

# **How Often Is CSE Receiving Ministerial Authorization to Launch Otherwise Prohibited Cyber Attacks -**

## **And Against Whom?**

By Matt Malone and Alexander Rudolph

May 2025



# About CIPPIC and Canadian Cyber in Context

CIPPIC is Canada's first and only public interest technology law clinic. Based at the Centre for Law, Technology and Society at the University of Ottawa's Faculty of Law, our team of legal experts and law students works together to advance the public interest on critical law and technology issues including privacy, free expression, intellectual property, telecommunications policy, and data and algorithmic governance. For more information, visit our website at [www.cippic.ca](http://www.cippic.ca).

Canadian Cyber in Context is Canada's first open research publication dedicated to public awareness and research into Canadian cyber defence policy. Founded by Alexander Rudolph in 2023, Canadian Cyber in Context provides nuanced and accessible research and analysis of the intersection of Canadian public policy and cyber conflict covering topics such as federal cyber defence policy, cyber warfare/conflict, CAFCYBERCOM, procurement, and cyber security standards. For more information, visit [www.cyberincontext.ca](http://www.cyberincontext.ca).

## About the Authors

Matt Malone is a lawyer and academic specializing in the protection of secret information, especially in the context of trade secrecy, confidential information, access to information, privacy, data protection, and cybersecurity. Before joining CIPPIC, Matt practiced law in California at Morrison & Foerster and Van Dermyden Makus. He is currently an academic partner at the Investigative Journalism Foundation and an advisory board member of the BC Freedom of Information and Privacy Association.

Alexander Rudolph is a Ph.D. candidate in the Department of Political Science at Carleton University where he researches the role of doctrine and force structures in cyber conflict. He uses the sociology of hackers, information security, and open-source intelligence to research cyber conflict and Canadian cyber defence policy, specializing in the Canadian Armed Forces. Alex works as a researcher, consultant and advisor in Ottawa, Canada.



# How Often Is CSE Receiving Ministerial Authorization to Launch Otherwise Prohibited Cyber Attacks – And Against Whom?

by Matt Malone and Alexander Rudolph<sup>[1]</sup>

This policy brief examines transparency issues relating to certain activities conducted by the Communication Security Establishment (CSE), Canada's national signals intelligence agency and technical authority for cyber security and information assurance. In limited cases, CSE engages in activities that require ministerial authorization – in particular, where it operates either in contravention of Canadian or foreign law or interferes with a reasonable expectation of privacy of Canadians or persons in Canada. The brief spotlights the ministerial authorizations that enable this activity, by presenting and analyzing the findings of an information package obtained under the Access to Information Act for the ministerial authorizations issued in 2024.<sup>[2]</sup> The brief begins by providing relevant background, presenting the findings, discussing transparency challenges and opportunities, and, finally, setting out some policy recommendations.

## Relevant Background

*CSE's Mandate and Its Various Aspects.* CSE has a dual mandate as Canada's signals intelligence agency for foreign intelligence and the country's technical authority for cyber security and information assurance.<sup>[3]</sup> CSE's legislation identifies five aspects of this dual mandate:<sup>[4]</sup>

Acronym	Aspect of Mandate	Type of Activity
FI	Foreign intelligence	"[T]o acquire, covertly or otherwise, information from or through the global information infrastructure." These activities must be conducted "in accordance with the Government of Canada's intelligence priorities." <sup>[5]</sup>

CSIA	Cyber Security and Information Assurance	"[T]o provide advice, guidance and services to help protect federal institutions' electronic information and information infrastructures" and those non-federal electronic information and information infrastructures "being of importance to the Government of Canada." <sup>[6]</sup>
DCO	Defensive Cyber Operations	To conduct activities "on or through the global information infrastructure to help protect" government and non-governmental (but of government importance) information infrastructures. <sup>[7]</sup>
ACO	Active Cyber Operations	"[T]o 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." <sup>[8]</sup>
TOA	Technical and Operational Assistance	"[T]o provide technical and operational assistance to federal law enforcement and security agencies, the Canadian Forces [CAF] and the Department of National Defence [DND]." <sup>[9]</sup>

