# Impacts of Bill C-59 and the New CSE Act on Journalism and Free Expression

By Canadian Journalists for Free Expression and Reporters Without Borders

Submitted to the House of Commons Standing Committee on Public Safety and National Security

February 2018

Table of Contents

## 1. INTRODUCTION

This is a joint submission from Canadian Journalists for Free Expression and Reporters Without Borders. We welcome the opportunity to make a public submission to the Standing Committee on Public Safety and National Security's study of Bill C-59, *the National Security Act, 2017*.

Canadian Journalists for Free Expression (CJFE) monitors, defends and reports on free expression and access to information in Canada and abroad. Rooted in the field of journalism, CJFE promotes a free media as essential to a fair and open society. CJFE boldly champions the free expression rights of all people, and encourages and supports individuals and groups in the protection of their own and others' free expression rights.

Reporters Without Borders/Reporters sans frontières (RSF) is an international non-profit organization defending freedom of information around the world for more than 30 years. Thanks to its unique global network of local correspondents investigating in 130 countries, 12 national offices (Austria, Brazil, Finland, France, Germany, Spain, Sweden, Switzerland, Taiwan, Tunisia, USA, UK) and a consultative status at the United Nations and UNESCO, RSF is able to have a global impact by gathering and providing on the ground intelligence, and defending and assisting news providers all around the world.

This memo explores how the activities of journalists and of other Canadians exercising their constitutional right to free expression may be impacted by proposed reforms to the statute governing the Communications Security Establishment (CSE).

On June 20, 2017, Bill C-59 (formally entitled "An Act Respecting National Security Matters") was introduced in the House of Commons by the Hon. Ralph Goodale, Canada's Minister of Public Safety. Part 3 of Bill C-59, entitled the "Communication Security Establishment Act," entrusts the CSE with a mandate composed of five aspects (foreign intelligence operations, cybersecurity and information assurance, defensive operations, active operations, and technical and operational assistance) and grants the CSE the power to enter into "arrangements" with other intelligence agencies.

This memo will explore both the procedural and substantive implications of each of the foregoing aspects of the CSE's mandate on the activities of Canadian journalists and all others wishing to speak freely on sensitive matters of public concern.

First, we outline the process established by Bill C-59 for authorizing foreign intelligence operations, for amending and extending such authorizations once granted, and for issuing emergency authorizations. In doing so, we examine whether the procedural provisions of Bill C-59 are adequate to protect the free expression rights of journalists and other Canadians.[1] Next, we review each of the five aspects of the CSE's mandate to

[1] Given that the procedure for authorizing intelligence collection under the foreign intelligence aspect of the mandate is quite similar to the process for the four other aspects of the mandate, we use the foreign intelligence provisions to identify procedural weaknesses throughout the Bill.

determine how intelligence gathering activities authorized under each one could cause problems for journalists. Specifically, we consider hypothetical examples of activities the CSE would be authorized to undertake under an aggressive reading of the statute. Finally, we consider the dangers posed by the CSE's unrestrained power to enter into "arrangements" with other intelligence agencies pursuant to Bill C-59.

## 2. IMPACTS OF PROCEDURAL PROVISIONS ON JOURNALISM AND FREE EXPRESSION

The procedural provisions in Bill C-59 are inadequate to protect journalism and free expression in Canada. Since the procedure for authorizing operations under all five aspects of the CSE mandate are relatively similar, we illustrate the weaknesses of C-59's authorization procedures using the example of the foreign intelligence aspect of the mandate below. Elsewhere in this memo, we highlight the relevant differences between the foreign intelligence authorization procedure and those for authorizing operations under the other four aspects of the mandate.

### 2.1. The CSE Mandate

The overarching framing device for the entirety of Part 3 of Bill C-59 is the CSE's mandate, which states that the CSE is Canada's "national signals intelligence agency for foreign intelligence and the technical authority for cybersecurity and information assurance."[2] The bill articulates five "aspects" of this mandate: "foreign intelligence, cybersecurity and information assurance, defensive cyber operations, active cyber operations and technical and operational assistance."[3] Each of these aspects is best thought of as a distinct species of activity the CSE may undertake, aiming at different ends and with discrete procedural hurdles.

When the CSE is conducting activities under the first four aspects of its mandate, it must obtain an "authorization" using the process described below whenever its activities would violate another Canadian law or in circumstances where the Canadian Charter of Rights and Freedom requires such authorization.

