or that information of importance will not be obtained without the warrant. These elements are referred to collectively as the "investigative necessity" requirements. This means that whether CSIS is seeking a warrant to obtain the name and address of an individual behind an IP address or the call detail records from a device, or to intercept an individual's private communications for up to a year, the same requirements apply.

Similarly, CSIS is required to meet the same strict requirements for a warrant authorizing CSIS to receive and examine the contents of a device one time (e.g., a USB key), as to conduct repeated examinations of an individual's devices or the interception of communications to and from those devices for up to a year. CSIS also lacks a separate authority to compel an entity to preserve perishable information (e.g., financial transaction data that would otherwise need to be deleted by the financial institution). This means that information of importance to an investigation could be lost while CSIS takes the necessary steps to obtain a section 21 warrant.

By contrast, law enforcement investigators have access to a variety of warranted powers tailored to the level of intrusiveness of the techniques being requested. There are important differences between CSIS' authorities and those available to law enforcement, such as the fact subjects of law enforcement warrants often receive notice and can more easily challenge these warrants whereas the subjects of CSIS warrants may never know for national security reasons. At the same time, CSIS is subject to strong Ministerial and review body oversight, something that law enforcement does not have comparably. Nonetheless, over the years, the *Criminal Code* has seen amendments to allow for greater flexibility while still ensuring effective judicial oversight. For example, the production order provisions were introduced to *Criminal* Code in 2004. In addition, in the context of a criminal investigation, demonstrating "investigative necessity" is frequently a requirement when law enforcement investigators seek to intercept private communications or intrusive video surveillance, but not for all warranted collection methods.

Potential area for legislative change

New tailored judicial authorization provisions could be considered, alongside CSIS' existing warrant authority, for specific investigative techniques. This could include a preservation order authority, which would allow CSIS to obtain a judicial authorization compelling a third party to preserve perishable information that CSIS has reasonable grounds to suspect will assist with an intelligence investigation, before seeking a production order or warrant to obtain the information, but without CSIS having to demonstrate the investigative necessity requirement to the court.

Another new tool that could streamline CSIS' ability to investigate threats is a production order authority, which would enable CSIS to compel a third party to produce information where CSIS has reasonable grounds to believe that the production of the information is likely to yield information of importance that is likely to assist CSIS in carrying out its duties and functions. The production order could be used to obtain information such as basic subscriber information, call detail records, or transaction records. A new tailored warrant authority could assist the Service in conducting a single collection activity, like obtaining and examining a USB stick. These types of single collection activities are inherently more predictable in terms of their impact on privacy interests – and as a result less privacy intrusive – than the types of activities that may be authorized under existing warrant powers, which can encompass all investigative techniques and continued collection for up to a year. This authority would still require CSIS to have reasonable grounds to believe that the collection activity is likely to yield information of importance that is

likely to assist CSIS' duties and functions under sections 12 or 16 of the *CSIS Act*, while continuing to provide effective judicial oversight.

Lastly, it may be impracticable at times for the Minister of Public Safety to authorize a CSIS warrant application. This could be for a number of reasons, including that the Minister is outside of the country and unable to review a time-sensitive application. In such instances, the Minister's authorization power could be delegated to enable CSIS to obtain the necessary warrants from the Federal Court to advance its national security investigations.

What Do You Think?

1) Should CSIS be able to compel an entity to preserve perishable information when it intends to seek a production order or a warrant to obtain that information?
2) Should CSIS be able to compel production of information when it reasonably believes that the information is likely to yield information of importance that is likely to assist in the performance of its duties and functions under sections 12 or 16 of the *CSIS Act*?
3) Should CSIS be able to conduct a single collection activity, like a one time collection and examination of a USB reasonably believed to contain threat-related information, without having to demonstrate investigative necessity? If yes, what requirements should CSIS have to meet for seeking different warrant powers?
4) In situations where the Minister of Public Safety is unable to authorize the making of a CSIS application for judicial authorization to the Federal Court and where the matter cannot wait, should there be a mechanism to delegate this authority? If yes, who should this authority be delegated to and in what types of situations should this apply to?

Issue #3: Whether to close the gap, created by technological evolution, and regain the ability for CSIS to collect, from within Canada, foreign intelligence about foreign states and foreign individuals in Canada

Context

Section 16 of the *CSIS Act* authorizes CSIS to collect, at the request of the Minister of Foreign Affairs or the Minister of National Defence, information relating to foreign states and persons (i.e., foreign intelligence) "within Canada." Technology has drastically evolved since the adoption of section 16 in 1984, and Parliament could not have foreseen how the "within Canada" geographic limitation would restrict foreign intelligence collection given how information today is largely digital and borderless.

What is the issue?

In 1984, through the *CSIS Act,* Parliament provided CSIS with its section 16 foreign intelligence assistance mandate. Parliament recognized that the collection of foreign intelligence in Canada

requires expertise, which was best provided by CSIS. However, Parliament limited this mandate to collection "within Canada," as it did not want CSIS to collect foreign intelligence abroad. Furthermore, the *Communications Security Establishment Act* explicitly prohibits the Communications Security Establishment (the CSE) from directing any of its collection activities at a Canadian or any person in Canada.

The Federal Court and Federal Court of Appeal (2018 FC 738, 2018 FCA 207, 2020 FC 757, 2021 FCA 165) have interpreted the "within Canada" limitation to mean that CSIS cannot collect information relating to foreign states and persons, from within Canada, when that information is located outside of Canada. Because of technological advancements, these decisions have reduced CSIS' visibility on the activities of foreign states or foreign individuals within Canada's borders when electronic information is located outside of Canada. The Courts have made it clear that "recalibrating the investigative techniques open to the Service [under section 16 of the *CSIS Act*] in light of significant technological change is a matter for Parliament and not the courts" (2021 FCA 165, para 6).

The wording of the *CSIS Act* and the *CSE Act* create a foreign intelligence gap. Closing this gap is critical to supporting the Government of Canada in managing Canada's foreign relations and national defence by understanding the capabilities, intentions or activities of foreign states or foreign individuals, who may be involved in foreign interference activities.

Potential area for legislative change

Regain an ability, lost largely due to technological advancements, for CSIS to collect, from within Canada, foreign intelligence about foreign states, and foreign individuals in Canada, which resides outside Canada, while still maintaining the other existing limitations. The collection has to be at the request of the Minister of Foreign Affairs or Minister of National Defence, with the consent of the Minister of Public Safety, and subject to the Federal Court's authorization and conditions. In addition, any collection under section 16 cannot be directed at Canadian citizens, permanent residents, or corporations incorporated in Canada.

What Do You Think?

1) Should the *CSIS Act* be amended so that CSIS' ability to collect foreign intelligence at the request of Ministers can keep pace with the evolution of technology, which creates digitally borderless information? If so, what should be the limitations?

Issue #4: Whether to amend the *CSIS Act* to enhance CSIS' capacity to capitalize on data analytics to investigate threats in a modern era

Context

The authority outlined in sections 11.01 to 11.25 of the *CSIS Act*, commonly referred to as the dataset regime, was introduced as part of Bill C-59 as an acknowledgement that data and

technology had re-shaped the threat and investigatory landscape, as well as in response to the Federal Court's "associated data" decision (2016 FC 1105). The regime was meant to provide CSIS with the authority to collect, retain, and use datasets that are not "directly and immediately related" to a threat to the security of Canada, but that may assist in CSIS' duties and functions under sections 12 to 16 of the *CSIS Act*. The regime includes numerous safeguards and protections to minimize the personal and private information of individuals in collected datasets, especially for Canadians and individuals in Canada.

What is the issue?

Despite the introduction of the dataset regime, CSIS' ability to retain and use datasets, even when the relevance to CSIS' mandate is clear and obvious, is limited.

The 90-day evaluation period is one of several requirements that hinders the ability to make use of this regime. Specifically, when CSIS collects a dataset, a strict 90-day evaluation period starts, during which CSIS must complete a series of tasks, including translation, decryption, applying privacy protections, and organizing the data. If it is a foreign dataset, CSIS must also, during the 90-day evaluation period, remove the Canadian records to either delete them or constitute a separate Canadian dataset. CSIS must also prepare and submit the requisite application for Ministerial or judicial authorization to retain the dataset within the same 90-days. Should CSIS be unable to fully evaluate the dataset and prepare and submit the requisite application for retention within the 90-day timeline, it must destroy the dataset.

For example, a trusted partner could provide the Service with a dataset of information (accounts, contact information, relationships) from a country known to engage in foreign interference. The information predominantly relates to non-Canadians outside Canada (foreign information), though the dataset may also contain some Canadian information. Under the legislation, foreign datasets and Canadian datasets have different pathways for approval and retention. For CSIS to retain the totality of this information under the dataset regime, it would need to evaluate the foreign dataset within the 90-day evaluation period, including removing any Canadian information, and request authorization from the Minister of Public Safety to retain the foreign dataset; the Intelligence Commissioner must also review and approve the Minister's authorization. Separately, CSIS would be required to obtain the Minister's approval to make an application to the Federal Court for authorization to retain the Canadian information as a Canadian dataset. Prior to doing so, the Service must reasonably believe that the Canadian information would belong to an approved class of Canadian datasets. The totality of this process could require up to five separate submissions for review by the Minister, Intelligence Commissioner, and/or the Court, resulting in a delay of up to six to nine months before CSIS can exploit the data, by which time its intelligence value may have diminished significantly. If CSIS cannot evaluate and apply to retain the dataset within the statutory time limit, it is required to destroy all the data.

The regime also contains certain ambiguities that have hindered CSIS' ability to leverage datasets in the way Parliament intended, and have the potential to derogate from CSIS' duties and

functions under sections 12 and 16 of the *CSIS Act*. Clarifying these ambiguities with select amendments would improve the viability of the regime and provide the clarity required to avoid multiple legal interpretations.

Other limitations in the dataset regime result in lost opportunity and value. For example, CSIS is currently unable to query or exploit Canadian datasets for the provision of security assessments or screening advice under section 15 of the *CSIS Act*. As part of screening applications, applicants must provide their education and employment histories, among other information, which supports the assessment of loyalty. Efforts by an applicant to hide or omit their association with certain institutions can be relevant to a screening investigation. A Canadian dataset of individuals in Canada that have studied at a university associated with a foreign military could not be queried for the purpose of a screening investigation.

