Government's Defence of Proposed CSE Act Falls Short

By Lex Gill, Tamir Israel, and Christopher Parsons

JANUARY 30, 2018
RESEARCH REPORT #105

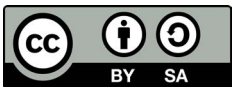
munk school
OF GLOBAL AFFAIRS & PUBLIC POLICY

UNIVERSITY OF TORONTO

THECITIZENLAB

Copyright

© The Citizen Lab



Licensed under the Creative Commons BY-SA 4.0 (Attribution-ShareAlike licence). Electronic version first published in 2018 by the Citizen Lab. This work can be accessed through https://citizenlab.ca/2018/01/governments-defence-of-proposed-cse-act-falls-short/.

Document Version: 1.0

The Creative Commons Attribution-ShareAlike 4.0 license under which this report is licensed lets you freely copy, distribute, remix, transform, and build on it, as long as you:

- give appropriate credit;
- indicate whether you made changes; and
- use and link to the same CC BY-SA 4.0 licence.

However, any rights in excerpts reproduced in this report remain with their respective authors; and any rights in brand and product names and associated logos remain with their respective owners. Uses of these that are protected by copyright or trademark rights require the rightsholder's prior written agreement.

Suggested Citation

Lex Gill, Tamir Israel, and Christopher Parsons. "Government's Defence of Proposed CSE Act Falls Short," Citizen Lab Research Report No. 105, University of Toronto, January 2018.

About the Citizen Lab, Munk School of Global Affairs and Public Policy, University of Toronto

The Citizen Lab is an interdisciplinary laboratory based at the Munk School of Global Affairs and Public Policy, University of Toronto, focusing on research, development, and high-level strategic policy and legal engagement at the intersection of information and communication technologies, human rights, and global security.

We use a “mixed methods” approach to research that combines methods from political science, law, computer science, and area studies. Our research includes investigating digital espionage against civil society, documenting Internet filtering and other technologies and practices that impact freedom of expression online, analyzing privacy, security, and information controls of popular applications, and examining transparency and accountability mechanisms relevant to the relationship between corporations and state agencies regarding personal data and other surveillance activities.

Contents

On Publicly Available Information 6

Cybersecurity Services for Non-GoC Clients: Deploying the CSE's "unique cybersecurity tools on non-government systems" at the request of system owners 7

A General Comment about the Proposed Cyber Operations Powers 8

- **Defensive Cyber Operations: "Disabling Foreign Servers Suspected of Stealing Information" or "Corrupting Stolen Information Stored on Foreign Servers"** 10
- **Defensive Cyber Operations: "Degrading Foreign Systems during State-Sponsored Cyber Operations against North American Financial Institutions or Against Canadian Democratic Institutions"** 11
- **Active Cyber Operations: "Disabling or Interfering with Terrorist Devices and Infrastructure Used for Media and Communications"** 12
- **Reflections on "Active" and "Defensive" Cyber Operations Powers, Human Rights, and the Charter** 12

Assistance: "Collecting and Processing Communications" and "Designing Technical Solutions" for Law Enforcement and Security Agencies 14

Concluding Thoughts on the Government of Canada's Briefing Notes 15

The Government of Canada introduced new national security legislation in the summer of 2017. Bill C-59, *National Security Act, 2017* ("Bill C-59" or "the Bill"), would significantly change how Canada's signals intelligence agency, the Communications Security Establishment (CSE) operates. These reforms are largely contained in the proposed *Communications Security Establishment Act* ("CSE Act") in Part 3 of the Bill.

