April 19, 2018

Private Networks, Public Importance: Reviewing the Communications Security Establishment's Private Network Cybersecurity Regime Under Bill C-59

By: Dana Hägg, Jocelyn Gerke and Marika Cherkawsky

Provision Commented On: Section 22(1) of the proposed *Communications Security Establishment Act* under Bill C-59, *An Act Respecting National Security Matters, 2017*

The proposed *Communications Security Establishment Act* (*CSE Act*), which would be enacted by Bill C-59, expands the Communications Security Establishment (CSE)'s mandate such that the CSE would be able to conduct cybersecurity and information assurance activities on private networks. Given the amount of critical infrastructure in the hands of the private sector, this is a much-needed enlargement of the CSE's powers.

This new power has been described as being entirely dependent on a request for assistance by the owner of the private information infrastructure (see Parliament, House of Commons, Standing Committee on Public Safety and National Security, *Evidence*, 42nd Parl, 1st Sess, Meeting 88 at 9:45 (Ms Greta Bossenmaier, Chief of the Communications Security Establishment)). However, this is not represented in the legislation. Under the proposed *CSE Act*, the CSE would be able to conduct a large amount of privacy-infringing cybersecurity and information assurance activity on private networks without the owner's knowledge or consent.

We recommend that the proposed *CSE Act* be amended such that the Minister may only designate information or information infrastructure under section 22(1) upon request of the owner or operator of that information or information infrastructure. This is an important step in earning the trust of the private sector. Without the trust of the private sector, the Government of Canada's cybersecurity strategy – which depends on public-private sector cooperation – will fail.

This post proceeds as follows: first, we summarize the cyber threat to private sector infrastructure and the importance of the cooperation and trust of the private sector. Second, we discuss how the existing legal framework does not provide adequate statutory powers to enable cybersecurity partnerships with private sector actors. Third, we summarize the framework proposed under Bill C-59 and highlight the issues with the drafting. Finally, we propose a minor amendment to the proposed *CSE Act*.

Critical Infrastructure Security Requires Cooperation Between the CSE and the Private Sector

What is the Cyber Threat to Private Information Infrastructure?

Cyberattacks on private information infrastructure threaten Canadian national security. Both state and non-state actors have targeted critical Canadian private sector information infrastructure such as power grids, utilities, hospitals, universities, and financial institutions (see Canadian Security Intelligence Service, *2014-2016 Public Report*). It is estimated that in a recent one-year period, 86% of large Canadian organizations have suffered a cyberattack (see Minister of Public Safety, *Canada's Cyber Security Strategy: For a Stronger and More Prosperous Canada* (Ottawa, 2010: Public Safety Canada) at 4). In particular, the advanced technology sector is targeted by intellectual property theft operations, undermining the competitive advantages of Canadian firms and threatening the integrity of the Canadian economy (see CSIS Public Report).

Attacks on private information infrastructure have the potential to cause real harm to citizens. For example, process control systems regulate almost every aspect of critical infrastructure: they keep dams from overflowing, electrical grids from collapsing, and transportation networks from malfunctioning. In December 2015, a cyberattack conducted against three Ukrainian power companies resulted in a power outage that left hundreds of thousands of people in the dark. In April 2018, a cyber-espionage attack on a shared data network forced four US natural gas pipeline operators to shut down their customer communications systems (see Clifford Kraus, Cyberattack Shows Vulnerability of Gas Pipeline Network, *New York Times* (4 April 2018)). These attacks exploited systems that are used by energy companies worldwide, including in Canada; thus, we too are vulnerable to such attacks (see Cyber Security Strategy at 12).

Private Sector Cooperation and Trust are Key

Many of the risks and impacts of cyberattacks are shared between the Government of Canada and the private sector. Cyberattacks can have cascading effects across industrial sectors and even across national borders (see Cyber Security Strategy at 12). Public Safety's 2017 *Horizontal Evaluation of Canada's Cyber Security Strategy* emphasized the critical importance of cooperating with private sector actors, as did Canada's *Cyber Security Strategy* and the *2017 Public Report on the Terrorist Threat to Canada*.