CSIS works with many domestic partners like CSE and the RCMP in furtherance of its national security mandate. The datasets that CSIS may be able to collect under the regime could be relevant to the mandate of other agencies. However, CSIS is unable to share those datasets with partner departments because the regime does not contemplate the sharing of whole datasets. This limitation also hinders cooperation with foreign partners in relation to datasets that could be of mutual relevance, such as a dataset that, although not directly related to a threat, is likely to assist in the investigation of a state known to engage in aggressive foreign interference tactics.

Potential area for legislative change

The Government could introduce targeted amendments to the dataset regime to alleviate some of the more challenging elements by, for example, permitting extensions of the evaluation period, as well as increasing the duration of the determination of classes of Canadian datasets and/or authorizations to retain foreign and Canadian datasets.

Other amendments could clarify that the dataset regime only applies to datasets that do not fall under any other *CSIS Act* authority, that the classes of Canadian datasets must be valid only at collection, and to enable foreign datasets that contain Canadian information to be treated as Canadian datasets (the more stringent process of the two) to avoid multiple applications for authorization. Further amendments could also enable CSIS to share datasets under strict conditions and could enable CSIS to query or exploit Canadian datasets for section 15 screening investigations.

What do you think?

1) How could CSIS increase its ability to collect and use datasets in a timely and relevant manner, while respecting protected *Charter* rights, in a data-driven world?
2) Should CSIS be able to query or exploit Canadian datasets for section 15 purposes? If so, do you think there should be additional safeguards or limitations in place?

3) Should CSIS be able to share Canadian or foreign datasets with domestic partners who have the lawful authority to collect the type of information contained in the dataset? If so, what safeguards or conditions should be in place, if any?

4) Should CSIS be allowed to share foreign datasets with foreign partners? If so, what safeguards or conditions should be in place, if any?

Issue #5: Whether to introduce a requirement to review the *CSIS Act* on a regular basis so that CSIS may keep pace with evolving threats

Context

The threat environment facing Canada is in a constant state of evolution, and Canada needs to ensure it has the tools necessary to detect and address national security threats. However, *CSIS Act* amendments are ad-hoc as there is no provision requiring statutory review.

What is the issue?

Unlike the majority of Canada's allied partners, there is no statutory requirement to review the *CSIS Act* on a regular basis to ensure that the Act keeps pace with technology and data, and their impact on national security threats. As a result, CSIS' authorities are prone to falling out of date, leaving Canada and Canadians vulnerable.

Better equipping CSIS to address the threats of today, but also the threats of the future is critical for protecting Canada and Canadians national security. Up to date authorities also bolster CSIS and Canada's ability to engage with allies, maintaining Canada's reputation as a trusted partner in the fight against national security threats that more frequently cross-borders.

Potential area for legislative change

Introduce a statutory requirement for Parliament to periodically review the *CSIS Act*.

What Do You Think?

1) Should legislation require that CSIS' authorities be regularly reviewed to keep pace with technological advances and Canada's adversaries? If so, how often?

2) Do you have any other views to share regarding the development and possible amendments to the *CSIS Act*?

French Version

RENFORCER LES MESURES VISANT À CONTRER L'INGÉRENCE ÉTRANGÈRE

DOCUMENT DE CONSULTATION PUBLIQUE

FAUT-IL MODIFIER LA *LOI SUR LE SERVICE CANADIEN DU RENSEIGNEMENT DE SÉCURITÉ*?

Évolution du contexte actuel de la menace

En tant que démocratie libre et ouverte jouissant d'une économie développée, le Canada est la cible d'États étrangers, ou d'acteurs agissant en leur nom, qui cherchent à servir leurs objectifs stratégiques. Pour ce faire, certains de ces États emploient des moyens transparents et légitimes, tandis que d'autres menacent ou intimident des personnes au Canada et leurs familles ailleurs dans le monde, ou mènent des activités clandestines et trompeuses qui nuisent aux intérêts nationaux du Canada.

Les défenseurs des droits de la personne et les dissidents qui exercent leur liberté d'expression, un droit protégé par la Constitution, sont les principales cibles des manœuvres d'intimidation appuyées par des États. L'ingérence et le harcèlement sont utilisés pour pousser des membres de diverses communautés au Canada à servir les intérêts d'États étrangers. Des acteurs étatiques parviennent à obtenir les renseignements personnels de Canadiennes et de Canadiens pour mener des activités d'ingérence étrangère dans tous les domaines. Ils tentent aussi de prendre pour cible les gouvernements provinciaux, territoriaux, municipaux et autochtones, qui n'ont qu'un accès limité aux évaluations fédérales du renseignement.

La technologie facilite et intensifie ces menaces, notamment en ligne, où il est difficile de repérer et d'identifier les auteurs de menace en raison de la grande disponibilité des applications et des outils sécurisés, comme les réseaux privés virtuels (RPV) et le chiffrement de bout en bout, que la population et les entreprises canadiennes utilisent pour protéger leurs renseignements personnels. Non seulement la technologie a changé, mais les attentes de la population canadienne en matière de confidentialité concernant les données et la technologie ont elles aussi évolué. Or, le SCRS dispose de pouvoirs qui lui ont été accordés en 1984, à une époque où l'omniprésence et le développement des technologies numériques étaient imprévisibles. Depuis, la *Loi sur le SCRS* (la *Loi*) n'a été modifiée que de façon ciblée.

Pour enquêter sur l'ingérence étrangère insistante et néfaste que subit le Canada aujourd'hui, le SCRS a besoin d'outils adaptés à la technologie et aux menaces modernes. Modifier la *Loi* doterait ce dernier de moyens mieux adaptés à sa mission, qui est d'enquêter sur les menaces pesant sur la sécurité nationale, de conseiller le gouvernement du Canada à ce sujet et de prendre des mesures visant à atténuer ces menaces.

Rôle du SCRS en matière de protection de la sécurité nationale du Canada

Le SCRS a pour mission :

- d'enquêter sur les activités soupçonnées de constituer des menaces pour la sécurité du Canada (espionnage ou sabotage, ingérence étrangère, terrorisme et subversion de la démocratie canadienne) et d'informer le gouvernement du Canada à leur sujet;
- de prendre des mesures visant à atténuer ces menaces;
- de fournir des évaluations de sécurité sur les personnes qui doivent accéder à des informations ou à des sites sensibles du gouvernement du Canada;
- de donner des conseils de sécurité en rapport avec la *Loi sur la citoyenneté* ou la *Loi sur l'immigration et la protection des réfugiés*;
- de recueillir des renseignements étrangers, dans les limites du Canada, à la demande des ministres des Affaires étrangères ou de la Défense nationale.

Les renseignements communiqués par le SCRS servent à conseiller le gouvernement du Canada. Par exemple, ceux qui concernent l'espionnage et l'ingérence étrangère sont employés pour déterminer les pratiques exemplaires en matière de protection des infrastructures, de travaux scientifiques financés par le gouvernement fédéral et d'innovation canadienne. Le SCRS peut aussi transmettre à la Gendarmerie royale du Canada (GRC) des informations tirées de ses enquêtes qui sont utiles à des enquêtes criminelles liées à la sécurité nationale.

Si le SCRS fournit au gouvernement du Canada des renseignements essentiels qui l'aident à combattre l'ingérence étrangère, ses pouvoirs sont limités, ce qui amoindrit la capacité du Canada de lutter contre les tactiques complexes et offensives utilisées aujourd'hui.

Principes directeurs de la modification de la *Loi sur le SCRS*

Les pouvoirs conférés par la *Loi* doivent tenir compte des valeurs et des idéaux de la population canadienne, que le SCRS cherche à protéger. Avant de modifier la *Loi*, il faut avoir une discussion éclairée avec la population pour obtenir son avis sur le rôle que le SCRS devrait jouer à titre de service de renseignement moderne et civil.

Le SCRS souhaite recueillir votre avis sur la façon dont il devrait continuer à protéger la sécurité nationale du Canada, tout en continuant à protéger les droits et les libertés de la population.

Les modifications proposées visent à doter le SCRS de pouvoirs mieux adaptés à la lutte contre l'ingérence étrangère et à la protection de la sécurité nationale dans un monde numérique. Elles contribueraient à :

- permettre au SCRS de communiquer des informations aux intervenants extérieurs au gouvernement du Canada, afin d'accroître la sensibilisation et la résilience contre l'ingérence étrangère;

- créer de nouveaux pouvoirs nécessitant l'obtention d'une autorisation judiciaire parfaitement adaptés au degré d'intrusion propre aux techniques à utiliser;
- combler l'écart creusé par les progrès technologiques et rétablir la capacité du SCRS de recueillir depuis le Canada des renseignements étrangers sur d'autres États et des ressortissants étrangers qui se trouvent au Canada;
- renforcer la capacité du SCRS de tirer parti de l'analyse des données pour enquêter sur les menaces;
- veiller à ce que les lois sur la sécurité nationale évoluent aussi vite que les menaces et les attentes de la population canadienne en matière de respect de la vie privée.

Mesures de protection

Le SCRS tient à accroître sa transparence pour que la population canadienne ait confiance en son service du renseignement de sécurité. Quelles que soient les modifications apportées à la *Loi*, le maintien des dispositifs d'examen, de surveillance et de transparence demeurera une priorité. Les droits et les libertés de la population canadienne sont au cœur même de la démocratie canadienne et leur respect est une considération majeure pour le SCRS dans le cadre de son travail. Le SCRS fait l'objet de nombreuses mesures visant à garantir le respect des droits de la population canadienne, qui sont protégés par la *Charte canadienne des droits et libertés* (la *Charte*). Par exemple, il est tenu d'obtenir un mandat de la Cour fédérale avant de mener des activités de collecte plus que minimalement envahissantes. Il doit également se soumettre à un examen externe non judiciaire rigoureux. L'Office de surveillance des activités en matière de sécurité nationale et de renseignement et le Comité des parlementaires sur la sécurité nationale et le renseignement examinent ses activités. D'autres de ses activités sont assujetties à l'examen et à l'approbation du commissaire au renseignement, organe de surveillance quasi judiciaire.

