Submission to the
Standing Committee on National Defence
for its study on Cybersecurity and Cyberwarfare

Prepared by the
International Civil Liberties Monitoring Group

April 6, 2023

International Civil Liberties Monitoring Group
#210-4 Florence Street, Ottawa, ON, K2P 0W7
national.coordination@iclmg.ca | http://iclmg.ca
(613) 241-5298

Note: *This submission is based on the oral remarks provided by International Civil Liberties Monitoring Group (ICLMG) national coordinator Tim McSorley to the Standing Committee on National Defence on 31 March, 2023.*

The ICLMG is a national coalition of 45 Canadian civil society organizations was established following the September 2001 terrorist attacks in the United States and the adoption of Canada's first Anti-terrorism Act later that same year. Our mandate is to defend civil liberties in Canada from the impacts of anti-terrorism laws and activities through advocacy and public education.

Given our organization mandate as a watchdog around national security, anti-terrorism and civil liberties in Canada, we have longstanding experience examining the work of the Communications Security Establishment (CSE).

The ICLMG agrees that it is vital that Canada take steps to modernize cybersecurity laws to protect the private information of Canadians and the information infrastructure on which we rely. It is also clear that as cyber-attacks increase in activity and in sophistication, that Canada must take steps to defend itself.

However, these actions must not come at the cost of accountability and transparency of government activities, including those of the CSE. In our work, we have seen how overly broad powers and extensive secrecy result in the violation of the rights of Canadians and people in Canada. These can have real-world impacts, including when the information of Canadians and people in Canada are shared internationally with the Five Eyes, as well as with other countries. In the hands of foreign jurisdictions, Canada loses control over how the information may be used, including in ways that can result in rights violations, abuse and even torture.[1]

We also disagree with the premise that the private information of non-Canadians outside of Canada is simply fair game for mass collection and retention; this approach reinforces ongoing global systems of mass surveillance and associated rights violations. This was revealed in detail by Edward Snowden,[2] and while it did lead to promises of reforms, it is unclear to what degree the CSE's activities have truly changed.

While much of these concerns are related to the CSE's signals intelligence work, they also apply to the CSE's cybersecurity and cyberwarfare activities.

For example, while the CSE may have two distinct areas within its mandate – signals intelligence

[1] See, for example, the *Report of the events relating to Maher Arar / Dennis R. O'Connor, Commissioner, Commission of Inquiry into the Actions of Canadian Officials in Relation to Maher Arar.* Online at: https://publications.gc.ca/site/eng/9.688875/publication.html

[2] https://www.cbc.ca/news/canada/cse-tracks-millions-of-downloads-daily-snowden-documents-1.2930120

International Civil Liberties Monitoring Group
#210-4 Florence Street, Ottawa, ON, K2P 0W7
national.coordination@iclmg.ca | http://iclmg.ca
(613) 241-5298

and cybersecurity and information assurance – they do not exist in a silo.

Recently, the BC Civil Liberties Association published material obtained from disclosure in their lawsuit against the federal government regarding the CSE's operations.[3] These documents reveal, for example, that under an agreement with the former Department of Foreign Affairs, information that the CSE collected during its provision of cybersecurity support to the department, including the private communications of Canadians, could be shared with its Five Eye counterparts. While this agreement dates to 2012, this concern persists under the *CSE Act*, adopted in 2019.

Specifically, the National Security and Intelligence Review Agency (NSIRA), noted in its 2021 annual report that the *CSE Act* explicitly allows for this kind of information sharing between the CSE's various mandates, including cybersecurity and foreign intelligence.[4] NSIRA raised concerns that this sharing must be narrow and on a case-by-case basis, and that the CSE should obtain legal advice on compliance with the Privacy Act. The CSE disagreed.

Why is this important? Bill C-26, currently being studied by parliament, world formalize the CSE's role in ensuring the protection of critical cyber infrastructure and would see the CSE obtain information about the security of critical infrastructure providers.[5] This means much more information will flow into the CSE, including potentially private information relating to Canadians. Without adequate safeguards in place – both in the *CSE Act* and in Bill C-26 – information collected by the CSE, included relating to Canadians, could be used in unexpected ways, and shared with unaccountable foreign partners.[6]

For more on this, I would direct committee members to an open letter[7] we co-signed raising significant concerns with C-26, as well the Citizen Lab report, *Cybersecurity Will Not Thrive in Darkness*.[8]

The CSE also has a troubling history of obfuscating the nature of its work and violating its mandate.