### 2.2. Authorization

Three different officials are involved in authorizing CSE activities under the first four aspects of its mandate that would violate another Canadian law. They are:

- the Chief of the Communications Security Establishment ("Chief"), who is appointed by the Governor in Council for a term not exceeding five years and can be re-appointed for a further term not exceeding five years;

[2] S. 16(1).
[3] S. 16(2).

- the "Minister," who by statute is the Minister of National Defence, though any other federal minister can be designated to play this role by the Governor in Council; and

- the Intelligence Commissioner ("Commissioner"), who is a retired judge of a superior court appointed by the Governor in Council for a term of not more than five years, renewable once.

The authorization process for operations under the foreign intelligence aspect of the mandate works as follows.

*First,* the Chief of CSE submits a written application to the Minister. This application must set out facts that would allow the Minister to conclude that there are reasonable grounds to believe that the authorization is necessary, and that the conditions for issuing it are met.[4]

*Second,* the Minister can issue an authorization when they are satisfied that:

- the activities in the authorization are reasonable and proportionate with regards to the nature of the objective;

- the information sought cannot be acquired by any other means;

- once gathered, the information will not be retained for longer than necessary; and

- the minimization requirements, as required by S. 25, adequately protect the privacy of Canadians and others in Canada.[5]

The Minister can issue an authorization for a period of up to a year.[6]

*Third,* once the Minister issues an authorization, they must forward it to the Commissioner, who reviews the authorization to ensure that the conclusions reached by the Minister are reasonable.[7] It is only once the Commissioner issues a written approval of the Minister's authorization that the CSE is empowered to begin an operation.[8]

[4] S. 34(1)–(2).
[5] S. 35.
[6] SS. 27(1), 37(1).
[7] S. 49(1). The Intelligence Commissioner Act, Part 2 of C-59, creates the office of the Intelligence Commissioner, and lays out their responsibilities. Sections 13 and 14 detail their interaction with the CSE.
[8] S. 29.

### 2.3. Reporting

The Chief must provide a written report to the Minister on the outcome of the activities carried out under the authorization within 90 days of its expiration.[9] The Minister provides the Commissioner a copy of the report.[10]

### 2.4. Renewal

The Minister can extend their authorization for up to a year. Although the initial authorization must be approved by the Commissioner, extensions are not reviewable by the Commissioner.[11]

### 2.5. Amendment

If there is a significant change in any fact that was set out in the Chief's application, the Chief must notify the Minister of the change as soon as feasible.[12] If the Minister concludes that the change is significant, the Minister can amend their existing authorization,[13] and must notify the Commissioner of the same.[14] The existing authorization continues to remain in force unless and until the Commissioner approves the amended authorization in writing.[15]

### 2.6. Repeal

The Minister can also repeal their authorization at any time.[16] Bill C-59 does not specify in what circumstances or on what grounds the Minister can repeal authorizations. Neither does it specify any particular repeal procedure.

### 2.7. Emergency Authorizations

The Minister may issue an emergency authorization if, in their sole discretion, they conclude that the conditions for issuing an authorization are met, but that the time required to obtain the Commissioner's approval would defeat the purpose of issuing an authorization.[17]

Emergency authorizations can be made in writing or orally, and the statute does not require a written record of the original authorization.[18] Each application must set out

[9] S. 53(1).
[10] S. 53(2).
[11] SS. 37 (2), (3).
[12] S. 38 (10).
[13] S. 40 (1).
[14] S. 38(2).
[15] S. 40(3).
[16] S. 39.
[17] S. 41(1).
[18] S. 41(3)(a).

facts sufficient for the Minister to reasonably conclude that the normal authorization procedure would take too long.[19]

Emergency authorizations are valid for a period not exceeding five days,[20] and the Minister must notify the Commissioner of any emergency authorization as soon as feasible after issuing it.[21] As with other authorizations, the Chief must issue a written report to the Minister within 90 days of the expiration of the emergency authorization.[22] As such, there would be no written record of the emergency authorization until the report issued, up to 95 days after the request. And that report would only have to detail the results of the surveillance – not the contents or intention of the original request.[23] Accordingly, the CSE could recast their emergency authorizations in a more favorable light by framing their reports as successfully obtaining what they got, rather than answering whether they accomplished the task they set out to do initially.