Since the Bill was first proposed, a range of civil society groups and academics have called for significant amendments to the proposed *CSE Act*. A co-authored report by the Citizen Lab and the Canadian Internet Policy & Public Interest Clinic (CIPPIC) represents the most detailed and comprehensive analysis of these reforms to date. Calls for amendment have principally focused on:

- Concerns related to the new "active" and "defensive" cyber operations powers, which would let the CSE use its expertise to engage in state-sponsored hacking
- The need to improve the review and oversight framework to ensure that they provide an adequate level of protection given the risk to the Charter-protected rights of Canadians and persons in Canada as well as internationally recognized human rights abroad
- The risk that the proposed *CSE Act* would normalize foreign-facing mass surveillance activities, which are neither inherently necessary nor proportionate
- The sweeping exceptions to the CSE's general prohibition on "directing" its activities at Canadians, including exceptions that allow the CSE to acquire "publicly available" information, a definition broad enough to include information stolen or otherwise illegally obtained by the seller

In support of its first appearance on the Bill in November at the House of Commons Standing Committee on Public Safety and National Security (SECU), the Government of Canada prepared a briefing book detailing its positions on the proposed *CSE Act*. Bill C-59 was referred to SECU immediately following its introduction in the House of Commons for a comprehensive review of the merits and flaws of the bill and to amend the legislation as it sees fit. We were provided with a lightly-redacted copy of that briefing book by the Government of Canada, which is available here.

In this post, we evaluate the Government's explanation of some of the more problematic elements of Bill C-59 in its briefing notes. Our comments regarding the Government's briefing notes draw from the joint report published in December 2017 by the Citizen Lab and CIPPIC. We ultimately conclude that while the government's

briefing material provides insight into some of the ways that the CSE might act following the passage of the *CSE Act*, the material itself does not resolve our concerns with the *CSE Act*.

On Publicly Available Information

The briefing document outlines a number of situations in which the CSE could obtain "publicly available information" should Bill C-59 become law. However, there is a vast gap between the examples provided in this briefing document and the actual breadth of the provision. Specifically, while the CSE is generally prohibited from 'directing' its activities at Canadians or people in Canada, the proposed *CSE Act* would permit the Establishment to do so when "acquiring, using, analyzing, retaining or disclosing" publicly available information.

Based on the briefing material, the CSE intends to use the "publicly available information" provision to "conduct basic research" but not to "conduct investigations" or use publicly available information as "a means of collecting intelligence." The material additionally spells out that the CSE "would not acquire information that was unlawfully obtained, such [as] through a compromise or a leak, under this provision" and instead would use this section of the proposed *CSE Act* to subscribe to academic and trade journals, read or access publicly available malware information to help reverse engineer malware sample, or look at company websites to identify points of contact when engaged in cybersecurity and information assurance activities.

- The intent of this provision is to allow CSE to conduct basic research in support of its mandate without fear of the restriction that it not direct its activities at Canadians or persons in Canada.
- This is not an authority to conduct investigations, or a means of collecting intelligence.
- For example, CSE may use publicly available information to provide useful context or background information to an intelligence or information assurance report.
- CSE 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 publicly available information.

If pressed:

- CSE would not acquire information that was unlawfully obtained, such through a compromise or a leak, under this provision.

Figure 1: Publicly Available Information Exception from Government of Canada's briefing book detailing its positions on the proposed CSE Act.

We agree that there are unlikely to be privacy concerns with the Establishment reviewing intelligence reports, reading blog posts, learning about mathematics, or searching for corporate contact information on public websites. We take no issue with the Establishment having such abilities and believe such conduct can be exempted from the CSE's general prohibition on directing its activities at Canadians. Unfortunately, these innocuous examples are far from the full extent of what the CSE can collect about Canadians under the "publicly available information" exception.

As pointed out in our co-authored report, Bill C-59's publicly available exception encompasses problematic activities such as wide-ranging profiling of Canadians based on public social media activity, purchasing information from foreign data brokers whose acquisition of Canadian data often occurs without regard of Canadian laws, and purchasing or otherwise acquiring highly sensitive personal information which has been illegally stolen or leaked from company or government servers.

Since, according to their brief, the CSE believes this kind of problematic conduct should be off limits, they should have no problem wholeheartedly supporting our recommended amendment to the CSE Act which would preclude it. While we are reassured to hear that they do not currently plan to engage in these problematic forms of surveillance, there is nothing in the law that would stop them from changing their mind at a later point. Hopefully we can all agree that this is an easy fix.