Les principes clés ci-dessous seraient utilisés pour orienter les modifications de la *Loi* :

Confiance : Protéger les droits et les libertés des citoyens, conformément à la *Charte* et aux attentes de la population.

Responsabilité : Agir conformément à la primauté du droit et aux exigences en matière de contrôle judiciaire et rendre des comptes au gouvernement et à la population du Canada.

Fiabilité : Aider le gouvernement fédéral à protéger la sécurité nationale, et demeurer un partenaire solide et digne de confiance tant au pays et qu'à l'étranger.

Gestion responsable : Utiliser adéquatement les ressources du gouvernement de façon à faire progresser les opérations du SCRS dans un monde avancé sur le plan technologique.

Préparation : Disposer des outils nécessaires pour contrer les menaces de demain.

Question nº 1 : Faut-il autoriser le SCRS à communiquer des informations à des personnes ou à des organisations extérieures au gouvernement du Canada pour renforcer la sensibilité et la résilience à l'ingérence étrangère?

Contexte

Lorsque la *Loi* a été adoptée, la sécurité nationale relevait exclusivement du gouvernement fédéral, car les activités d'espionnage et d'ingérence étrangère prenaient alors pour cible les technologies militaires et les institutions fédérales. Pour cette raison, le SCRS est autorisé à recueillir, à conserver et à communiquer les renseignements nécessaires au gouvernement du Canada pour l'aider à prendre des décisions visant à protéger la sécurité nationale. Aujourd'hui, l'ingérence étrangère touche tous les ordres de gouvernement et tous les pans de la société, notamment les communautés canadiennes, le milieu universitaire, les médias et les entreprises privées. L'expertise et les renseignements du SCRS sont de plus en plus utiles aux personnes et aux organisations extérieures au gouvernement fédéral, et ces partenaires se tournent plus que jamais vers le SCRS pour obtenir des informations. La sécurité nationale demeure une compétence fédérale, mais il ne fait aucun doute que la lutte contre l'ingérence étrangère nécessite un effort concerté de toute la société.

Quel est le problème?

La *Loi* n'autorise pas le SCRS à communiquer des renseignements classifiés à des partenaires canadiens extérieurs au gouvernement du Canada. Autrement dit, en règle générale, le SCRS ne peut transmettre d'informations pertinentes aux provinces, aux territoires, aux municipalités ou aux gouvernements autochtones, sauf dans certaines situations (p. ex., pour les besoins des forces de l'ordre ou lorsque ces partenaires peuvent agir pour atténuer une menace précise, en vertu du mandat qu'a le SCRS de prendre des mesures de réduction de la menace [MRM]). Il arrive que le SCRS se serve de ses pouvoirs relatifs aux MRM pour fournir des informations à des partenaires extérieurs au gouvernement du Canada en vue d'atténuer des menaces précises, lorsqu'il n'y a pas d'autres solutions possibles. Toutefois, les MRM ne doivent pas servir à communiquer des informations à des fins de sensibilisation, mais à affaiblir une menace donnée.

Cette interdiction limite aussi les informations utiles que le SCRS peut transmettre au secteur privé et aux établissements universitaires. Cela empêche le SCRS de communiquer directement à ces partenaires des informations qui pourraient les aider à renforcer leur résilience face aux menaces associées à l'ingérence étrangère et à l'espionnage.

Devant la multiplication des menaces visant le Canada, le SCRS a déployé des efforts considérables pour accroître la collaboration et la sensibilisation à ces menaces. Cependant, comme la *Loi* limite les informations qu'il peut communiquer, il offre des séances d'information générales, de haut niveau et non classifiées sur la menace aux personnes et aux organisations extérieures au gouvernement du Canada qui sont visées par l'ingérence étrangère. Son incapacité à transmettre des informations précises et concrètes fait obstacle à des discussions franches sur toute

l'ampleur et la nature des menaces, donc empêche ses partenaires de prendre des mesures d'atténuation éclairées et d'accentuer leur résilience.

Une fois la *Loi* modifiée, les informations données par le SCRS pourraient aider ses partenaires à mieux connaître les menaces qui pèsent sur eux, à mieux repérer certaines techniques d'ingérence étrangère et à prendre des mesures de protection pour y résister.

Changement législatif possible

Le SCRS serait autorisé à transmettre des informations sur les menaces pour la sécurité nationale à des personnes ou à des organisations extérieures au gouvernement du Canada, afin de renforcer la sensibilité et la résilience aux menaces pour la sécurité du pays. S'il pouvait communiquer plus largement ces informations, il prendrait des mesures répondant au besoin de protéger à la fois les renseignements personnels et ses techniques d'enquête et ses sources.

Qu'en pensez-vous?

1) Faut-il autoriser le SCRS à fournir des informations à des personnes ou à des organisations extérieures au gouvernement du Canada pour renforcer leur résilience aux menaces, notamment à l'ingérence étrangère?
2) À votre avis, quelles considérations devraient s'appliquer à la communication d'informations à des personnes ou à des organisations extérieures au gouvernement du Canada au sujet des menaces dont elles font l'objet? Quelles limites faudrait-il fixer quant aux destinataires auxquels le SCRS peut donner des informations et au moment où il peut le faire?

Question nº 2 : Faut-il doter le SCRS de nouveaux pouvoirs nécessitant une autorisation judiciaire adaptés au degré d'intrusion propre aux techniques à employer?

Contexte

En vertu de l'article 12 et de l'article 16 de la *Loi*, le SCRS peut collecter des informations quand les moyens utilisés sont très peu intrusifs. Si la collecte nécessite des moyens plus intrusifs, le SCRS invoque l'article 21 pour demander un mandat à la Cour fédérale. Auparavant, il doit consulter le sous-ministre de Sécurité publique, et le ministre de la Sécurité publique doit approuver le dépôt de la demande à la Cour fédérale. Aux termes de l'article 21, il faut que toutes les demandes de mandat satisfassent les mêmes critères, même si le degré d'intrusion varie grandement en fonction des techniques d'enquête employées. Ainsi, il n'existe actuellement qu'un seul type de demande de mandat, dont les critères correspondent aux techniques d'enquête les plus intrusives. Par conséquent, pour être autorisé à mener une activité de collecte ponctuelle (comme l'examen d'une clé USB), le SCRS doit remplir les mêmes critères que pour obtenir un mandat l'autorisant à exercer de façon répétée, pendant un an, des pouvoirs plus étendus nécessitant l'obtention d'un tel mandat (p. ex. l'interception en continu de communications privées).

Quel est le problème?

Pour obtenir un mandat, le SCRS doit démontrer qu'il a essayé, en vain, les techniques ne nécessitant pas de mandat, que de telles techniques ont peu de chances de succès ou sont impraticables quand il y a urgence, ou que, sans mandat, il n'obtiendra aucune information importante, et ce, quel que soit le type de technique nécessitant un mandat qu'il désire employer (une exigence appelée « nécessité pour les besoins de l'enquête »). Ainsi, il est tenu de respecter les mêmes critères, qu'il souhaite avoir un mandat pour connaître le nom et l'adresse d'un individu qui utilise une adresse IP donnée, pour consulter le registre détaillé des appels effectués sur un appareil ou pour intercepter les communications privées d'une personne pendant un an au maximum.

De la même façon, le SCRS doit remplir les mêmes critères stricts pour demander un mandat l'autorisant à recevoir un appareil (p. ex. une clé USB) et à en examiner le contenu une seule fois que pour effectuer des examens répétés des appareils d'une personne ou d'intercepter les communications en provenance ou à destination de ces appareils pendant un an au maximum. Par ailleurs, le SCRS manque d'un pouvoir distinct de contraindre une organisation à conserver des informations éphémères (p. ex. des données sur des transactions que l'institution financière concernée devrait autrement effacer). Il peut donc perdre des informations importantes pour une enquête pendant la démarche nécessaire à l'obtention d'un mandat en vertu de l'article 21.

Au contraire, les enquêteurs des forces de l'ordre ont accès à un éventail de pouvoirs autorisés par mandat qui sont mieux adaptés au degré d'intrusion propre aux techniques à autoriser. Il existe des différences considérables entre les pouvoirs dont peuvent se prévaloir le SCRS et les forces de l'ordre. Par exemple, les personnes visées par un mandat policier en sont souvent avisées et peuvent plus facilement le contester que celles qui font l'objet d'un mandat du SCRS, qui pourraient ne jamais l'apprendre, pour des questions de sécurité nationale. Cependant, le SCRS fait l'objet d'une étroite surveillance par le ministère et par des organismes de surveillance, ce qui n'est pas le cas des forces de l'ordre. Cela dit, au fil des ans, des modifications ont été apportées au *Code criminel,* pour une plus grande souplesse des pouvoirs nécessitant un mandat, sans compromis pour l'exercice d'un contrôle judiciaire efficace. Par exemple, les dispositions sur les ordonnances de communication ont été introduites dans le *Code criminel* en 2004. En outre, dans le cadre d'une enquête criminelle, les enquêteurs des forces de l'ordre doivent souvent établir la « nécessité pour les besoins de l'enquête » pour intercepter des communications privées ou effectuer une vidéosurveillance intrusive, mais pas pour toutes les méthodes de collecte exigeant un mandat.

Changement législatif possible

De nouvelles autorisations judiciaires adaptées pourraient être envisagées pour certaines techniques d'enquête, en plus des pouvoirs prévus dans les mandats auxquels le SCRS a déjà accès. Par exemple, le SCRS pourrait demander une ordonnance de préservation à la Cour, sans avoir à en établir la nécessité pour les besoins de l'enquête, ce qui l'autoriserait à contraindre un

tiers à préserver des informations éphémères, s'il a des motifs raisonnables de soupçonner qu'elles seront utiles dans une enquête de renseignement et s'il a l'intention de demander une ordonnance de communication ou un mandat pour les obtenir.