### 2.8. Targeting and Minimization

Bill C-59 establishes as a general rule that no CSE operations may be "directed at" a Canadian citizen or person in Canada (hereinafter, "Canadians").[24] This principle is subject to at least two major exceptions that come close to swallowing the rule. First, this limitation against directing operations at Canadians does not apply to the technical assistance aspect of CSE's mandate. Second, and of much greater concern, the public data exception allows the CSE to collect *all* publicly available information about everyone, everywhere—regardless of their citizenship or residency (discussed further in Section 3.1.2., below).

Even taking the general principle against targeting Canadians at face value, Bill C-59 expressly permits the CSE to collect "incidental" information about Canadians while conducting its operations.[25] "Incidental" collection occurs when information about Canadians is collected as part of an operation targeting one or more non-Canadians. For example:

*The CSE is monitoring the communications of Alicia, a Spanish national living in Italy. Alicia emails with Brandon, a Canadian citizen living in England, and Carole, a French citizen living in Canada. The CSE cannot direct any operation at Brandon or Carole. However, any information relating to Brandon or Carole collected while monitoring Alicia, such as their email communications, is "incidental" collection.*

---

[19] S. 41(3)(b).
[20] S. 43.
[21] S. 42.
[22] S. 53(1).
[23] S. 53(1) ("a written report … on the outcome of the activities").
[24] S. 23.
[25] S. 24(4).

Some such incidental collection of the communications of Canadians is perhaps inevitable, but the problem with Bill C-59 is that its measures for dealing with the risks that incidental collection poses to the privacy of Canadians is inadequate. Bill C-59 includes a minimization clause that, in theory, limits the CSE's use, retention, and sharing of information it has incidentally collected about Canadians. However, the *entire* minimization provision of Bill C-59 reads as follows:

The Establishment must ensure that measures are in place to protect the privacy of Canadians and of persons in Canada in the use, analysis, retention and disclosure of [information collected pursuant to any of aspects of the mandate or the public data exception.][26]

The skeletal nature of C-59's minimization provisions should give all Canadians who care about their privacy serious cause for concern. This is because it delegates substantial power to the CSE to decide what "measures" (if any) it wishes to take to "protect the privacy of Canadians and of persons in Canada…." This is tantamount to placing the foxes in charge of the henhouse, given that the CSE—like all intelligence agencies—has a structural interest in collecting as much information as it possibly can.

One potential check on the CSE comes from the authorization procedures. In those situations where the CSE must obtain an authorization before it acts under its foreign intelligence or cybersecurity mandates, the Minister must determine (among other things) that the CSE has minimization procedures in place that will result in information pertaining to Canadians being retained and analyzed only when it is "essential."[27] Since the Minister is broadly responsible for the administration of Canada's national defence regime, they have similar structural incentives to the CSE to favour gathering more information over thorough privacy protections—although it is of some consolation that Ministerial authorizations are (usually) subject to the approval of the Intelligence Commissioner.

In any event, the threadbare language of C-59's minimization provisions raise serious democratic accountability concerns. It ought to be for Parliament specify what measures are adequate to protect the privacy interests of Canadians, rather than leaving such questions to be answered by yet-to-be-written regulations[28] and the secret processes by which the CSE's operations are authorized.

### 2.9. Analysis of Authorization Provisions

In many respects, C-59 is a structural, procedural bill that defines how the CSE should go about seeking authorization for various kinds of operations. Unfortunately, these

---

[26] S. 25.

[27] Supra Section 2.1. See also S.35(2)(c) and 35(3)(d).

[28] The exact rules of Section 25 would be filled in by the CSE's general regulations procedure, where the Governor in Council may, on the recommendation of a Minister, make regulations governing the conduct of the CSE. S. 61(b).

processes are insufficient to safeguard the privacy and free expression rights of Canadians because they vest too much authority in the hands of a few decision-makers without providing concrete substantive standards to guide decision-making. This structure merely serves to reinforce the CSE's power to collect vast amounts of information in secret.

Another weakness concerns the scope of activities that may be covered by a single authorization. The authorization provisions for the CSE's activities under its foreign intelligence and cybersecurity mandates are both blanket in nature. The authorization provisions for the former mandate are, for example, written in terms of authorizing "activities and classes of activities."[29] The breadth of the activities that can be authorized with a single authorization raises hard questions about the adequacy of Bill C-59's three-step process for issuing authorizations.

On a different note, the amendment, extension, and emergency authorization processes are rife with the possibility of abuse, since the Minister is the sole decision-maker for all three of these processes. The emergency authorization procedure should be of particular concern to Canadians since Bill C-59 does not contain any anti-abuse provisions, such as a limit on consecutive emergency authorizations or even the requirement that written records of such authorizations be kept.