However, the recent review of Canada's cybersecurity activities revealed that private sector actors "lack trust in the public sector's ability to safeguard their information" (see Horizontal Evaluation at 20). If private sector actors do not trust the public sector, they may not cooperate with Government agencies and may not consent to CSE assistance. This would lead to a breakdown in sharing of information regarding cyber-threats and could leave critical infrastructure vulnerable to attack.

The Government Cannot Effectively Support Private Sector Actors Under Current Law

The cybersecurity mandate generally falls within the purview of the CSE and Public Safety Canada. Traditionally, the respective mandates of the organizations are focused as follows: CSE addresses issues related to "systems of importance to Canada", and Public Safety's Canadian Cyber Incident Response Centre plays a coordination role in information-sharing and incident management (see *Horizontal Evaluation* at 8). However, there remains significant confusion within the private sector and even within government regarding which organization takes the

lead on private sector cybersecurity incident response and, as we will discuss below, their respective statutes leave significant doubt that either one actually has the authority to provide active cybersecurity assistance to private information infrastructure owners (see Horizontal Evaluation at 8).

Current CSE Statutory Authority Under the National Defence Act

The CSE currently has three statutory mandates. The cybersecurity mandate is Mandate B as set out in the *National Defence Act*, RSC 1985, c N-5:

> 273.64(1) The mandate of the Communications Security Establishment is
> (a) to acquire and use information from the global information infrastructure for the purpose of providing foreign intelligence, in accordance with Government of Canada intelligence priorities;
> **(b) to provide advice, guidance and services to help ensure the protection of electronic information and of information infrastructures of importance to the Government of Canada**; and
> (c) to provide technical and operational assistance to federal law enforcement and security agencies in the performance of their lawful duties. (emphasis added)

However, foreign intelligence (Mandate A) and cybersecurity (Mandate B) activities "shall not be directed at Canadians or any person in Canada" (see *National Defence Act*, section 273.64(2)) which includes corporations incorporated in Canada or a Canadian province (see *National Defence Act*, section 273.61, "Canadian"). The Federal Court has held, albeit in a slightly different context, that an activity may *incidentally* involve a Canadian without being "directed at" a Canadian (*Canadian Security Intelligence Service, Re*, 2012 FC 1437 (CanLII) at para 106). Nonetheless, the CSE is prohibited from "directing" its cybersecurity activities at Canadian private sector actors, that is, persons or corporations that are Canadian or located in Canada.

Public Safety Canada's Statutory Role

The Minister of Public Safety and Emergency Preparedness is responsible for exercising a leadership role at the national level and the coordination of the activities of the Public Safety portfolio agencies such as the RCMP, the CSIS, and the Canadian Border Services Agency (CBSA) (but not the CSE, which currently falls within the Department of National Defence) (see *Department of Public Safety and Emergency Preparedness Act*, SC 2005, c 10, ss 4(2) and 5). Further, the Minister of Public Safety is responsible for planning and coordinating emergency management (see *Emergency Management Act*, SC 2007, c 15, s 4). Thus, Public Safety Canada's express statutory duties all concern leadership, coordination and information-sharing.

The Canadian Cyber Incident Response Centre (CCIRC) works within Public Safety Canada in partnership with stakeholders – including private sector actors – to provide advice and mitigation for cyber events, technical advice and support, and information-sharing (see Public Safety Canada, *Canadian Cyber Incident Response Centre*). This includes early detection indicators, malware analysis and forensics, and technical information on threats, vulnerabilities, risk and incidents. There is no mechanism for the sharing of sensitive information with private sector

partners, such as information regarding cyber threats or malware that are not publicly known or available. Thus, the CCIRC's technical assistance function appears to be informational, general, and public-facing, rather than individualized monitoring, testing, or research and development.