---

[3] https://bccla.org/2023/03/pulling-back-the-curtain-on-canadas-mass-surveillance-programs-part-two-the-cse-secret-spying-archive/
[4] https://nsira-ossnr.gc.ca/wp-content/uploads/Annual-Report-2021-PDF.pdf
[5] https://citizenlab.ca/2022/10/a-critical-analysis-of-proposed-amendments-in-bill-c-26-to-the-telecommunications-act/
[6] See https://citizenlab.ca/2022/10/a-critical-analysis-of-proposed-amendments-in-bill-c-26-to-the-telecommunications-act/ and https://iclmg.ca/groups-highlight-concerns-with-deeply-problematic-bill-c-26/
[7] https://iclmg.ca/groups-highlight-concerns-with-deeply-problematic-bill-c-26/
[8] https://citizenlab.ca/2022/10/a-critical-analysis-of-proposed-amendments-in-bill-c-26-to-the-telecommunications-act/

International Civil Liberties Monitoring Group
#210-4 Florence Street, Ottawa, ON, K2P 0W7
national.coordination@iclmg.ca | http://iclmg.ca
(613) 241-5298

For example, the CSE tracked the Wi-Fi connections of Canadians at a major airport, despite not being allowed to conduct surveillance within Canada;[9] it collected massive amounts of Internet traffic through 200 "Internet backbone" sites worldwide;[10] despite prohibitions, it regularly collected Canadians' information and received it from foreign partners;[11] and it violated Canadian law for five years by failing to minimize Canadian information shared with Five Eyes partners.[12]

The CSE also resists fully complying with review and oversight. For example, the CSE refuses to grant NSIRA full access to records the Agency needed to carry out its review function. Instead, the CSE requires NSIRA submit a request, and CSE staff provide what they say are relevant documents. This approach, NSIRA wrote in its latest annual report, "undercuts NSIRA's authority to decide whether information relates to its reviews and contributes to significant delays in the provision of information to NSIRA."[13]

The Intelligence Commissioner has also raised concerns that CSE authorizations for both foreign intelligence and cybersecurity have not included information crucial to the approval process, particularly regarding the outcomes of previous authorized activities or explanations of specific activities based on facts and not theory.[14]

Finally, NSIRA has also raised concerns that the CSE is not providing adequate information on the impact of active or defensive cyber operations, nor appropriately delineating between the two kinds of activities despite each requiring a different approval process.[15]

In conclusion, we'd like to make some general recommendations:

- That strict separations be established between the CSE's signals intelligence and cybersecurity activities, including restrictions on information sharing, both in the *CSE Act* and in Bill C-26
- That greater restrictions be placed on the collection, retention and use of both metadata and so-called "publicly available information"
- That stricter requirements be place on foreign intelligence and cybersecurity authorizations, as well as approvals of active and defensive cyber operations, to ensure

[9] https://www.cbc.ca/news/politics/csec-used-airport-wi-fi-to-track-canadian-travellers-edward-snowden-documents-1.2517881
[10] See https://www.thestar.com/news/canada/2015/04/01/canadas-spy-review-bodies-struggling-to-keep-tabs-on-agencies.html and https://iclmg.ca/issues/oversight-and-review-of-national-security-agencies/
[11] https://bccla.org/2023/03/pulling-back-the-curtain-on-canadas-mass-surveillance-programs-part-two-the-cse-secret-spying-archive/
[12] https://bccla.org/2023/03/pulling-back-the-curtain-on-canadas-mass-surveillance-programs-part-two-the-cse-secret-spying-archive/
[13] https://nsira-ossnr.gc.ca/wp-content/uploads/Annual-Report-2021-PDF.pdf
[14] https://www.canada.ca/content/dam/oic-bcr/documents/ICO-Annual%20Report-2021.pdf
[15] https://nsira-ossnr.gc.ca/wp-content/uploads/Annual-Report-2021-PDF.pdf

International Civil Liberties Monitoring Group
#210-4 Florence Street, Ottawa, ON, K2P 0W7
national.coordination@iclmg.ca | http://iclmg.ca
(613) 241-5298

the CSE's compliance with its obligations towards oversight and review bodies; this includes reporting on the impact of previous activities

- That the CSE immediately implement a system to allow NSIRA to access its records
- That a full review of the CSE's active and defensive cyber activities take place, with a particular view to compliance with international law and Canada's role in escalating the promulgation of cyberwarfare activities
- That the government review and restrict the CSE's international mass surveillance activities

International Civil Liberties Monitoring Group
#210-4 Florence Street, Ottawa, ON, K2P 0W7
national.coordination@iclmg.ca | http://iclmg.ca
(613) 241-5298