### *Guardrails on CSE's Conduct.*

CSE must follow certain guardrails. Notably, it is specifically prohibited from directing activities at Canadians or persons in Canada.<sup>[10]</sup> Likewise, it cannot infringe the *Canadian Charter of Rights and Freedoms*.<sup>[11]</sup> CSE is also constrained by other Canadian laws (and, in the case of the FI, DCO, and ACO aspects of its mandate, foreign state laws, too).<sup>[12]</sup>

### *Exceptions to These Guardrails.*

CSE may deviate from non-Charter Canadian law, foreign law, and the reasonable expectation of privacy of Canadians or persons in Canada in certain cases when it receives lawful authorization from the Minister of National Defence. Although the ministerial authorizations enabling such activity have never been made public, CSE's legislative framework specifically allows CSE to rely on such authorizations for certain activities that further the FI, CSIA, DCO, and ACO aspects of its mandate.<sup>[13]</sup>

### *Obligations When Stepping Outside of Guardrails.*

When CSE seeks to step outside of these guardrails on the basis of a ministerial authorization permitting specific activity, it must adhere to several obligations. These obligations can be broadly categorized as *ex ante* and *ex post*. Although the *ex ante* obligations vary for the different ministerial authorizations that CSE can obtain from the Minister of National Defence (depending on the particular aspect of CSE's mandate the activity seeks to further), these conditions include, among other measures, such requirements as representing the need for the authorization and the nature of the activity CSE will engage in, obtaining prior approval from the Intelligence Commissioner, and undertaking to protect privacy rights.<sup>[14]</sup>

CSE must also adhere to several *ex post* obligations when it obtains ministerial authorization in these circumstances. For example, an authorization given by the Minister of National Defence for CSE to engage in activity that furthers the FI, CSIA, DCO, or ACO aspects of its mandate but which oversteps the organization's legislative guardrails is only valid for up to one year.<sup>[15]</sup> In exceptional cases, the Minister may also issue "emergency authorizations" for up to five days for CSE to engage in activity furthering the FI and CSIA aspects of its mandate, where adherence to certain *ex ante* obligations – in particular, obtaining approval from the Intelligence Commissioner – would "defeat the purpose of issuing an authorization."<sup>[16]</sup> In the case of FI, CSIA, and emergency authorizations, the report must also be provided to the Intelligence Commissioner.

### *Obligation for an End of Authorization Report.*

Within 90 days after one of these ministerial authorizations expires, CSE's Chief must provide a written End of Authorization report to the Minister of National Defence "on the outcome of the activities carried out under the authorization."<sup>[17]</sup> The Minister must then give this report to the National Security and Intelligence Review Agency (NSIRA), which reviews activities carried out by CSE.<sup>[18]</sup> To date, these documents have not been made public.

## Ministerial Authorizations: What We Know So Far

To date, there is inconsistent information in the public domain regarding the type and scope of ministerial authorizations that have been issued since 2019. Most available information comes from CSE's annual reports. As part of this brief, the authors sought the End of Authorizations reports issued for 2024, by filing a request under the Access to Information Act (the information was heavily redacted – see Annex 1 – but the record revealed the number of various ministerial authorizations, which is not yet in the public domain). The following chart combines the findings from all of these sources to provide a breakdown of ministerial authorizations given between 2019 and 2024:

Source <sup>[19]</sup>	2019	2020	2021	2022	2023	2024*
DCOs	1	1	1	1	1	≥1
ACOs	1	1	2	3	3	≥3
FI	3	3	Fully Approved: 2  Partially Approved: 1	3	Partially Approved: 3	≥3
CSIA - Federal Institutions	1	1	1	Partially Approved: 1	1	≥1
CSIA - Non- Federal Institutions	1	0	1	2	2	Unknown

\*Based on disclosures under the *Access to Information Act* (see Annex 1).