Une ordonnance de communication serait un autre outil qui pourrait simplifier la tenue d'une enquête sur une menace. Elle permettrait au SCRS de contraindre un tiers à lui communiquer des informations, s'il a des motifs raisonnables de croire qu'elles sont probablement importantes et qu'elles l'aideront probablement dans l'exercice de ses fonctions. Il pourrait demander une ordonnance de communication pour obtenir des données comme des informations de base sur un abonné, des relevés détaillés des appels ou des relevés de transactions. Ce nouveau pouvoir adapté autorisé par un mandat pourrait aider le SCRS à mener une activité de collecte une seule fois, par exemple obtenir et examiner une clé USB. Par nature, ces types d'activités de collecte ponctuelles ont des répercussions plus prévisibles – et par conséquent moins importantes – sur le droit à la vie privée que les types d'activités qui peuvent être autorisées en vertu des pouvoirs prévus dans les mandats actuels, qui peuvent comprendre l'utilisation de toutes les techniques d'enquête et une collecte en continu pendant un an au maximum. Comme le SCRS devrait toujours avoir des motifs raisonnables de croire que l'activité de collecte lui permettra probablement d'obtenir des informations importantes qui l'aideront probablement à exercer les fonctions qui lui sont conférées en vertu des articles 12 ou 16 de la *Loi sur le SCRS*, une surveillance judiciaire efficace serait maintenue.

Enfin, il sera parfois irréalisable pour le ministre de la Sécurité publique d'approuver que le SCRS fasse une demande de mandat , et ce pour un certain nombre de raisons, dont le fait que le ministre est à l'étranger et qu'il n'est pas en mesure d'examiner une demande urgente. Dans de tels cas, le pouvoir d'autorisation du ministre pourrait être délégué afin que le SCRS puisse obtenir les mandats nécessaires de la Cour fédérale pour faire avancer ses enquêtes sur la sécurité nationale.

Qu'en pensez-vous?

1) Le SCRS devrait-il être en mesure de contraindre une personne ou une organisation à préserver des informations éphémères lorsqu'il a l'intention de demander une ordonnance de communication ou un mandat pour obtenir ces informations?

2) Le SCRS devrait-il être en mesure de contraindre une personne ou une organisation à lui communiquer des informations s'il a des motifs raisonnables de croire que ces informations sont probablement importantes et qu'elles l'aideront probablement dans l'exercice des fonctions qui lui sont conférées en vertu des articles 12 ou 16 de la *Loi sur le SCRS*?

3) Le SCRS devrait-il être en mesure de mener une activité de collecte ponctuelle, par exemple obtenir et examiner une clé USB s'il a des motifs raisonnables de croire qu'elle contient des informations liées à la menace, sans avoir à en prouver la nécessité pour les

besoins de l'enquête? Dans l'affirmative, quelles exigences lui faudrait-il respecter pour demander des mandats qui autorisent différents pouvoirs?

4) Lorsque le ministre de la Sécurité publique n'est pas en mesure d'autoriser le SCRS à présenter une demande d'autorisation judiciaire à la Cour fédérale et que la question ne peut pas attendre, devrait-il exister un mécanisme de délégation de ce pouvoir? Dans l'affirmative, à qui ce pouvoir devrait-il être délégué et dans quels types de situations devrait-il s'appliquer?

Question nº 3 : Faut-il combler une lacune causée par les progrès technologiques et rétablir la capacité du SCRS de recueillir, depuis le Canada, des informations sur d'autres États et des ressortissants étrangers qui se trouvent au Canada?

Contexte

L'article 16 de la *Loi sur le SCRS* autorise le SCRS à recueillir, à la demande du ministre des Affaires étrangères ou du ministre de la Défense nationale, des informations sur des États ou des ressortissants étrangers (c'est-à-dire des renseignements étrangers) « dans les limites du Canada ». Comme la technologie a énormément évolué depuis l'adoption de l'article 16 en 1984, le Parlement ne pouvait pas savoir à quel point la limite géographique « dans les limites du Canada » restreindrait la collecte de renseignements dans un contexte où les informations sont numériques dans une large mesure et ne connaissent pas de frontières.

Quel est le problème?

Lorsqu'il a adopté la *Loi sur le SCRS* en 1984, le Parlement a donné au SCRS le mandat de prêter assistance à la collecte de renseignements étrangers. Il a reconnu que la collecte de renseignements étrangers au Canada nécessitait du savoir-faire, et que le SCRS était le mieux placé pour accomplir cette tâche. Toutefois, le Parlement a restreint ce mandat à la collecte « dans les limites du Canada », parce qu'il ne voulait pas que le SCRS recueille des renseignements étrangers dans d'autres pays. En outre, la *Loi sur le Centre de la sécurité des télécommunications* interdit au Centre de la sécurité des télécommunications (CST) de viser, dans ses activités de collecte, des Canadiens ou des personnes se trouvant au Canada.

La Cour fédérale et la Cour d'appel fédérale (2018 CF 738, 2018 CAF 207, 2020 CF 757, 2021 CAF 165) ont interprété l'expression « dans les limites du Canada » ainsi : il est interdit au SCRS de recueillir, depuis le Canada, des informations sur des États ou des ressortissants étrangers si elles se trouvent à l'extérieur du Canada. Depuis que ces décisions ont été rendues, étant donné les avancées technologiques, le SCRS n'a plus qu'une vue limitée sur les activités menées par des États ou des ressortissants étrangers en sol canadien lorsque les informations électroniques se trouvent à l'extérieur du Canada. Les tribunaux ont clairement indiqué qu'« il incombe au législateur, et non aux tribunaux, de rajuster en fonction des percées technologiques les techniques d'enquête dont peut faire usage le Service [en vertu de l'article 16 de la *Loi sur le SCRS*] » (2021 CAF 165, paragraphe 6).

Les libellés de la *Loi sur le SCRS* et de la *Loi sur le CST* engendrent une lacune en matière de renseignements étrangers. Il est essentiel d'aider le gouvernement du Canada à gérer ses relations étrangères et à assurer la défense nationale. Il faut absolument combler cette lacune si l'on veut que le gouvernement comprenne bien les moyens, les intentions ou les activités des États ou ressortissants étrangers qui peuvent se livrer à des activités d'ingérence étrangère.

Changement législatif possible

Redonner au SCRS une certaine capacité, perdue essentiellement en raison des progrès technologiques, de recueillir depuis le Canada des renseignements étrangers qui se trouvent à l'extérieur du Canada sur d'autres États et des ressortissants étrangers se trouvant au Canada, tout en conservant les autres limites imposées. La collecte d'informations doit être effectuée à la demande du ministre des Affaires étrangères ou du ministre de la Défense nationale et est assujettie au consentement du ministre de la Sécurité publique ainsi qu'à l'approbation et aux conditions de la Cour fédérale. De plus, les activités de collecte menées en vertu de l'article 16 ne peuvent pas viser des citoyens canadiens, des résidents permanents ou des personnes morales constituées au Canada.

Qu'en pensez-vous?

1) La *Loi sur le SCRS* devrait-elle être modifiée afin que la capacité du SCRS de recueillir des renseignements étrangers à la demande de ministres évolue au même rythme que la technologie, qui se trouve à générer des informations numériques qui ne connaissent pas de frontières? Dans l'affirmative, quelles devraient être les limites?

Question nº 4 : Faut-il modifier la *Loi sur le SCRS* pour accroître la capacité du SCRS de tirer profit de l'analytique des données pour enquêter sur les menaces à l'ère moderne?

Contexte

En ajoutant au projet de loi C-59 le régime applicable aux ensembles de données établi aux articles 11.01 à 11.25 de la *Loi sur le SCRS*, le législateur a reconnu que les données et la technologie avaient redéfini le contexte de la menace et des enquêtes. Il se trouvait aussi à donner suite à la décision de la Cour fédérale sur les « données connexes » (2016 CF 1105). Ce régime visait à autoriser le SCRS à recueillir, à conserver et à utiliser les ensembles de données qui, « dans l'immédiat, ne sont pas directement liés » à une menace envers la sécurité nationale, mais qui peuvent l'aider dans l'exercice des fonctions qui lui sont conférées en vertu des articles 12 à 16 de la *Loi sur le SCRS*. Il prévoit de nombreuses mesures de protection pour réduire au minimum les informations personnelles et privées figurant dans les ensembles de données recueillis, surtout celles qui sont liées à des Canadiens ou à d'autres individus se trouvant au Canada.

Quel est le problème?

Malgré l'entrée en vigueur du régime applicable aux ensembles de données, le SCRS n'est pas vraiment en mesure de conserver et d'utiliser des ensembles de données, même quand il est manifeste qu'ils sont utiles à l'exercice de son mandat.

La période d'évaluation de 90 jours est une de ces exigences qui compliquent l'application du régime. Plus précisément, lorsque le SCRS recueille un ensemble de données, une période d'évaluation de 90 jours stricte commence, au cours de laquelle le SCRS doit accomplir une série de tâches, dont en traduire et en décrypter le contenu, utiliser des techniques de révision liées à la protection de la vie privée et en organiser les données. S'il s'agit d'un ensemble de données étranger, le SCRS doit également, pendant la période d'évaluation de 90 jours, en extraire les informations ayant trait à des Canadiens afin soit de les détruire soit de constituer un ensemble de données canadien distinct. Il doit aussi préparer et présenter les demandes d'approbation par le ministre et d'autorisation judiciaire nécessaires pour conserver l'ensemble de données au cours de la même période de 90 jours. Si le SCRS est incapable d'évaluer pleinement l'ensemble de données et de présenter la demande de conservation requise dans le délai de 90 jours, il doit détruire l'ensemble de données.

Par exemple, un partenaire de confiance fournit au SCRS un ensemble de données renfermant des informations (comptes, coordonnées, relations) tirées des dossiers d'un pays qui a l'habitude de se livrer à des activités d'ingérence étrangère. Les informations portent principalement sur des individus qui ne sont pas des Canadiens et qui se trouvent à l'extérieur du Canada (informations étrangères), mais l'ensemble de données pourrait également contenir des informations liées à des Canadiens. La *Loi* prévoit des processus d'approbation et de conservation différents pour les ensembles de données étrangers et les ensembles de données canadiens. Pour être en mesure de conserver la totalité de ces informations en vertu du régime applicable, le SCRS doit évaluer l'ensemble de données étranger dans les 90 jours suivant la collecte, en extraire toutes les informations liées à des Canadiens, puis demander au ministre de la Sécurité publique l'autorisation de le conserver. Le commissaire au renseignement doit aussi examiner et approuver l'autorisation du ministre. Par ailleurs, le SCRS doit obtenir l'approbation du ministre pour demander à la Cour fédérale l'autorisation de conserver les informations liées à des Canadiens sous la forme d'un ensemble de données canadien. Au préalable cependant, le Service doit avoir des motifs raisonnables de croire que les informations liées à des Canadiens font partie d'une catégorie approuvée d'ensembles de données canadiens. La totalité du processus pourrait nécessiter jusqu'à cinq demandes distinctes qui seront présentées au ministre, au commissaire au renseignement ou à la Cour, ce qui signifie que le SCRS ne pourrait pas exploiter les données avant six à neuf mois. Il est possible qu'elles soient beaucoup moins utiles sur le plan du renseignement à ce moment-là. Si le SCRS ne peut pas évaluer l'ensemble de données et présenter les demandes nécessaires pour le conserver dans les délais fixés par la *Loi*, il est obligé de détruire toutes les données.