## 3. IMPACTS OF ASPECTS OF THE MANDATE ON JOURNALISM AND FREE EXPRESSION

Each aspect of the CSE's mandate draws on different tools, and thus presents distinct threats to free expression. The sections below walk through each of these aspects and identify the most serious threat each presents.

### 3.1. Foreign Intelligence Operations

The foreign intelligence aspect of the mandate gives the CSE wide latitude to "acquire" and use information from the "global information infrastructure" to serve Canada's intelligence and national security interest. The verb "acquire" is not defined anywhere in Bill C-59, while the "global information infrastructure" is defined as pretty much anything that stores or transports data, including the underlying data itself.[30]

It is in the CSE's interest for these terms to be defined as broadly as possible. If "acquire" was limited to certain enumerated methods, the CSE could find itself unable to change its information-gathering strategies without going through Parliament. The upshot, however, is that there are effectively no limits on *how* the CSE may collect information.

[29] S. 27(2).

[30] Bill C-59 defines the "global information infrastructure" to include "electromagnetic emissions, any equipment producing such emissions, communications systems, information technology systems and networks, and any data or technical information carried on, contained in or relating to those emissions, that equipment, those systems or those networks. (*infrastructure mondiale de l'information*)." S. 2.

Conscious of this incredibly broad collection authority, C-59 attempts to channel the activity of the CSE in two ways. First, each aspect of the mandate has internal structural limitations on what activities may be carried out under that aspect. For example, authorizations under the 'cybersecurity' aspect are limited to providing advice or services to statutorily identified entities.[31] Second, when actually submitting a request for authorization, the CSE must specify the particular means that will be employed in the operation, and identify conditions or restrictions on those means to ensure that the CSE's behavior is reasonable and proportional to the goal of the authorization.[32]

For example, the CSE may monitor any "electromagnetic emissions [or] any equipment producing such emissions."[33] This definition allows the CSE, most mission critically, to monitor wireless networks but encompasses any device that produces even a small amount of emissions. As such, all of the work narrowing where and when the CSE acts is done not by the authorizing statute, but by internal establishment requests, away from the public eye.

Considering the broad scope of the foreign intelligence aspect of the mandate, and the weakness of Bill C-59's authorization procedures and privacy protection measures, below are some illustrative hypotheticals demonstrating how the powers conferred in this legislation can be used to interfere with the work of journalists and others exercising their free expression rights.

3.1.1. Foreign Source Protection

Once it is operating under an Authorization, there are few if any restraints on the CSE monitoring non-Canadians, or collecting and analyzing communications between non-Canadians and Canadians.

*Hypothetical Scenario: The CSE obtains an Authorization for a Foreign Intelligence operation in Syria, where Canada has standing counter-terrorism concerns.[34] A Canadian journalist, writing on both the situation in Syria and the Syrian diaspora in Canada, corresponds with persons in Syria whose communications are being monitored by the CSE. Consequently, the Canadian journalist's communications with her Syrian sources end up being collected by the CSE.*

The possibility that the CSE can collect and monitor Canadian journalists' communications with sources located abroad may chill or frustrate the legitimate activities of such journalists. It may also deter foreign sources from speaking with Canadian reporters.

---

[31] S. 18.

[32] S. 36(a). Note, however, that these restrictions do not apply to the technical assistance aspect of the mandate.

[33] S. 2.

[34] Department of Public Safety, *2014 Public Report On The Terrorist Threat To Canada*, 21 (2014). Available at: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2014-pblc-rpr-trrrst-thrt/2014-pblc-rpr-trrrst-thrt-eng.pdf [https://perma.cc/C3J3-H358]

### 3.1.2. Public Data Exception

C-59 authorizes the CSE to collect "publically available information"[35] in pursuing all aspects of its mandate save for technical and operational assistance.[36] Publicly available information includes anything *anyone* posts on the open web or on social media. It may even include data collected by third-party data aggregators, such as Equifax Canada, or even information that has been hacked and made available for sale on the 'dark web.' As a consequence, the CSE has substantial capacity to collect and retain information relating to Canadians, independent of any authorization issued under a particular aspect of the mandate.

The most troubling implication of the public data exception is that there are no real limits on what the CSE may do with the information it gathers. The use of such publicly available information may not have to be connected to an extant authorization under an aspect of the mandate. The relevant language says only that such information must be used "in furtherance of [the CSE's] mandate."[37] Notably, similar authorizations elsewhere in the bill are framed in reference to *specific* aspects of the mandate.[38] As such, the public collection authority could plausibly be a permanent capability of the CSE, untethered to the authorization structure designed to channel the CSE's behavior.