In addition to those ministerial authorizations, this next chart provides a breakdown of activities related to furtherance of the TOA aspect of CSE's mandate. The TOA aspect enables CSE to provide technical and operational assistance to federal law enforcement and security agencies, as well as DND/CAF.<sup>[20]</sup> TOAs can only be requested by one of CSE's federal partners, after which CSE operates under the authority of the requesting partner's mandate and legal authority.

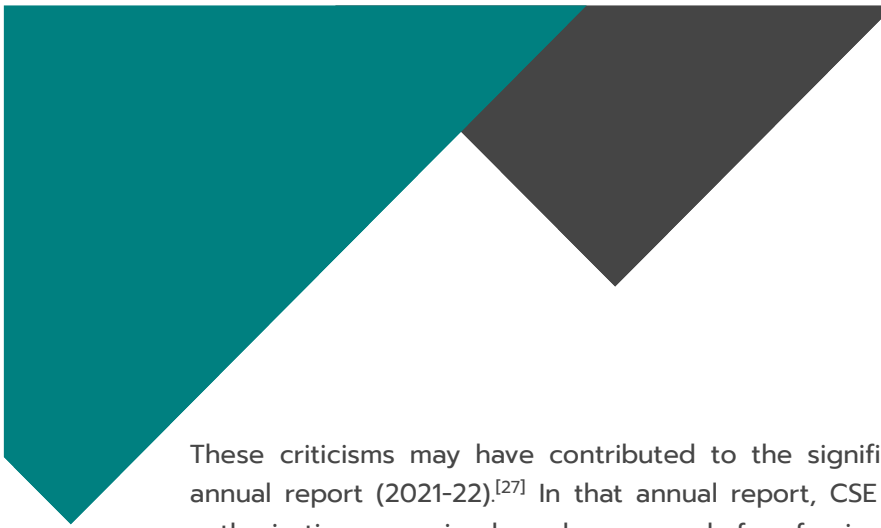
Source <sup>[21]</sup>	2019	2020	2021	2022	2023	2024*
TOA	Unknown	Received: 24 Approved: 23	Received: 35 Approved: 32	Received: 62 Approved: 59	Received: 45 Approved: 43	Unknown

\*Based on disclosures under the *Access to Information Act* (see Annex 1).

## A Note on CSE's Annual Reports

The information in the above charts for years preceding 2024 is culled from CSE's annual reports. Since the *Communications Security Establishment Act* was enacted in 2019, which provided the mandate to allow for ACOs and DCOs (collectively, "foreign cyber operations"), CSE has been mandated to release an annual report within three months after the end of each fiscal year.<sup>[22]</sup> However, the law does not stipulate exactly what the report must disclose or include; it merely states that "[t]he establishment must ... publish an annual report on its activities during that fiscal year."<sup>[23]</sup> Given the absence of specific content requirements for these reports, it is, perhaps, unsurprising that the contents of CSE's annual reports have evolved over the last six years – generally speaking, towards more disclosure.

CSE's first two annual reports (2019-20 and 2020-21) provided little information related to authorizations, other than already public information about how and when CSE could be authorized to engage in activities under its mandate.<sup>[24]</sup> This lack of transparency and reporting was not exclusive to its annual reports, but included a lack of transparency in legally mandated areas, as noted by NSIRA in its rebuke of CSE for failing to engage in required disclosure.<sup>[25]</sup> Similar criticism was also reflected in NSIRA's second review of CSE's DCO and ACOs, which noted improvements by CSE since NSIRA's initial review; however, it reiterated the need for improvements in CSE's communication and transparency with the rest of the federal government.<sup>[26]</sup>



These criticisms may have contributed to the significant increase in transparency in CSE's third annual report (2021-22).<sup>[27]</sup> In that annual report, CSE publicly disclosed the number of ministerial authorizations received and approved for foreign cyber operations for the first time. In subsequent years, CSE has steadily increased the amount of information disclosed in its annual reports, including for previous years where the number of authorizations and information about them were not previously disclosed.