Le régime comporte aussi des ambiguïtés qui empêchent le SCRS de tirer parti des ensembles de données de la façon prévue par le Parlement et qui pourraient nuire à l'exercice des fonctions qui lui sont conférées en vertu des articles 12 et 16 de la *Loi sur le SCRS*. Un nombre restreint de modifications qui dissiperaient ces ambiguïtés améliorerait la viabilité du régime et fournirait les éclaircissements nécessaires pour éviter de multiples interprétations juridiques.

D'autres limites du régime applicable aux ensembles de données font aussi que le SCRS perd des occasions et des informations utiles. Par exemple, à l'heure actuelle, le SCRS ne peut pas interroger ou exploiter des ensembles de données canadiens pour fournir des évaluations de sécurité ou des conseils au titre de l'article 15 de la *Loi sur le SCRS*. Dans le cadre du processus de filtrage de sécurité, les demandeurs doivent, entre autres, fournir des informations sur leurs études et leurs antécédents professionnels, ce qui est utile pour évaluer leur loyauté. Les efforts d'un demandeur pour dissimuler ou omettre ses liens avec certaines institutions peuvent être pertinents dans une enquête de filtrage. Le SCRS ne peut cependant pas interroger un ensemble de données canadien portant sur les personnes au Canada qui ont étudié dans une université associée aux forces armées d'un autre pays dans le cadre d'une enquête de filtrage.

Le SCRS collabore avec de nombreux partenaires canadiens, comme le CST et la GRC, dans l'exercice de son mandat lié à la sécurité nationale. Les ensembles de données qu'il pourrait être en mesure de recueillir en vertu du régime pourraient présenter un intérêt dans le cadre du mandat d'autres organismes. Toutefois, le SCRS ne peut pas communiquer ces ensembles de données à des organismes partenaires parce que le régime ne prévoit pas la communication d'ensembles de données complets. Cette limite l'empêche aussi de collaborer avec des partenaires étrangers lorsque des ensembles de données pourraient être d'intérêt mutuel, par exemple lorsqu'un ensemble de données, bien qu'il ne soit pas directement lié à une menace, pourrait être utile dans l'enquête sur un État qui se livre énergiquement à des activités d'ingérence étrangère.

Changement législatif possible

Le gouvernement pourrait proposer des modifications ciblées au régime applicable aux ensembles de données afin d'atténuer certaines des pires difficultés, par exemple, permettre des prolongations de la période d'évaluation ou accroître la durée des catégories d'ensembles de données approuvées ou des autorisations de conserver des ensembles de données canadiens et étrangers.

D'autres modifications pourraient préciser que le régime ne s'applique qu'aux ensembles de données qui ne sont visés par aucun autre pouvoir dans la *Loi sur le SCRS*, que les catégories d'ensembles de données canadiens ne doivent être valides qu'à l'étape de la collecte et que les ensembles de données étrangers qui contiennent des informations liées à des Canadiens peuvent être traités comme des ensembles de données canadiens (le plus rigoureux des deux processus) afin d'éviter de multiples demandes d'autorisations. D'autres encore pourraient permettre au SCRS de communiquer des ensembles de données sous réserve de conditions strictes et d'interroger ou d'exploiter des ensembles de données canadiens dans le cadre d'enquêtes de filtrage menées au titre de l'article 15.

Qu'en pensez-vous?

1) Comment le SCRS pourrait-il s'y prendre pour être mieux en mesure de recueillir et d'utiliser des ensembles de données rapidement et efficacement, tout en respectant les droits garantis par la *Charte*, dans un monde axé sur les données?
2) Le SCRS devrait-il pouvoir interroger ou exploiter des ensembles de données canadiens aux fins de l'article 15? Dans l'affirmative, pensez-vous que des mesures de protection ou des limites additionnelles devraient être mises en place?
3) Le SCRS devrait-il pouvoir communiquer des ensembles de données canadiens ou étrangers à des partenaires canadiens qui sont autorisés par la loi à recueillir le type d'informations que ces ensembles de données contiennent? Dans l'affirmative, quelles mesures de protection ou conditions devraient être mises en place, le cas échéant?
4) Le SCRS devrait-il être autorisé à communiquer des ensembles de données étrangers à des partenaires étrangers? Dans l'affirmative, quelles mesures de protection ou conditions devraient être mises en place, le cas échéant?

Question nº 5 : Faut-il ajouter une disposition exigeant que la *Loi sur le SCRS* fasse l'objet d'un examen régulier afin que le SCRS puisse évoluer au même rythme que les menaces?

Contexte

Le contexte de la menace est en constante évolution, et le Canada doit s'assurer de disposer des outils dont il a besoin pour détecter les menaces pour la sécurité nationale et les contrer. Toutefois, la *Loi sur le SCRS* n'est modifiée que de façon ponctuelle parce qu'aucune disposition ne prévoit qu'elle fasse l'objet d'un examen régulier.

Quel est le problème?

Contrairement à la majorité de ses alliés, le Canada n'a prévu aucune disposition législative exigeant que la *Loi sur le SCRS* fasse l'objet d'un examen régulier pour s'assurer qu'elle évolue au même rythme que les technologies et les données et qu'elle tient compte de leurs répercussions sur les menaces pour la sécurité nationale. Par conséquent, il est à peu près inévitable que les pouvoirs du SCRS deviennent désuets, ce qui rend le Canada et les Canadiens vulnérables.

Il est essentiel de donner au SCRS les outils nécessaires pour contrer les menaces actuelles, mais aussi celles de demain, et ainsi protéger le Canada et les Canadiens contre les menaces pour la sécurité nationale. Des pouvoirs à jour renforceraient la capacité du SCRS et du Canada de collaborer avec des alliés et permettraient au Canada de conserver sa réputation à titre de partenaire de confiance dans la lutte contre les menaces pour la sécurité nationale qui transcendent de plus en plus souvent les frontières.

Changement législatif possible

Ajouter une disposition exigeant que le Parlement examine régulièrement la *Loi sur le SCRS*.

Qu'en pensez-vous?

1) Faudrait-il que la *Loi* exige que les pouvoirs conférés au SCRS fassent l'objet d'un examen régulier, de manière à évoluer au même rythme que les technologies et les adversaires du Canada? Dans l'affirmative, à quelle fréquence?

2) Avez-vous d'autres opinions dont vous aimeriez nous faire part concernant les modifications possibles de la *Loi sur le SCRS*?

TAB E

Annex 1

ADDRESSING FOREIGN INTERFERENCE

Whether to Amend the *Security of Information Act* and Modernize certain *Criminal Code* offences, and to Introduce a review mechanism in the *Canada Evidence Act* to manage sensitive information

Context

As an advanced economy and open democracy, Canada is often targeted by foreign states, or those acting on their behalf, seeking to advance their own strategic objectives. While foreign states usually advance their interests in legitimate and transparent ways, some also act in ways that threaten or intimidate people in Canada, their families elsewhere or are covert and deceptive, and harmful to Canada's national interests.

Often described as foreign interference, these deceptive, coercive and threatening activities can target all levels of government, the private sector, academia, diverse communities and the general public.

We know that in Canada, threat actors seek, among other things, to:

- Attack or undermine the integrity of democratic institutions, and covertly influence the outcomes of electoral processes, including the nomination of candidates,
- Cultivate influential people to sway government decision-making and policies to advance their interests, and discredit those who threaten their interests,
- Intimidate or harass individuals who speak out against repression in foreign states, in attempts to stamp out dissent and limit democratic rights and freedoms in Canada, as part of a campaign of transnational repression,
- Intimidate the families of these individuals who reside in those foreign states,
- Steal Canadian-made knowledge and innovation to support their own military or economic objectives,
- Undermine the legitimacy of Canada's representatives abroad, or the goals of the Canadian government's international activities, and
- Insert themselves into Canada's supply chains and critical infrastructure.

While foreign interference activities are not new, they have increased in volume and complexity in recent years. This is why, more than ever, Canada must be equipped with the necessary tools to take proactive and decisive action against the threats posed by foreign interference.

Annex 1

Existing Measures

The Government currently uses various measures to counter foreign interference, including investigating and laying criminal charges in accordance with Canadian laws. These laws include Canada's *Security of Information Act* (SOIA), which criminalizes information-related conduct that may be harmful to Canada, such as unauthorized disclosure of information, spying, economic espionage and foreign-influenced threats or violence. There are *Criminal Code* offences that address different types of conduct in connection with foreign interference, such as sabotage, intimidation, computer hacking and bribery, amongst others. In addition, there are offences and other provisions in the *Canada Elections Act*, which address foreign involvement in our federal electoral processes. For example, it is an offence for a foreign individual or entity to unduly influence an elector's vote. It is also an offence for third parties in an election to use foreign funds for their activities.

In recent years, however, many experts have called on Canada to modernize its laws to address new and evolving foreign interference threats, such as those emanating from emboldened and assertive foreign states, and the growth of community and online media, and social media avenues for threats and other forms of interference, and to ensure consistency with allied countries. The SOIA, for example, has not had a substantial revision since 2001 and may benefit from updates that would better respond to modern threats. Australia, the United States (US) and the United Kingdom (UK) have all recently taken steps to enhance their ability to identify and counter foreign interference.

Key concerns with the existing legal framework include uncertainty as to whether conduct linked to foreign interference would always be adequately captured under existing laws, or would provide police and prosecutors with enforceable foreign interference offences that are consistent with the *Canadian Charter of Rights and Freedoms* (the *Charter*), including freedom of expression which includes freedom of the press.