Read more about the "publicly available information" exception:

- "Spy bill allows government security agency to collect 'publicly available' info on Canadians," by Alex Boutilier in the *Toronto Star*
- "Canada's spy agencies casting wider net on citizens' electronic data, parliamentary report says," by Colin Freeze in the *Globe and Mail*

Cybersecurity Services for Non-GoC Clients: Deploying the CSE's "unique cybersecurity tools on non-government systems" at the request of system owners

Per the proposed *CSE Act*, the CSE would be permitted to intercept private data and carry out other intrusive activities on a government agency's internal networks when providing its assessment of the threat or providing defensive services. However, the Minister has broad discretion to designate non-governmental electronic information or infrastructure as "important", bringing it within the CSE's mandate. Whereas

the CSE may already "share information about specific cyber threats" with non-government clients, the ability to carry out intrusive activities on private Canadian systems and infrastructure is an exceptional departure from the CSE's current legal framework, and can potentially implicate a large number of private sector actors. While it is difficult to speculate with regard to the full range of information and infrastructure that will ultimately be designated as 'important', at minimum this designation is likely to apply to entities in sectors such as banking, defense, energy, telecommunications, and transportation.

Past revelations of the CSE's activities included realizations that the Establishment has deployed a global sensor network, cover-named EONBLUE, which analyzes vast quantities of information that is directed at the Government of Canada's infrastructure as well as information which transits the global information infrastructure. This proposal may expand the CSE's ability to further deploy its sensor network which, in addition to passively *monitoring* for threats is also intended to *interdict and degrade* possible threats by manipulating communications. There is a significant risk that such activities both may inadvertently target legitimate communications made by Canadians, persons in Canada, and residents and citizens of foreign countries. Moreover, such activities constitute mass surveillance of communications infrastructure and, thus, an explicit approval for the CSE to engage in highly controversial and rights-infringing activities.

A General Comment about the Proposed Cyber Operations Powers

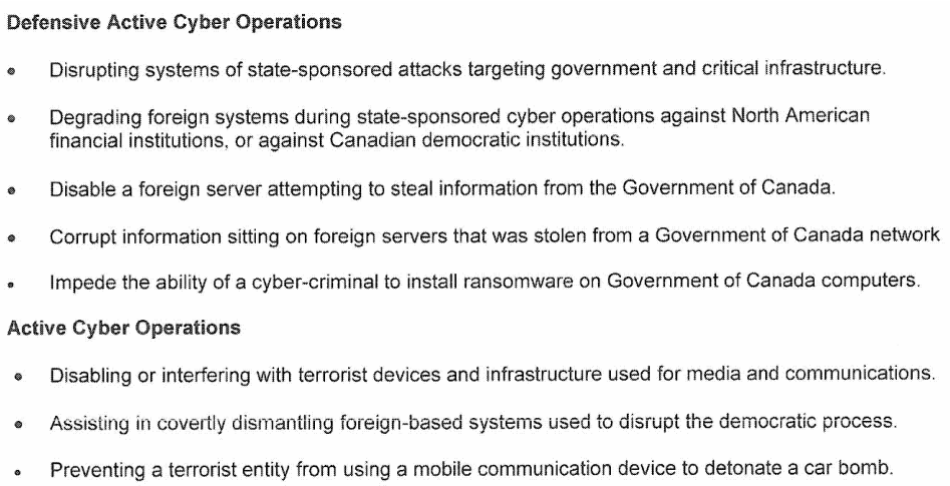
As part of the proposed legislation, the CSE would gain the ability to engage in defensive and active (or offensive) cyber operations. The defensive cyber operations aspect of the mandate would enable the CSE to carry out activities "to help protect federal institutions' electronic information and information infrastructures as well as other electronic information and information infrastructures which have been designated as being of importance to the Government of Canada." In contrast, the active cyber operations aspect of the mandate would allow the CSE to carry out activities "to degrade, disrupt, influence, respond to or interfere with the capabilities, intentions or activities of a foreign individual, state, organization or terrorist group as they relate to international affairs, defence or security."