Considering the breadth of information available online, in combination with the CSE's powers to collect information from foreign allies by entering into Arrangements,[39] and from other branches of government, the CSE could potentially build comprehensive digital dossiers on Canadians without ever running afoul of Bill C-59's prohibition on directly targeting Canadians.

*Hypothetical Scenario: Looking to identify and curb the incidence of "extremist travelers" (i.e., Canadians who travel abroad to conflict zones to engage in terrorism), the CSE obtains a foreign intelligence authorization to monitor the communications of suspected recruiters located in Somalia, a popular 'extremist traveler' destination. To bolster their formal intelligence gathering, the CSE also decides to create periodic copies of publically available Twitter and Facebook posts that mention Somalia, or other related hashtags. The CSE then combines these two sets of information, matching the contents of intercepted communications with the publicly available information. The result is the creation of a large database containing the information of large numbers of entirely innocent people with some connection to Somalia (including most Somali-Canadians, and practically all journalists writing about Somalia in Canada and beyond), in order to collect intelligence on a few potential extremist travelers.*

---

[35] Bill C-59 defines "publicly available information" as "information that has been published or broadcast for public consumption, is accessible to the public on the global information infrastructure or otherwise or is available to the public on request, by subscription or by purchase. (*information accessible au public*)." S. 2.
[36] S. 24. The scope of Section 24(1) is defined by reference to Sections 23(1) and 23(2). This immunizes the section from the prohibition of directing CSE action at Canadian citizens or persons in Canada.
[37] S. 24.
[38] *See, e.g.,* SS. 24(3), 25(a), 26(1)–(2), 27(1).
[39] S. 55.

### 3.2. Cybersecurity and Information Assurance Authorizations

The cybersecurity and information assurance aspect of the CSE's mandate authorizes the Establishment to carry out two basic kinds of activities. First, the CSE may provide technical advice or support to other federal institutions or to private infrastructure providers designated as "being of importance to the Government of Canada."[40] These provisions raise two immediate concerns: first, the entities that may be defined as "of importance" includes not only any type of information infrastructure, but also encompasses electronic information itself.[41] It appears that this aspect of the mandate covers the integrity of the information itself, not just the systems that house it. Second, the Minister has full discretion to designate structures or information as "of importance" and thus falling within the aspect of the mandate. Consequently, this aspect of the mandate has no conceivable limiting principle as to what data or systems the CSE could operate within.

Second, the CSE may acquire information from the global information infrastructure "or other sources" to provide such services.[42] Narrowly read, this aspect of the mandate appears to authorize the CSE to collect information from the entity they are working on in order to address whatever concern has manifested. However, the language equally supports a wider scope of collection—especially given the blanket nature of authorizations under this mandate. As the expert in signals intelligence and cybersecurity, and the explicit provider of technical assistance to federal institutions, the CSE may (justifiably) be presumed to be dealing with complicated or pernicious threats. Given that Canadian government networks and infrastructure "of importance to the Government of Canada" is under constant cyber-attack, the text of the statute would support expansive inquiries to understand such attacks, their implications, and their sources, with attendant consequences on the privacy rights of Canadians. Such large-scale monitoring by the CSE of government and private communications networks may chill sources and whistle-blowers from sharing information with journalists, for fear that they might be detected by these programs.

#### 3.2.1. Disclosure and Information Sharing

Bill C-59 gives the CSE the ability to disclose the information obtained through cybersecurity and foreign intelligence operations to "any person" who the Minister (of National Defence) chooses to designate.[43] The bill provides no limiting principles on who the Minister may designate, nor does it contain any language preventing the CSE from disclosing information that can identify a Canadian person or the contents of their intercepted communications.

---

[40] S. 18(a).
[41] S. 22(1).
[42] S. 18.
[43] SS. 44, 46.

Section 44 permits the disclosure of information obtained through foreign intelligence operations—including the identity of Canadian persons—if the CSE determines that disclosure is "*essential*" to "international affairs, defence, security or cybersecurity."[44] Similarly, section 45 permits the disclosure of information collected in cybersecurity operations, when such disclosure would be "*necessary*" to protect "information infrastructures" covered by the Cybersecurity aspect of the CSE mandate.[45]

While "essential" and "necessary" are admittedly high bars, they are amorphous concepts, left entirely for the CSE to define internally. Unlike the authorization structure in place for operations, there is no oversight mechanism or required formal reporting mechanism for disclosures. It is unclear who, aside from the CSE itself, would be in place to hold the CSE responsible for disclosures that may not rise to their own high bar of "essential."