Section 20 of the SOIA, for example, addresses foreign interference, but only in a limited way. The offence is limited to circumstances where someone uses threats or violence to advance the interests of a foreign entity, and the burden is on the prosecution to show that the purpose was to increase the capacity of a foreign entity to harm Canadian interests, or where the threats or violence are reasonably likely to harm Canadian interests. It does not cover, for example, other types of non-violent foreign interference, including interference with democratic processes.

Some other acts may be an offence under the *Criminal Code* or other statutes, but existing criminal offences that are committed for the benefit of foreign states may not fully reflect the serious impact of the foreign interference.

The Government is assessing whether it is desirable and appropriate to amend the criminal law to address these concerns. This consultation paper describes how existing provisions could be modernized, such as the dated sabotage offence in the *Criminal Code* and the SOIA provisions on unauthorized disclosure, which were struck down by a lower court in Ontario under section 7 (life, liberty and security of the person) and 2(b) (freedom of expression) of the *Charter*.

Similar to recent reforms in the UK and Australia, the Government is considering creating new offences that respond to the modern threat landscape. The amendments being considered could provide more certainty as to what activities would be criminalized as foreign interference, and provide penalties that reflect the seriousness of such activities. In addition, the Government is considering whether there are ways to enhance deterrence by increasing the risks to foreign entities considering such activities in Canada.

Furthermore, this consultation paper seeks input on measures that could be taken to provide an overall legislative scheme in the *Canada Evidence Act* and the *Criminal Code* for the protection and use of national security information in judicial reviews and statutory appeals of governmental decision-making. Finally, it will seek views on potential reforms regarding how national security information is used and protected.

Respecting Individual Rights and Freedoms

The *Charter* sets out the fundamental rights and freedoms that we, as a country, believe are necessary in a free and democratic society. The *Charter* applies to all levels of government and protects the following: fundamental freedoms, including freedom of expression and democratic rights; the right to live and seek employment anywhere in Canada; legal and equality rights; the official languages of Canada and minority language education rights; Canada's multicultural heritage; and the rights of Indigenous peoples.

Subject to a few exceptions, including the right to vote and the right to enter, remain in and leave Canada, any person in Canada – whether a Canadian citizen, permanent resident or newcomer – benefits from the rights and freedoms contained in the *Charter*.

The SOIA and *Criminal Code* can affect rights that are protected by the *Charter*, as well as the public interest, in various ways. In the national security context, legitimate concerns have been raised as to whether government powers to address serious threats to Canada's safety and security unnecessarily impede individual rights and freedoms, such as freedom of expression under section 2(b), the right to life, liberty and security of the person under section 7, and the right to be free from unreasonable search and seizure under section 8 of the *Charter*.

Indeed, these concerns came to the forefront in the successful legal challenge to section 4 of the SOIA in the early 2000s, when the media, civil liberty organizations, and others, criticized the provision for its chilling effect on freedom of expression and the press. Any new amendments to Canada's laws that protect against foreign interference or unlawful disclosure of information that can damage Canada's interests will give rise to legitimate worries about the protection of other

important values, rights, and interests. These interests include the *Charter* protection for freedom of expression, which includes freedom of the press, and ensuring that any new offences are not overly broad. With this in mind, it is crucial that any reforms strike an appropriate balance between ensuring an effective criminal justice response to foreign interference and respecting the fundamental rights and freedoms of people in Canada.

Link back to the main PS consultations page, as well as the other consultations (To be determined in consultation with Comms, PS, and CSIS.) Links could be made to other informative sites: https://www.canada.ca/en/security-intelligence-service/corporate/publications/foreign-interference-threat-to-canadas-democratic-process.html#toc5

Annex 1

These illustrative scenarios might help explain what is meant by foreign interference:

Scenario 1

Ms. M is community organizer in a small Canadian city. Her family and friends have encouraged her to run for elected office. Because Country F disagrees with her views, Country F initiates a disinformation campaign against her, with the help of other people in Canada. The disinformation campaign targets the supporters of Ms. M and aims to create confusion about her campaign with false narratives. Country F interferes with her nomination campaign by sending confusing information to her supporters about when, where, and how to vote for Ms. M.

Scenario 2

Mr. A is a student attending a Canadian university. They organized a series of on-campus protests against Country X, a foreign state that is known to violate the human rights of minorities based on their religious beliefs and racial ethnicity. Mr. A (as the organizer) and participants begin to receive threatening and harassing emails, social media messages, and phone calls. Mr. A's personal information, and that of other participants, is also posted online, and family members begin to receive threats. Country X has been involved in the coordination of this harassment campaign.

Scenario 3

Ms. C is a permanent resident that emigrated from Country Z. She has lived in Canada for several years, but recently started receiving emails and phone calls from individuals identifying themselves as security officials from Country Z telling her to return home to face prosecution for alleged crimes. She has received visits from unknown individuals at her residence claiming to be officials from Country Z advising her to return home. She has also received recent photographs of herself and her family members in the mail. She suspects that she is being followed, and that spyware might have been installed in her personal electronic devices, as the callers know personal and private information, including where she lives, her family and friends, and where she works. The phone calls are increasingly hostile and threatening; most recently, she has been told that if she does not return home, her family members in Country Z will be arrested and tried for her alleged crimes.

Scenario 4

Mr. B is a scientist working for a Canadian tech company. While working at that company, he begins to receive offers from a tech company based in Country Y, a foreign state that is doing similar work, and considers moving to the new company. At the direction of the tech company based in Country Y, which was working in association with the foreign state, Mr. B. begins to transfer highly sensitive protected data from the Canadian company he works for to his personal devices, without their knowledge or consent. The employee then submits his resignation to the Canadian company and leaves Canada to work for the foreign company. He transfers that protected data to the new place he works. The foreign state in which that company is located benefits from the stolen information, and the disclosure of the information results in harm to Canadian interests.

Solicitor-Client Privilege

Solicitor-Client Privilege

Solicitor-Client Privilege

Solicitor-Client Privilege

Solicitor-Client Privilege

Solicitor-Client Privilege

Solicitor-Client Privilege

Solicitor-Client Privilege

Solicitor-Client Privilege

Solicitor-Client Privilege

Solicitor-Client Privilege

Solicitor-Client Privilege

Solicitor-Client Privilege

Solicitor-Client Privilege

Solicitor-Client Privilege

Solicitor-Client Privilege

Solicitor-Client Privilege

Solicitor-Client Privilege

Solicitor-Client Privilege

Solicitor-Client Privilege

Solicitor-Client Privilege

Solicitor-Client Privilege

Solicitor-Client Privilege

Solicitor-Client Privilege

Solicitor-Client Privilege

Solicitor-Client Privilege

Solicitor-Client Privilege

TAB F

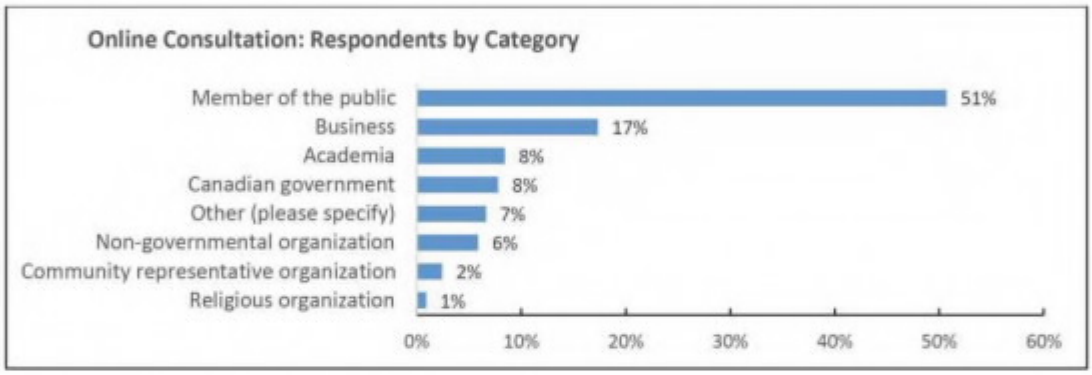
What We've Heard So Far:

Foreign Influence Transparency Registry Consultations Summary

On 10 March 2023, the Government of Canada launched public consultations to guide the creation of a Foreign Influence Transparency Registry (FITR).

Public Safety Canada (PS) received almost 1,000 responses from Canadians across the country through an online consultation portal. PS also engaged with a diverse range of stakeholders that brought forward unique perspectives to help shape the design of the FITR.

- A total of 932 responses were received through the online portal and 71 separate email submissions were received.



- Over 80 individual stakeholders were engaged.
  - PS engaged with representatives from over 40 different organizations, as well as individual academics and subject matter experts.
  - In-person and virtual stakeholder consultations took place with various stakeholder groups, including academics, business, and community organizations.

While online consultations closed on 9 May, dialogue with stakeholders has remained ongoing on the FITR and on foreign interference (FI) more broadly.

Key Themes:

- There is very broad support for the FITR. Supportive feedback indicates that it will:
  - enhance transparency;
  - help protect communities targeted by malign foreign influence; and,
  - strengthen deterrence.

- Among the primary concerns raised are that the FITR may:
  a) disproportionately target minority communities;
  b) be misused to create a "blacklist";
  c) lead foreign states, especially non-democratic ones, to reciprocate with a similar registry to target Canadian NGOs and diplomats;
  d) fail to capture the activities of nefarious actors who do not want to comply;

e) not address all aspects of FI; and,
f) create unnecessary bureaucracy for legitimate actors.

- In addition, stakeholders urged the Government to undertake structural and cultural reform within the national security bureaucracy, continue outreach with communities at particular risk from FI, and allocate additional resources towards the enforcement of existing counter-interference legislation.

Targeted Feedback:

General Administration

- Purpose and guiding principles: There is broad support for the FITR between online respondents and stakeholders. Feedback indicates the FITR will: enhance transparency; help protect communities targeted by malign foreign influence; and strengthen deterrence.

- Foreign principals: Respondents agreed that foreign states and their proxies should be included in the definition of foreign principal. Most stakeholders also agreed that the registry should apply to all countries, while a small minority of stakeholders think that there should be exemptions for NATO or FEYES allies, and some argued in favour of a list of problematic countries only. Some participants wondered if non-state actors and non-state affiliated foreign actors should be included as registrable principals.