Despite differences in purpose, in both cases, these proposed aspects of the CSE's mandate involve a more active role than what legislation has historically afforded

the Establishment. The types of activities which could be authorized under either aspect of the mandate would be the same. They may include:

- gaining access to a portion of the global information infrastructure
- installing, maintaining, copying, distributing, searching, modifying, disrupting, deleting, or intercepting anything on or through the global information Infrastructure
- doing anything that is reasonably necessary to maintain the covert nature of the activity
- carrying out any other activity that is reasonable in the circumstances and reasonably necessary in aid of any other activity, or class of activities, authorized by the authorization

The Government of Canada's briefing notes provide a series of fairly innocuous examples of contexts in which these expansive powers might be deployed. These activities are shown in Figure 2:



Defensive Active Cyber Operations

- Disrupting systems of state-sponsored attacks targeting government and critical infrastructure.
- Degrading foreign systems during state-sponsored cyber operations against North American financial institutions, or against Canadian democratic institutions.
- Disable a foreign server attempting to steal information from the Government of Canada.
- Corrupt information sitting on foreign servers that was stolen from a Government of Canada network
- Impede the ability of a cyber-criminal to install ransomware on Government of Canada computers.

Active Cyber Operations

- Disabling or interfering with terrorist devices and infrastructure used for media and communications.
- Assisting in covertly dismantling foreign-based systems used to disrupt the democratic process.
- Preventing a terrorist entity from using a mobile communication device to detonate a car bomb.

Figure 2: Defensive Active Cyber Operations and Active Cyber Operations from Government of Canada's briefing book detailing its positions on the proposed CSE Act.

If the CSE foresees the "active" and "defensive" aspects of the mandate will be used only to engage in the types of issues described in Figure 1, the new powers proposed in the CSE Act would be entirely unnecessary. The CSE already has an "assistance" aspect of its mandate under its current legislation, the *National Defence Act*. This means that CSE can **already** provide technical support to the Canadian Security Intelligence Service (CSIS) when it conducts "threat reduction" to disrupt security threats, and under C-59, the CSE will also more clearly be allowed to help Canadian Armed Forces (CAF) conduct operations abroad. Every single one of the activities

listed in Figure 1 under "defensive" and "active" cyber operations **can be done through the assistance power in support of CSIS or CAF. They do not require the CSE to gain independent "cyber operations" powers**.

So the real question we have is: why does the CSE need the ability to engage in this kind of activity *independently*, without involving CSIS or CAF? The Government of Canada has yet to provide a compelling answer to this question, and this memo does not provide any kind of illumination on the issue.

Read more about the proposed "cyber operations" powers:

- "New powers for Canadian spy agency alarming," by the Editorial Board of the *Toronto Star*
- "Sajjan defends proposed new spy powers to conduct 'information' warfare," by Alex Boutilier in the *Toronto Star*
- "Critics fear the government's national security bill puts Canadians in the crosshairs," by Stuart Thomson in the *National Post*
- "Black Mirror Canada," interview with Jesse Brown on *Canadaland*

Defensive Cyber Operations: "Disabling Foreign Servers Suspected of Stealing Information" or "Corrupting Stolen Information Stored on Foreign Servers"

The power to corrupt information on foreign servers that the CSE deems to have been stolen from a Government of Canada network is broad. It can include information that has been provided to foreign news organizations by whistleblowers, held by human rights organizations abroad, or held by whistleblowers themselves. Notably, many government agencies continue to consider documents released by former NSA contractor Edward Snowden as inappropriately taken years after the broad public dissemination of these documents.

Disabling foreign infrastructure believed to be implicated 'in the act' of stealing government information can have wide-ranging unintended consequences. Attribution challenges inherent in addressing such attacks are well documented and, frequently, what appears to be a foreign server engaged in data theft is actually a company's compromised network. If the compromised network involved in the attack is responsible for critical functionality (a power plant, a hospital), its destruction or disabling can have wide-ranging impact on foreign individuals reliant on it. Attribution can also complicate the ability to identify intruders on a network

and their reasons for intruding, let alone to gauge an appropriate and proportionate response to such intrusion. Incorrect attribution can mean a benevolent foreign security researcher must contend with a cyber assault of a magnitude intended for a foreign state actor.

This 'hacking back' approach to cybersecurity can also initiate a rapid and difficult to anticipate escalation, leading to political sanctions, and potentially inviting responses that might ultimately be viewed as acts of war. Requiring the Minister of Global Affairs' consent as is the case with offensive cyber operations (currently, the Minister must be consulted, but cannot refuse a defensive cyber operations authorization) might help mitigate these concerns, but this type of escalation has proven difficult for anyone to predict.