What is more, when the CSE has reason to believe they possess information about a Canadian citizen relevant to "an immediate danger of death or bodily harm to *any individual*," it may then analyze and then disclose such information to "any relevant person."[46]

None of these disclosure provisions mention the minimization procedures laid out in Section 25.[47] Given that section 25 is currently a skeletal provision, it is not clear if information that is disclosed under sections 44–47 is subject to minimization *before* it is shared.

The narrowest reading of these provisions is that they permit the CSE to disclose critical information to other parts of the Canadian government so that they can act upon it. The more troubling possibility is that they permit the CSE to collect private communications or identifying information regarding any individual, and then share this information with *anyone* in the "class of persons" designated by the Minister.

*Hypothetical Scenario: A foreign intelligence authorization to monitor communications in Pakistan, where Canada has ongoing counter-terrorism concerns, uncovers communications between persons of interest in Pakistan and several residents of Canada. The CSE discloses all of the information to the RMCP, a previously authorized person under the statute. Among the communications was a reporter researching the Pakistani diaspora; she is now caught up in both foreign signals intelligence monitoring and domestic watch lists.*

There are compelling reasons for why the CSE should be able to analyze and share the information it collects in certain circumstances, but leaving the entirety of the 'who' and

[44] S. 44.
[45] S. 45.
[46] S. 47.
[47] *See infra* Section II.7.

'when' to be decided by the CSE does not meaningfully inform the people of Canada about the scope of permitted disclosures.

### 3.3. Defensive and Active Cyber Operations

The Defensive and Active Cyber Operations aspects of the CSE's mandate under Bill C-59 can be thought of as a shield paired with a sword, for they have similar authorization procedures and use similar tools.

The defensive cyber operations aspect of the mandate allows CSE to protect the federal government's data or electronic information infrastructures, as well as private-sector data and infrastructure identified as "of importance" to the Government of Canada.[48] Meanwhile, the active cyber operations aspect of the mandate allows the CSE to act on outside systems to "degrade, disrupt, influence, respond to or interfere with the capabilities of a foreign individual, state, organization or terrorist group as they relate to international affairs, defence or security."[49]

The authorization process for defensive cyber operations differs from the authorization process for foreign intelligence and cybersecurity operations in four ways.

- First, the Minister must consult with the Minister of Foreign Affairs before issuing an authorization.
- Second, authorizations under this aspect of the mandate do not need the approval of the Commissioner; thus, the Minister is the sole decision-maker.
- Third, the Minister cannot extend defensive cyber operations authorizations.
- Finally, the emergency authorization procedure does not apply to defensive cyber operations (presumably because the Minister can authorize such operations by herself).

The authorization process for active cyber operations is identical to that for defensive cyber operations authorizations, except that the Minister of Foreign Affairs must consent to the authorization before any operations can begin.

#### 3.3.1. Risks to Journalists & Free Expression

Journalists and the free press in Canada and abroad face particular risks from the CSE's new active operations mandate. The crux of the problem relates to the CSE's ability to "degrade, disrupt, influence, respond to or interfere with the capabilities" of non-Canadian entities "as they relate to international affairs." The term "international affairs" is left undefined by Bill C-59, and it is sufficiently vague that one could conceive of the CSE engaging in the following kinds of operations under this aspect of its mandate:

[48] S. 19.
[49] S. 20.

- The CSE could "disrupt" the capabilities of a foreign news organization (regardless of whether it is publicly- or privately owned) by disrupting access to its website or disrupting its internal communication networks.
- The CSE could "influence" a foreign news organization by forging or altering documents relied upon by its journalists, and in so doing "influence" a foreign government or other entity to do something that the Canadian government deems advantageous.
- The CSE could "interfere with" the capabilities of foreign actors, including journalists, by interfering with key technologies such as encryption tools and anonymity software that journalists and others routinely use in their work.

Even if the CSE's activities under all three of these hypothetical scenarios were targeted at non-Canadian entities, each of the scenarios would directly impact Canadians. For example, if the CSE were to "disrupt" a foreign news organization, the ability of Canadians to access that information source would be disrupted, and so too would the work of any Canadian journalists who collaborate with that foreign outlet. In the second hypothetical, if the CSE were to induce a foreign news organization to report on a false story, that story would result in Canadians being misinformed as well, and the story could even end up being picked up by a Canadian news outlet. And under the third scenario, CSE interference with the tools that foreign governments or journalists use would equally impact Canadians (including journalists) who rely on those tools in the course of their professional and private activities.