In theory, the Minister of Public Safety's powers extend to "all matters over which Parliament has jurisdiction – and that have not been assigned by law to another department, board or agency of the Government of Canada – relating to public safety and emergency preparedness" (see *Department of Public Safety and Emergency Preparedness Act*, s 4(1)). If the CSE does not have the statutory authority to provide cybersecurity assistance to private information infrastructure owners, it arguably "relate[s] to public safety and emergency preparedness" and thus would fall within the purview of the Minister of Public Safety. However, this provision must be read in the context of the whole *Act*; it is absurd to suggest that *every* conceivable national security-related power vests in the Minister. The more consistent interpretation would be that "public safety and emergency preparedness" means high-level leadership and coordination activities like those enumerated in the *Department of Public Safety and Emergency Preparedness Act* and the *Emergency Management Act*, rather than ongoing technical assistance.

The Proposed *CSE Act* Overshoots this Objective

Designation Scheme Under the Proposed CSE Act

Under section 22(1) of the proposed *CSE Act*, the Minister may, by order, designate any electronic information, any information infrastructures or any class of electronic information or information infrastructures as electronic information or information infrastructures — as the case may be — "of importance to the Government of Canada" (see Bill C-59, *An Act respecting national security matters*, 1st Sess, 49th Parl, 2017, Part 3 (Proposed *CSE Act)*, s 22(1)). Therefore, per section 6 of the Proposed *CSE Act*, the Minister responsible for the CSE (currently, the Minister of National Defence) has the power to designate any electronic information or information infrastructure as important to the government of Canada.

Once the Minister designates any electronic information or information infrastructure as being "of importance to the Government of Canada", it falls within the CSE's mandate under section 18 of the Proposed *CSE Act*, which states that:

> 18. The cybersecurity and information assurance aspect of the Establishment's mandate is to
> (a) provide advice, guidance and services to help protect
> (i) federal institutions' electronic information and information infrastructures, and
> **(ii) electronic information and information infrastructures designated under subsection 22(1) as being of importance to the Government of Canada;** and
> (b) acquire, use and analyse information from the global information infrastructure or from other sources in order to provide such advice, guidance and services. (emphasis added)

Therefore, as soon as the Minister "designates" electronic infrastructure or information infrastructure as falling in this category as important to the Government of Canada, then the CSE

has the power to "provide advice, guidance and services to help protect" this infrastructure and subsequently can "acquire, use and analyse information from the global information infrastructure" to fulfill this role (see Proposed *CSE Act*, section 18(b)). It is unclear what the wording of "acquire, use and analyse information" means, but it presumably grants the CSE power to do whatever is required with the information in order to provide advice, guidance and service to protect the designated infrastructure.

Section 23(4) provides that activities carried out by the CSE to further cybersecurity and information assurance parts of its mandate under section 18 "must not contravene any other Act of Parliament unless they are carried out under authorization issued under subsection 28(1) or (2) or 41(1)." Consequently, the above mandate of the CSE to protect the designated infrastructure is constrained by any Act of Parliament, unless the CSE obtains a cybersecurity authorization. Section 28(2) prescribes the requirements for cybersecurity authorizations pertaining to non-federal infrastructure:

> 28(2). The Minister may issue a Cybersecurity Authorization to the Establishment that authorizes it, despite any other Act of Parliament, to, in the furtherance of the cybersecurity and information assurance aspect of its mandate, access an information infrastructure designated under subsection 22(1) as an information infrastructure of importance to the Government of Canada and **acquire any information originating from, directed to, stored on or being transmitted on or through that infrastructure for the purpose of helping to protect it,** in the circumstances described in paragraph 184(2)(e) of the Criminal Code, **from mischief, unauthorized use or disruption**. (emphasis added)

Thus, this cybersecurity authorization is issued to the CSE by the Minister and allows access to an information infrastructure that the same Minister designated as "of importance to the Government of Canada" under section 22(1). Note the wide scope of the information described under section 28(2) of the Proposed *CSE Act:* "any information originating from, directed to, stored on or being transmitted on or through that infrastructure". This could conceivably cover all information that touches the designated infrastructure, whether that information is retained or simply transmitted through the infrastructure.