Finally, it should be noted that the CSE will soon be able to hack foreign servers on behalf of Canadian companies or private sector information designated as 'important' by the government, further complicating escalation challenges. Hacking back towards foreign aggressors on behalf of Canadian companies can lead to reprisals that may be crippling in their impact on the very private companies that invoked the CSE's assistance in the first place. Canadian bank customer's records can be ransomware-d, mobile networks disrupted, or confidential client information publicly exposed. In light of this anticipatable impact on the rights and legitimate expectations of Canadians, approval from the Intelligence Commissioner must be a prerequisite for defensive cyber operations if Canada is to embrace this 'wild wild west' approach to cybersecurity.

Defensive Cyber Operations: "Degrading Foreign Systems during State-Sponsored Cyber Operations against North American Financial Institutions or Against Canadian Democratic Institutions"

It is extremely challenging for even the best-placed agencies and groups to positively identify who is responsible for online attacks in after-action analysis, let alone in real time as an attack is occurring. Moreover, while the talking point refers to 'state-sponsored' operations, there is no requirement in the legislation for a response to only take place when a state actor is believed responsible: individuals, organizations, and any other groups which act detrimentally to Canada's international affairs, defence, or security can be targeted under defensive cyber operations.

It is noteworthy that while in the example provided by the CSE, they would attempt to degrade attacks against *Canadian* democratic institutions—the term, itself, undefined and thus perhaps only referring to elections Canada, or potentially extending to political parties, or even further to media organizations responsible for spreading knowledge that Canadians needs to participate in their democracy—the Establishment also proposes degrading an attack against *any* North American financial institution. This would include, presumably, institutions in both the United States of America as well as Mexico: such efforts, especially in defence of Mexican institutions, seem like a considerable extension of what Canadians may believe the CSE is authorized to do as part of its defensive operations to protect Canadian interests.

Active Cyber Operations: "Disabling or Interfering with Terrorist Devices and Infrastructure Used for Media and Communications"

The proposed *CSE Act* would let the CSE, as they suggest in their example, disable infrastructure with the dual consent of the Minister overseeing the CSE and the Minister of Foreign Affairs under the "active" cyber operations aspect of the mandate. However, active cyber operations run the serious risk of disrupting the services which are used by innocent persons. It is essential to realize that terrorists use the same infrastructure as everyday Canadians: they, like us, will use WhatsApp, Signal, PGP, and other privacy- and security-enhancing tools. As such, it is imperative that additional steps be put in place to protect Canadians from having their Charter-protected rights infringed upon, and to ensure that Canada does not violate its human rights commitments. At a minimum, this should include requiring the Intelligence Commissioner to approve all active cyber operations and for that Commissioner's decisions concerning their approval or refusal to be issued as publicly as possible to invite public scrutiny of the legal rationales for approvals or denials.

Reflections on "Active" and "Defensive" Cyber Operations Powers, Human Rights, and the Charter

The "global information infrastructure" does not in any meaningful way conform to territorial boundaries. Refraining from "directing" cyber operations activities at Canadians or people in Canada doesn't stop the CSE's activities from potentially having significant collateral impacts on their rights. In the cyber operations context, under the proposed legislation the CSE could receive authorization to disrupt and interfere with communications technologies—like messaging apps and anonymity

software—that are used globally, including by Canadians and people in Canada. Activities like mass denial of service attacks, or modifying the contents of a newspaper's website, will often inherently involve a violation of a Charter-protected right. Such rights include the freedom of expression and the corresponding right to receive and impart information. Collateral impacts on privacy rights—as a result of interference with, say, encryption and anonymity tools—may also result depending on how the CSE exercises these powers.The CSE Act doesn't meaningfully account for this impact, and doesn't provide appropriate oversight given the risks.

Canada also has international human rights obligations to respect freedom of expression, privacy, and other rights abroad — rights which may be seriously impacted by these new powers.