To be sure, the CSE's powers under the active cyber operations mandate may not be used to "cause… death or bodily harm to any individual" or to "obstruct, pervert or defeat the course of justice or democracy."[50] These vague constraints are an insufficient safeguard on powers that are vaguely defined and potentially vast in their impact on Canadians and non-Canadians alike.

There are also a number of risks to journalists in Canada and beyond and to the right of free expression more generally from the defensive cyber operations aspect of the CSE's mandate, which allows the Establishment to "protect" federal information and computers, or other systems designated as having national importance.[51] For example, malware developed by the CSE for, say, the purpose of disabling a cyber-attack could infect and disable the computers of innocent third parties, including journalists.[52] Alternatively, a journalist relying on confidential sources or 'white-hat' actors may be caught up in defensive measures designed to prevent intrusions or exfiltration of information.

---

[50] S. 33(1)(a) and (b).

[51] S. 19.

[52] For example, it is widely believed that the Stuxnet worm was developed to specifically target Iranian nuclear centrifuges, but it managed to infiltrate and infect a large number of civilian computers as well. James Ball, *U.S. Hacked Into Iran's Critical Civilian Infrastructure For Massive Cyberattack, New Film Claims*, BUZZFEED NEWS (Fed. 16, 2016) https://www.buzzfeed.com/jamesball/us-hacked-into-irans-critical-civilian-infrastructure-for-ma?utm_term=.slQoAjkNG#.osO6ap48Y. [https://perma.cc/76KX-VLSE].

### 3.4. Technical and Operational Assistance

Sections 21 and 26 of Bill C-59 set out the technical and operational assistance aspect of the CSE's mandate. Section 26 expressly empowers the CSE to provide "technical or operational assistance to federal law enforcement or security agencies, the Canadian Forces or the Department of National Defence."[53] The text of the bill is not clear as to whether the CSE may proactively offer their help to these other agencies, or whether they may only react to a request from one of these agencies for help. Insofar as Bill C-59 states, however, that the CSE would have the same legal authority, obligations, and immunities as whatever government agency they are assisting,[54] it would seem that this aspect of the mandate is reactive, rather than proactive.

The technical and operational assistance provisions of Bill C-59 do not detail what sorts of activities the CSE can perform under this authority. It might be wise from a practical perspective not to enumerate exactly what kinds of assistance the CSE can provide, so that it can respond appropriately as needs arise. Yet this decision leaves Canadians in the dark as to how exactly the CSE's capabilities can be used in the domestic law enforcement context.

Furthermore, it is worrisome that the privacy protections in Section 25 and the prohibition on directing activities against Canadian citizens or residents in Section 23 could be read to not apply to authorizations under this aspect of the mandate. The text of Section 25 explicitly references other aspects of the mandate, but does not mention the technical and operational assistance aspect; the same is true for Section 23(a). Therefore, an aggressive reading of the statute would suggest that the CSE is less bound when acting domestically than when acting abroad – flying in the face of the entire statutory scheme of enshrining more protections on domestic persons.

Admittedly, the CSE is limited by the "same limitations" imposed by domestic law as whatever agency they are supporting, which explicitly include warrant requirements.[55] These domestic restraints may fill in for the CSE's own restrictions when acting domestically – but, as regulations for "normal" law enforcement agencies that do not have the technical capacity that a signals intelligence agency might, run the risk of being inadequate to protect individuals' privacy rights. Additionally, the text of these provisions leave it to the CSE to interpret how far this authority really extends, rather than having such limits expressly defined in their own statute.

Consequently, the technical assistance aspect of the mandate may bolster domestic surveillance by other Canadian law enforcement agencies. To the extent that those agencies may seek to suppress journalistic activity and free expression, this provision strengthens those efforts. Depending on how aggressively the CSE decides to interpret its

[53] S. 26.
[54] SS. 26(1)–(2).
[55] S. 26(1).

own limitations, the impacts could be quite substantial. Increasing the specificity on what types of assistance may be provided would be one way of lessening these concerns.