Under section 29(1) of the proposed *CSE Act*, the authorization provided by the Minister is valid when "the Commissioner provides the Minister with a written decision approving the authorization." This approval is under section 21(1)(a) of the proposed *Intelligence Commissioner Act* which mandates that "the Commissioner, in a written decision, (a) must approve the authorization…if he or she is satisfied that the conclusions at issue are reasonable." Section 29(2) provides greater clarity that the authorization issued by the Minister to the CSE is not authorized until valid under section 29(1). The Intelligence Commissioner is a new position established under the proposed *Intelligence Commissioner Act.* The key function of the Commissioner is to act as an independent and judicial officer responsible for reviewing certain authorizations, amendments, or determinations made by CSIS and CSE. The position is filled by a retired judge of the Superior Court.

The "Under-Inclusive Trigger"

Professor Craig Forcese, in his brief for the Standing Committee on Public Safety and National Security, described the trigger requiring the CSE to obtain a cybersecurity authorization – that is, when the CSE's activities would "contravene an Act of Parliament" – as "under-inclusive" (see Craig Forcese, *Putting the Law to Work for CSE: Bill C-59 and Reforming the CSE Foreign Intelligence Collection and Cybersecurity Process* (Brief to the Commons Standing Committee on Public Safety and National Security) (5 December 2017) at 1). Professor Forcese's brief and testimony to the SECU Committee covered in detail the constitutional concerns raised by this drafting; in brief, the "trigger" is under-inclusive because the CSE could still conduct certain activities that would engage an individual's reasonable expectation of privacy, such as the collection and retention of metadata, without judicial oversight (a cybersecurity authorization) (*Putting the Law to Work for CSE* at 3-4). This is largely because the legislative definition of "private communication" under section 183 of the *Criminal Code* excludes metadata. As such, the collection of metadata does not contravene an Act of Parliament. We agree with Professor Forcese's comments, and rather than reproduce them here, would refer to his brief for discussion of the constitutional objections to the "under-inclusive trigger."

Rather, our critique focuses on a corollary of the under-inclusive trigger: under the proposed *CSE Act*, the CSE would be able to conduct certain cybersecurity activities on private networks without a cybersecurity authorization and without the knowledge or consent of the owner of those networks, as long as those activities did not breach the under-inclusive threshold of "contravening an Act of Parliament" (see Proposed *CSE Act*, ss 23(4) and 34(3)).

What Cybersecurity Activities Could the CSE Conduct Without Consent?

Once the private information or information infrastructure is designated by the Minister as being "of importance to the Government of Canada", it falls within the cybersecurity mandate of the CSE (see Proposed *CSE Act*, s 18(1)(ii)), so it is subject to a broad range of cybersecurity activities without the consent or knowledge of the owner under s 24 of the Proposed *CSE Act*:

> 24(1)(b) **acquiring, using, analysing, retaining or disclosing infrastructure information** for the purpose of research and development, for the purpose of testing systems or conducting cybersecurity and information assurance activities on the infrastructure from which the infrastructure was acquired;
> […]
> 24(3)(a) carrying out activities on information infrastructures to **identify or isolate malicious software**, **prevent** malicious software from harming those information infrastructures or **mitigate** any harm that malicious software causes to them; and
> (b) **analysing information in order to be able to provide advice** on the integrity of supply chains and on the trustworthiness of telecommunications, equipment and services. (emphasis added)

Given the secrecy of the CSE's operations, it is difficult to surmise how these provisions will actually be used.

On the one hand, the Act is explicit that these powers exist despite the usual prohibition on directing activities towards Canadians or persons in Canada (see Proposed *CSE Act*, s 24). On the other hand, it is unclear whether these enumerated activities are still subject to the cybersecurity authorization scheme, or whether the CSE would be permitted to "contravene an Act of Parliament" without having to obtain Intelligence Commissioner authorization or consent of the owner.