FITR Components

- Registrable activities: Most respondents agreed with the categories proposed by Public Safety (parliamentary lobbying, general political lobbying and advocacy, disbursement, and communications activity). A key outstanding issue to address remains whether exchange-of-favor might also be considered as a registrable activity.

- Exemptions: While online respondents largely disagreed with the use of exemptions, stakeholder groups felt that exemptions should exist and be as narrow as possible. Legal practitioners asserted that an exemption should exist for persons who provide legal advice and representation to foreign governments. Academic representatives asserted that an exemption should exist for activities that are predominantly academic or scholastic in nature (e.g., teaching and research activities; advocacy efforts on behalf of international students and temporary foreign workers). And Community Organizations asserted that an exemption should exist for humanitarian organizations.

- Compliance and penalties: The overwhelming majority of online respondents agreed that there should be penalties for non-compliance, and that those penalties should be scalable. Monetary penalties alone may not deter wealthy individuals/entities and may call into question the impartiality of the FITR. Additionally, respondents noted that legislation (i.e., s. 19 of the *CSIS Act*) should be amended to better enable enforcement of FITR (particular as it related to the sharing of information). Complications associated with the use of sensitive material in legal proceedings was raise by Legal practitioners as particularly relevant in the context of the FITR

- Enforcement: Respondents noted that the success of the FITR will depend on sufficient enforcement of the Registry. Respondents noted that enforcement capacity will need to be robustly resourced to

be effective. Legal practitioners expressed interest in including provisions to allow for the seeking of advisory opinions – similar to the *Lobbying Act*.

- Handling of privacy information: One stakeholder recommended that the Government consider information disclosure requirements as set out in Section 5(2) of the *Lobbying Act*. In stakeholder consultations a common theme was that all information requested for the purpose of registration should be publicly available to avoid the appearance of a "secret list" or "black list." Legal practitioners raise the need to diligently apply the *Canadian Charter of Rights and Freedoms*.

Next Steps:

The input from these consultations is informing decision-making and the design of new measures that may be brought forward. As this takes shape, continued outreach, particularly with Provinces, Territories and Indigenous partners, will be required.

French Version

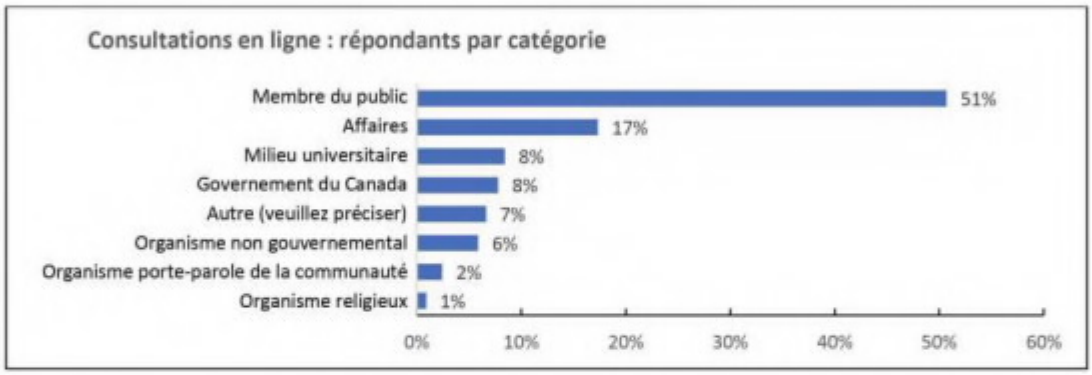
Ce qu'on nous a dit jusqu'ici:

Sommaire des consultations sur un registre pour la transparence en matière d'influence étrangère

Le 10 mars 2023, le gouvernement du Canada a lancé des consultations publiques pour orienter la création d'un registre pour la transparence en matière d'influence étrangère (RTMIE).

Sécurité publique Canada (SP) a reçu près de 1 000 réponses de la part de Canadiens de partout au pays par le biais d'un portail de consultation en ligne. SP a également mobilisé un large éventail d'intervenants qui ont présenté différentes perspectives pour aider à façonner la conception du RTMIE.

- Au total, 932 réponses ont été reçues par le biais du portail en ligne et 71 par courriel.



- Plus de 80 intervenants ont été mobilisés.
  - SP a mobilisé des représentants de plus de 40 organismes différents, ainsi que des universitaires et des experts en la matière.
  - Des consultations en personne et virtuelles ont eu lieu avec divers intervenants, notamment des universitaires, des entreprises et des organisations communautaires.

Bien que les consultations en ligne ont pris fin le 9 mai, les échanges se poursuivent avec les intervenants, tant au sujet du RTMIE que sur la plus vaste question de l'ingérence étrangère (IE).

Principaux thèmes

- Le RTMIE bénéficie d'un très large soutien. Les commentaires favorables indiquent qu'il permettra :
  - d'améliorer la transparence;
  - d'aider à protéger les communautés ciblées par l'influence étrangère malveillante;
  - et de renforcer la dissuasion.

- Selon les principales préoccupations soulevées, le RTMIE pourrait :
  a) cibler de manière disproportionnée les communautés minoritaires;

b) être utilisé à mauvais escient pour créer une « liste noire »;
c) inciter les États étrangers, en particulier ceux qui ne sont pas démocratiques, à créer un registre similaire pour cibler les ONG et les diplomates canadiens;
d) ne pas consigner les activités des acteurs malveillants qui refusent de se conformer;
e) ne pas aborder pas tous les aspects de l'IE;
f) créer des formalités bureaucratiques inutiles pour les acteurs légitimes.

- En outre, les intervenants ont exhorté le gouvernement à entreprendre une réforme structurelle et culturelle au sein de la bureaucratie en matière de sécurité nationale, à poursuivre la sensibilisation des communautés particulièrement menacées par l'IE et à allouer des ressources supplémentaires à l'application des lois existantes à l'appui de la lutte contre l'ingérence.

Rétroaction ciblée

Administration générale

- Objectif et principes directeurs : les répondants en ligne et les intervenants se sont dits largement en faveur du RTMIE. Les commentaires indiquent qu'il permettra d'améliorer la transparence, de protéger les communautés ciblées par l'influence étrangère malveillante et de renforcer la dissuasion.

- Commettants étrangers : les répondants ont convenu que la définition de « commettant étranger » devrait comprendre les États étrangers et leurs mandataires. La plupart des intervenants ont également convenu que le registre devrait s'appliquer à tous les pays, tandis qu'une petite minorité d'entre eux pensent qu'il devrait y avoir des exemptions pour les alliés de l'OTAN ou du Groupe des cinq; d'autres ont plaidé en faveur d'une liste de pays problématiques uniquement. Certains participants se sont demandé si les acteurs non étatiques et les acteurs étrangers non affiliés à un État devaient être inclus dans la liste des mandants soumis à l'obligation de déclaration.

Composantes du RTMIE

- Activités devant être inscrites au registre : la plupart des répondants se sont dits d'accord avec les catégories proposées par SP (lobbying parlementaire, lobbying et défense des intérêts politique généraux, décaissement et activité de communication). Une question reste en suspens, à savoir si l'échange de faveurs peut également être considéré comme une activité devant être inscrite au registre.

- Exemptions : alors que les répondants en ligne se sont dits largement en désaccord avec le recours aux exemptions, les groupes d'intervenants ont affirmé qu'il devrait y en avoir, et qu'elles devraient être aussi limitées que possible. Les praticiens du droit jugent que les personnes qui fournissent des conseils juridiques et celles en représentation auprès de gouvernements étrangers devraient être exemptées. Les représentants du milieu universitaire estiment qu'une exemption devrait exister pour les activités de nature principalement universitaire ou scolaire (par exemple, les activités d'enseignement et de recherche, les efforts de défense des intérêts des étudiants internationaux et des travailleurs étrangers temporaires). Les organisations communautaires ont affirmé que les organisations humanitaires devraient être exemptées.

- Conformité et sanctions : la très grande majorité des répondants en ligne a convenu qu'il faudrait prévoir des sanctions en cas de non-conformité et que ces sanctions devraient être modulables. Les sanctions pécuniaires ne suffisent pas à dissuader les personnes et entités fortunées et peuvent mener à une remise en question de l'impartialité du registre. En outre, les répondants estiment que certaines lois (c'est-à-dire l'article 19 de la *Loi sur le SCRS*) devraient être modifiées pour permettre une meilleure application du RTMIE (en particulier sur le plan de l'échange de renseignements). Les juristes ont indiqué que les complications liées à l'utilisation de matériel sensible dans les procédures judiciaires étaient particulièrement pertinentes dans le contexte du registre.

- Application du registre : les répondants ont fait valoir que le succès du RTMIE dépendra de son application suffisante et qu'il faudra se doter de ressources solides pour être efficace à cet égard. Les juristes ont exprimé leur intérêt envers l'inclusion de dispositions permettant de demander des avis consultatifs, à l'instar de celles de la *Loi sur le lobbying*.

- Traitement des renseignements sur la vie privée : un intervenant a recommandé au gouvernement d'envisager des exigences en matière de divulgation de renseignements conformes à celles prévues au paragraphe 5(2) de la *Loi sur le lobbying*. Lors des consultations, les intervenants ont soulevé un thème commun : tous les renseignements demandés aux fins de déclaration devraient être accessibles au public afin d'éviter l'apparition d'une « liste secrète » ou d'une « liste noire ». Les juristes ont souligné la nécessité d'appliquer avec diligence la *Charte canadienne des droits et libertés*.

Prochaines étapes:
Les commentaires recueillis lors de ces consultations éclairement la prise de décision et la conception de nouvelles mesures qui pourraient être présentées. Au fur et à mesure que ce projet prend forme, il faut poursuivre la sensibilisation, en particulier auprès des provinces, des territoires et des partenaires autochtones.