Although there has been a steady increase in transparency related to the number of CSE's foreign cyber operations, little information has ever been disclosed as to their purpose or target(s). While CSE and the federal government must maintain some level of secrecy classification to ensure operational security, better communication is needed to clarify how these operations are used to protect Canada from threats. To recall, the federal government and CSE state that foreign cyber operations are used "to help protect Canada and Canadians."<sup>[28]</sup> But current disclosures do not directly specify from which threats these operations are protecting Canadians.

Despite this lack of direct connection, the federal government does, indeed, identify what cyber threats target Canada and Canadians through the Canadian Centre for Cyber Security's (CCCS) *National Cyber Threat Assessment*. However, there are opportunities to improve public communication about threats to Canada by linking CSE's annual reports of authorizations it receives with the CCCS biennial *National Cyber Threat Assessment*. So far, though, it is up to non-governmental stakeholders to create such linkages.

## Can We Link the Ministerial Authorization with Public Reporting on Canada's Cyber Threat Environment?

In the absence of explicit comment, one can infer that many of the likely threats targeted for foreign cyber operations are identified in other public materials identifying threats, such as the *National Cyber Security Assessment*. This is particularly true for FI ministerial authorizations, given that CSE is limited in this aspect of its mandate by operating "in accordance with the Government of Canada's intelligence priorities."<sup>[29]</sup> Although this obligation refers to published priorities, those remain imprecise and broadly construed.<sup>[30]</sup>

Since CCCS was created in 2018, it has published a biennial *National Cyber Threat Assessment*. These reports provide a comprehensive description and explanation of the cyber threat environment and trends facing Canada, with the intent of informing the general public. These reports leverage open source intelligence with declassified intelligence from CSE to provide a tailored, Canadian-focused threat assessment.



To take an example, the CCCS 2025-2026 *National Cyber Threat Assessment* is divided into two sections: state adversary threats and cybercrime threats.<sup>[31]</sup> Under state adversary threats, the report identifies China, Russia, Iran, North Korea, and India as potential threats. Under cybercrime threats, the report lists broad cybercrime trends and current ransomware threats, and includes a list of top ransomware threat actors such as LockBit and ALPHV. Although there is no clear indication through existing disclosures about who or what threats CSE is countering with its ministerial authorizations, one can infer that the likely targets of CSE foreign cyber operations include these actors. Although CSE and CCCS's reports broadly indicate threats to Canada and potential uses of foreign cyber operations, the federal government can better communicate its use of foreign cyber operations by directly linking the reasons for these operations with existing intelligence-backed, threat-informed public information from CSE and CCCS.

There is precedent for such transparency. For example, beginning in CSE's 2021-2022 Annual Report, the federal government began to disclose the types of criminal organizations that can and have been targeted with ACOs.<sup>[32]</sup> The primary criminal organizations targeted include terrorist organizations and ransomware groups, which is unsurprising given that many Canadian allies deploy such techniques to stop such groups from targeting civilians and governments. Although CSE has not identified which ransomware groups it has targeted, CCCS regularly releases reports and advisories related to ransomware to better inform the public on such threats.<sup>[33]</sup>

But even here, there are transparency shortcomings. Despite CSE disseminating reports to government industry stakeholders, many such reports are not released to the public; instead, they are withheld under the classification of Traffic Light Protocol (TLP): Amber. Under an "Amber Light" classification, cyber security-related documents and information are only disclosed to a limited number of stakeholders because the document may contain information that is "sensitive and carries risks to privacy, reputation, or operations." As such, "[r]ecipients may only share or discuss ['Amber Light'] information with their employees or agents who have a need to know."<sup>[34]</sup> However, it is unclear why such reports produced annually to inform public and private stakeholders are withheld from the public when there are minimal or no perceivable redactions when the document is released through a request under the *Access to Information Act*.