We would also note that the list of activities described in Figure 1 is exclusively oriented toward issues of national defense and security. However, this neglects the fact that the "active" cyber powers can also be justified on the basis of a wide range of more general international affairs reasons, including the desire to influence and manipulate economic and political outcomes abroad.

As a general note, it is important to recognize that the international norms surrounding state-sponsored hacking are in flux and far from settled. By passing Bill C-59 in its current form, Canada would be normalizing conduct that remains extremely controversial. We are not obligated to engage in reckless, unchecked, state-sponsored hacking or other kinds of problematic conduct just because authoritarian regimes do it, or for that matter just because our allies do so.

Instead, we should be moving towards international prohibitions on hacking and joint enforcement, not escalation and legitimization. We also have to think about the economic impacts — CSE acquisition of malware, spyware, and hacking tools is likely to help legitimize a market predicated on undermining and subverting, rather than strengthening, the security of the global information infrastructure. Those tools, as we know, don't stay in the hands of democratic governments, but rather also end up in the hands of authoritarian regimes and criminal organizations. The same types of technologies are also even trickling into consumer markets and are being exploited for everything from domestic violence to extortion.

Assistance: "Collecting and Processing Communications" and "Designing Technical Solutions" for Law Enforcement and Security Agencies

The "assistance" aspect of the CSE mandate does not significantly change in Bill C-59, with the exception that under the new law, the CSE would be explicitly able to support the Department of National Defence and the Canadian Armed Forces. As a result, historic problems with the mandate remain unaddressed.

The CSE must play by the rules that bind the agency it is assisting, and CSE assistance doesn't allow a law enforcement or security agency to do anything it isn't otherwise lawfully allowed to do. In our report, we raise concerns regarding the proportionality and lawfulness of these powers. The CSE's technological capabilities are designed for high-tech spycraft involving sophisticated adversaries, including nation states. Many of these tools are developed or acquired in a manner that would not have been lawful had the requesting agency (such as the RCMP) developed it themselves, and will sometimes involve the support of Five Eyes allies.

Additionally, since our report was released, research from Human Rights Watch has analyzed a practice undertaken by policing agencies and which involves 'reproducing' evidence first obtained by various intelligence agencies, including the National Security Agency (the CSE's US counterpart) and presenting it as the object of domestic policing. While the prevalence of such parallel construction practices requires further study in the Canadian context, the *CSE Act*'s permissive approach to the Establishment's assistance mandate leaves open the possibility of similar activities taking root in Canada.

Bringing these extraordinary powers to bear in the domestic law enforcement context (for example, through assistance to Royal Canadian Mounted Police or Canadian Border Services Agency) may be disproportionate in some cases. In our report, we recommend imposing certain constraints on these powers, such as preventing the CSE from providing access to the data it collects in the course of foreign intelligence or information assurance operations, and restricting the assistance to that which is developed 'in-house' by the CSE. Of course, this requires a careful balance. Allowing the CSE to lend its technical expertise to domestic law enforcement agencies is non-controversial. However, extending assistance to include the CSE's unique access to the global information infrastructure—access justified by its foreign intelligence mandate—is an entirely different proposition. To take an extreme example, highly intrusive tools designed for the national security

context are not likely to be proportionate, constitutional, or appropriate when deployed in detecting low-level drug offences or highway safety violations.

Concluding Thoughts on the Government of Canada's Briefing Notes

Some of the positions taken by the Government of Canada in the document—such as regarding limits on publicly available information—are reassuring. Unfortunately, however, there is a vast difference between how the CSE publicly describes its intended use of these powers, and ways they could be used (and abused) in the future. For a detailed analysis and critique of the proposed legislation, including over 50 recommendations, see our full report.

Unless the proposed *CSE Act* section pertaining to publicly available information is amended, our concerns remain. The same is true of the other examples raised and which we respond to, above: the government has chosen to selectively present a series of relatively innocuous examples and to highlight some of the least intrusive ways that the new powers might be used. But even these uses include the prospect of interfering with the communications tools used by Canadians every day, disrupting legitimate journalistic activities, and broadening the scope of the CSE's mass surveillance activities. Does this document change our initial findings from December 2017? Generally, no. While it provides insight into some of the ways the CSE might act following the passage of the *CSE Act*, it does not alleviate our concerns.