TAB G

Tentative Consolidated Stakeholder List

DOJ: 92; CSIS: 47; Overlap: 33: **Total: 163**

	SOIA/CC/CEA	BOTH	CSIS Act
Academics	• Dr. Ali Ghorbani, Canadian Institute for Cybersecurity, Universtity of New Brunswick • Dr. Amira Halperin, University of British Columbia • Dr. Farhaan Ladhani, Digital Public Square, Munk School of Global Affairs and Public Policy, University of Toronto • Frédéric Gagnon, Chaire Raoul-Dandurand en études stratégiques et diplomatiques, Université du Québec à Montréal • Kaveh Shahrooz, University of Toronto • Lynette Ong, University of Toronto • Sergey Sukhankin, University of Alberta • Richard Moon, U of Windsor • Dr. Heidi Tworek, UBC • Michael Geist, U of Ottawa • Kathleen Mahoney, U of Calgary • Anjalee de Silva, doctoral student, U of Melbourne • Marilyn Poitras, Indigenous Law Centre, U Sask	• Leah West, Norman Paterson School of International Affairs • Michael Nesbitt, University of Calgary • Vincent Rigby, Max Bell School of Public Policy, McGill University • Wesley Wark, University of Ottawa	• Baljit Nagra (UOttawa) • Dr. Anver Emon (UToronto) • Dr. David Morin (USherbrooke) • Dr. Kawser Ahmed (UManitoba) • Dr. Roromme Chantal (UMoncton) • Dr. Signa Daum Shanks (UOttawa) • Dr. Stephanie Carvin (Carleton) • Dr. Thomas Juneau (UOttawa) • Dr. Tina Park (Carleton) • Ms. Margaret McCuaig Johnston (UOttawa) • Dr. Christian Leuprecht (QueensU) • Dr. Scott Simon (UOttawa) • Dr. Benjamin Fung (McGill) • Dr. Arjun Chowdhury (UBC)
Advocacy and Community Organizations	• Advocates Society • Ahmadiyya Muslim Jama`at • Alberta Muslim Public Affairs Council • Amnesty International • Belarus Canadian Association • Canadian Civil Liberties Association • Canada Tibet Committee • Canada-Hong Kong Link • Canadian Center for Research-Action on Race Relations	• Alliance Canada Hong Kong • Canadian Anti-Hate Network • Human Rights Watch Canada • League for Human Rights • National Council for Canadian Muslims • National Endowment for Democracy • Ukrainian Canadian Congress • World Sikh Organisation of Canada	• Hamed Esmaeilion • B'nai B'rith • Canada Race Relations Foundation (Mohammed Hashim) • Chinese Canadian National Council for Social Justice • Cross-Cultural Roundtable on Security • Friends of the Simon Wiesenthal Centre • Iranian Women's organization of Ontario (Dr. Fariba Bashiri)

	SOIA/CC/CEA	BOTH	CSIS Act
	• Canadian Council of Muslim Women • Canadian Human Rights Commission • Chinese Canadian National Council • Council of Agencies Service South Asians • Council of Iranian Canadians • Federation for a Democratic China • Freedom House • Islamic Association of NW Calgary • Islamic Community Centre of Ontario • Montreal Institute for Genocide and Human Rights Studies • Mosaic Institute • Movement for Democracy in China (Calgary) • Muslim Association of Canada • Muslim Association of Canada (MAC) – Edmonton • Muslim Community of Quebec • Muslim Council of Calgary Foundation • Mustafa Bahran, member of the Friends of Yemen and a former Yemeni minister engaged in civil society issues in the diaspora • Nathan Law, Hong Kong Activist, Former Legislator • National Congress of Black Women Foundation • National Council of Canadian Muslims • Ontario South Asian Community Association • Ottawa Muslim Association • Peace Track Initiative (Yemen) • Saskatchewan Human Rights Commission	• The Central and Eastern European Council in Canada • Raoul Wallenberg Centre for Human Rights	• Local 88 (Laura Luu) • Medécins sans Frontières (Joanne Liu) • National Japanese Association of Canada • Dr. Nima Machouf • Pakistan-Canada Association (Haroon Khan) • Richmond Chinese Community Society (Clara Show) • The Centre of Israel and Jewish Affairs • Vancouver Chinatown Foundation (Carol Lee)

	SOIA/CC/CEA	BOTH	CSIS Act
	• The Democracy Fund • Toronto Association for Democracy in China • Uyghur Canadian Solidarity • Uyghur Research Institute • Vancouver Society in Support of Democratic Movement in China		
Industry and Business	• Biotech Industry Association (TBC) • Canadian Association of Defence and Security Industries • Canadian Gas Association • Canadian Security Telecommunications Advisory Committee • Canadian Water and Wastewater Association • Canadian Internet Registration Authority Jennifer Quaid, Canadian Cyber Threat Exchange	• Business Council of Canada	• Canadian Chamber of Commerce • Canadian Council of Innovators • Communitech • Credible Professional Accountable Canada/Chinese Professional Association of Canada (Andi Shi) • MARS Discovery District (Yung Wu) • Supply Chain Canada • The Digital Technology Supercluster
Legal	• Arab Canadian Lawyers' Association • Association des avocats de la défense de Montréal • Barreau du Québec • Canadian Association of Muslim Women in Law • Canadian Bar Association – Criminal Law Section • Canadian Constitutional Foundation • Canadian Council of Criminal Defence Lawyers • Muslim Canada Lawyers' Association • Chinese and South East Asian Legal Clinic • Criminal Lawyers Association • Federation of Asian Canadian Lawyers • South Asian Bar Association • South Asian Bar Association – BC	• Matthew Gourlay (Amici) • Anil Kapoor: Barrister, Kapoor Barristers and Adjunct Prof, York University Osgoode Hall Law School • Gib Van Ert: partner and lawyer, Olthius Ven Art • Shontana Chaudhury: Lawyer, Pape Chaudhury LLP	

	SOIA/CC/CEA	BOTH	CSIS Act
	• South Asian Legal Clinic of Ontario		
Media	• Canadian Association of Journalists • Canadian Ethnic Media Association • Canadian Journalism Foundation • Canadian Journalism Project • Canadian Journalists for Free Expression • Journalists for Human Rights		
NS Practitioners /Law Enforcement	• Canadian Association of Chief of Police – Law Amendments Committee • Daniel Jean, former National Security Advisor to the Prime Minister • Greta Bossenmaier, former Chief, CSE • Mr. Michel Juneau-Katsuya, former Senior Intelligence Officer and Manager, CSIS • Ms. Carolyn Bartholomew, Chairman, United States-China Economic and Security Review Commission • Ms. Jessica Davis • P/T/M law enforcement agencies • Richard B. Fadden, former National Security Adviser to the Prime Minister of Canada, Deputy Minister of National Defence and Director of the CSIS • Ward P.D. Elcock, former Director, CSIS		
PTMIs and Agents or Officers of Parliament		• Federation of Canadian Municipalities • Inuit Tapirlit Kanatami • Metis National Council • P/T officials • Assembly of First Nations	• Office of the Privacy Commissioner
Public Policy	• Government Relations Institute of Canada • Public Affairs Association of Canada	• Centre for International Governance Innovation	• Canadian Institute for Advanced Research

	SOIA/CC/CEA	BOTH	CSIS Act
	• Public Affairs Council • Public Policy Forum		• Mr. Aaron Shull (Centre for International Governance Innovation – CIGI)
Transportation and Aviation	• Air Transport Association of Canada • Association of Canadian Port Authorities • Canadian Airports Council • National Airlines Council of Canada		
Universities/ University Institutions and Associations	• Universities Working Group on Research Security	• Canadian Association of University Teachers • Colleges and Technical Institutes of Canada • U15 • Universities Canada	

TAB H

UNCLASSIFIED
DRAFT FOR INTERNAL USE ONLY

Launch of the Government of Canada Consultations on Foreign Interference Communications Approach

Background

As part of the Government of Canada's ongoing efforts to counter foreign interference (FI), a multi-pronged consultation may be launched mid- to late-August 2023 (TBC). The work includes consultations on the *Canadian Security Intelligence Service Act* (CSIS Act), *Criminal Code*, *Security of Information Act* (SOIA), *Canada Evidence Act* (CAE), as well as ongoing engagement (targeted and general) on the Foreign Influence Transparency Registry (FITR).

Communication Objectives

- Inform the Canadian public and stakeholders about the consultations in order to encourage greater participation and solicit feedback.
- Promote transparency on potential amendments to the law, and the development of new measures, policies or programs targeting foreign Interference, in accordance with Open Government principles.
- Tie various consultations into a broader Government of Canada narrative on ongoing efforts to counter FI.

Recommended Approach

A medium profile approach is recommended to launch the consultations. This includes:

- A joint Public Safety (PS) and Department of Justice (DoJ) news release to announce the consultations, supported by a media lines and questions & answers (MLQA) document. The news release would situate the consultation in a broader context of regular engagement with Canadians on national security issues.
- Hosting a combined narrative (the "chapeau piece") on the Consulting with Canadians webpage that explains the whole-of-government approach to FI and links to the PS webpage (CSIS Act and ongoing FITR efforts) and the DoJ webpage (Criminal Code, SOIA, CEA) where the online consultation papers will be housed.
- Online consultation papers will be made available through the PS and DoJ webpages respectively. The PS webpage will be updated to include a link entitled "Consultations and Engagement on Countering Foreign Interference." This will replicate the combined narrative and include the *CSIS Act* online consultation paper and the updated FITR paper, as well as a link to the DoJ webpage.
- The CSIS website will also be leveraged to drive potential participants to the Consulting with Canadians site.
- Beyond the launch, communications opportunities will be assessed and additional communications activities could be implemented to maintain momentum during the consultation period, including:
    - Bolstering Public Safety's FI web presence.
    - Leveraging PS's Cross Cultural Roundtable September meeting, and any other FI-related ministerial events.
- Consideration will be given to communications for targeted/affected (diaspora) communities (i.e., comms in languages other than EN/FR).

LAST UPDATED: August 21, 2023

- Developing a media relations protocol in support of communications following the consultation launch (e.g., for proactive media engagement) to provide clarity on which department is speaking to what.
- Partners will amplify the PS social media plan and issue social media posts to promote individual launches. Partner posts will be amplified by PS for greater reach as well. Further posts will be published to encourage public participation in the consultations while they are still open.
- Communications will help support a coordinated approach in releasing the consultations "What We Heard" reports in due course.
- While not a response to current events, this plan will be revisited to re-validate approach and activities should a public enquiry on FI in electoral processes proceed in alignment with that potential public enquiry.