The Private Sector Security Framework Does Not Work as Advertised

The procedure codified in the proposed *CSE Act* differs from the procedure proposed by representatives from the CSE before the House Committee. The Chief of the CSE testified before the Standing Committee on Public Safety and National Security that the CSE would only conduct cybersecurity activities on private infrastructure upon request by the owner:

> CSE currently deploys a number of very sophisticated tools to protect the Government of Canada's systems. With this legislation that's being proposed, one piece of it would allow CSE, upon request from a piece of infrastructure that's been designated as important to the Government of Canada, **upon the request of the infrastructure owner**, to deploy our sophisticated tools to help defend a piece of critical infrastructure that's, for example, being attacked from outside of Canada. (see Parliament, House of Commons, Standing Committee on Public Safety and National Security, *Evidence*, 42nd Parl, 1st Sess, Meeting 88 at 9:45 (Ms Greta Bossenmaier), emphasis added)

The Associate Chief of the CSE echoed this description:

> […] [The] CSE, which is currently focused on defending and blocking activities on the government infrastructure, is limited right now to providing advice and guidance only to critical infrastructure owners in a way such that the information is available to the general public. […] CSE would be able to go even further with this legislation to **helping critical infrastructure owners who request our assistance** and whom the minister has designated as eligible to receive assistance from CSE. (see Parliament, House of Commons, Standing Committee on Public Safety and National Security, *Evidence*, 42nd Parl, 1st Sess, Meeting 97 at 12:55 (Ms Shelly Bruce), emphasis added)

Even the *Charter* Statement on Bill C-59 oversells the consent requirement, and describes the proposed scheme as "authoriz[ing] the CSE to extend its cyber protection activities to include private networks of importance to the Government of Canada, with the consent of the owner or operator of the network" (see here).

Thus, the request-based characterization of the enlarged cybersecurity mandate differs from the power as codified in Bill C-59, which as drafted, empowers the CSE to conduct certain cybersecurity activities without even the knowledge or consent, much less the request, of the owner of the information or infrastructure.

Recommendations

If the CSE only intends to perform cybersecurity and information assurance activities with the consent of the owner of the infrastructure, then that should be reflected in the legislation. In light of the recent finding that private sector actors "lack trust in the public sector's ability to safeguard their information," it is critical that the CSE renew its commitment to a fully cooperative private sector cyber strategy (see Horizontal Evaluation at 20). A consent-based, transparent strategy will better serve the goal of earning the trust of private sector actors. The trust and cooperation of private sector actors are critical to staying ahead of the cyber threat and protecting Canada's critical infrastructure.

In order to bring the text of the proposed *CSE Act* in line with its stated purpose, the consent of the owner of the information or information infrastructure must also be obtained up-front, during the Ministerial designation process:

> **Section 22 of the Act should be amended by adding the following after subsection (1):**
>
> 22(1.1) The Minister may only designate electronic information, information infrastructures or a class of electronic information or information infrastructures upon written request of the owner or operator of the information infrastructure to the Establishment to carry out cybersecurity and information assurance activities.

Further, and in the alternative, we endorse Professor Forcese's recommended amendments to fix the under-inclusive trigger, which would place a reference to a "reasonable expectation of privacy" within the "trigger" sections of 23(3) and (4) (*Putting the Law to Work* at 1-2). As noted by Professor Forcese, this would mitigate the risk of court challenges and controversies that undermine public trust in the CSE, which would in turn make it difficult for private sector actors to partner with the CSE on cybersecurity "without risking reputational fall-out themselves" (at 9).

This post may be cited as: Dana Hägg, Jocelyn Gerke and Marika Cherkawsky "Private Networks, Public Importance: Reviewing the Communications Security Establishment's Private Network Cybersecurity Regime Under Bill C-59" (19 April, 2018), online: ABlawg, http://ablawg.ca/wp-content/uploads/2018/04/Blog_DH_JG_MC_Cybersecurity.pdf