*Hypothetical Scenario: The RMCP is concerned about protestors using encrypted communication services. They request the assistance of the CSE, which leverages its technical expertise to compromise the encryption, and further uses its public data collection to identify users and their immediate contacts.*

### 3.5. Arrangements

Under Section 55, the CSE may enter into "Arrangements" with peer intelligence agencies to cooperate, share information, or otherwise further its mandate.[56] The only procedural requirement for entering into Arrangements is that the Minister must consult with the Minister of Foreign Affairs before approving a new "Arrangement."[57]

The text of Section 55 does not appear to limit what the "Arrangements" may entail. It does not limit what the CSE can do to help its foreign partners, or what those partners can do to help the CSE. There is nothing in the text of Bill C-59 that expressly requires the CSE to minimize or limit its ability to incidentally access or collect information about Canadian persons through resources made available by foreign agencies to the CSE in the course of an "arrangement." While some foreign agencies, notably the CSE's Five Eye partners, may not 'direct' their activities at Canadians, these agencies may retain Canadian data even if it is not immediately essential to their respective mandates.[58] Other foreign entities with whom the CSE might enter into arrangements may not be limited from directing their activities at Canadians at all. In short, "arrangements" with foreign partners are likely to provide the CSE with access to far greater amounts of Canadian data than it would otherwise have.

Furthermore, what exactly constitutes an "Arrangement" remains unclear. This is troubling because the precise procedural and informational protections that may apply to collected information are therefore left undefined. The procedure required by C-59 before the CSE may enter into an "arrangement" is much more limited when compared to the procedures to obtain authorizations under other aspects of the mandate. Data made available by foreign partners may potentially be acquired in a manner that bypasses safeguards under which the CSE normally operates—in other words, it may be data which the CSE would otherwise require an authorization from the Minister and Intelligence Commissioner to collect on its own. And unlike those latter procedures,

---

[56] S. 55.

[57] S. 55(2).

[58] Similarly, the CSE is only obligated to limit its retention of non-essential Canadian data, not its retention of incidentally collected yet non-essential data of citizens of its Five Eye partners. See proposed paragraph 35(2)(c) (CSE cannot retain use, analyze or retain information identified as relating to a Canadian or a person in Canada unless that information is deemed to be essential to international affairs, defence or security); and proposed section 44 (CSE may disclose to third parties any Canadian identifying information collected, used, analyzed or retained under a foreign intelligence authorization if the disclosure is deemed essential to foreign intelligence).

which tie back to specific aspects of the CSE's mandate, Bill C-59 lets the CSE enter into arrangements on broader terms, "the purposes of the furtherance of [the CSE's] mandate." S. 55(1).

In view of this confusion and the substantial powers that the CSE could gain by entering into arrangements, it is incredibly important that Parliament provide a clearer public legal framework for entering into "arrangements."

The gravest risk therefore is that the CSE can do an end run around limitations on under which it otherwise operates, including domestic minimization obligations by entering into arrangements. Even if that is not the intent of the provision, Bill C-59's lack of guidance on what such arrangements may contain is troubling.

## 4. CONCLUSION AND RECOMMENDATIONS

1. Privacy and Minimization Procedures: Section 25 currently contains no substantive protections for Canadians' information. There is no indication of what procedures may be adopted, or when the CSE will elect to put them into effect. Even if the government is unwilling to move away from the purely regulatory approach to CSE's privacy protections, C-59 should at the very least articulate a set of privacy principles so that the general public understands what the Establishment may or may not do.

2. Public Data Exception: Giving the CSE carte blanche to collect and use information in the public sphere furnishes the Establishment with extensive capabilities to monitor Canadians directly. Though these concerns could be addressed by strengthening Section 25, the public data exception itself should be limited to foreclose potential abuse.

3. Technical and Operational Assistance: the public cannot meaningfully evaluate what CSE cooperation with other national authorities looks like, from either a procedural or substantive perspective. Given the CSE's significant technical expertise, and the risk that such technical assistance is free from the restrictions that would otherwise bind the CSE, the technical assistance aspect may be a way for the CSE to directly act or encourage domestic invasions of privacy or restrictions on free speech.

4. Arrangements: at present, there is no guidance on what an arrangement entails, or what sort sorts of information may be exchanged. There ought to be greater specificity on what steps the CSE must take, and what information they may receive and share.

C-59 is a bill that is long on process but short on substance where it matters. It successfully outlines how the CSE should function from a procedural point of view, but does not detail what that Agency can and cannot substantively do. To ensure that the CSE does not run roughshod over human rights, Bill C-59 should define the substance of its aspects of the mandate as clearly as it defines the Agency's internal procedures.