Although CSE and CCCS have steadily increased how the federal government communicates what cyber threats are targeting Canada, the government has not maintained a similar level of transparency in how foreign cyber operations are used to counter these threats. For example, the federal government and CSE/CCCS regularly release threat advisories and guidance related to Russian and Chinese threats, both of which have been identified in the biennial *National Cyber Threat Assessment* reports since they were first published in 2018.<sup>[35]</sup> However, CSE has disclosed much less about the manner in which these threats inform foreign cyber operations. Because foreign cyber operations authorizations can include a broad spectrum of operations, the federal government and CSE can use these regular disclosures of cyber threats to better communicate active threats against Canada.

# Oversight and Review Provide Some Public Insight

When CSE was given its mandate to conduct foreign cyber operations in the *Communications Security Establishment Act*, the Intelligence Commissioner and NSIRA were selected to serve as separate mechanisms to review or approve certain CSE authorizations. In addition to these bodies, the National Security and Intelligence Committee of Parliamentarians (NSICOP) has an important review role.

## Intelligence Commissioner.

The Intelligence Commissioner's approval is required for CSE and the Canadian Security Intelligence Service to engage in certain activities furthering different aspects of their respective mandates.<sup>[36]</sup> For CSE, the Intelligence Commissioner approves FI and CSIA activities of CSE. In past annual reports, the Commissioner has noted that ministerial authorizations for FI activities are "typically" required where CSE would breach the *Criminal Code of Canada*, in particular the provisions around interception; ministerial authorizations for CSIA activities are generally granted pertaining to "organizations and companies falling within those sectors that comprise Canada's critical infrastructure."<sup>[37]</sup> Like CSE, the Commissioner's reporting has evolved over the last six years – towards more disclosure, with the annual report from 2023 being notable in citing from its otherwise classified decisions.

The Commissioner has not fully approved all FI ministerial authorizations submitted for approval.<sup>[38]</sup>

	2019	2020	2021	2022	2023	2024
Received	3	3	3	3	3	≥3
Fully Approved	3	3	2	3	0	≥3
Partially Approved	N/A	N/A	1	N/A	3	

In particular, in 2023, the Commissioner noted that FI ministerial authorizations failed to include sufficient details required to demonstrate a commitment to operating within the class of activities permitted by the statute. The Commissioner gave a particularly strong wording about reliance on a catch-all provision in the *Communication Security Establishment Act*.<sup>[39]</sup> In that same report, the Commissioner questioned the Minister's threshold for assessing interference with the privacy interests of Canadians persons in Canada, noting the ban in the statute was absolute.<sup>[40]</sup>

The Commissioner has also not fully approved all CSIA - Federal Institution ministerial authorizations submitted for approval:<sup>[41]</sup>

	2019	2020	2021	2022	2023	2024*
Received	1	1	1	1	1	≥1
Fully Approved	1	1	1	0	1	≥1
Partially Approved	N/A	N/A	N/A	1	N/A	

The Commissioner has approved all CSIA - Non-Federal Institution ministerial authorizations submitted for approval:<sup>[42]</sup>

	2019	2020	2021	2022	2023	2024
Received	1	0	1	2	2	Unknown
Fully Approved	1	N/A	1	2	2	Unknown

The Intelligence Commissioner also receives an End of Authorization report on the outcome of the activities carried out under ministerial authorization to further the FI and CSIA aspects of its mandate (as well as emergency ministerial authorizations).

#### *NSIRA*

NSIRA is an independent, external body reporting directly to Parliament that reviews and investigates the federal government's national security and intelligence activities to ensure they are necessary and compliant with Canadian law.<sup>[43]</sup> NSIRA receives the same End of Authorization reports as the Intelligence Commissioner and End of Authorization reports for DCOs and ACOs.

## NSICOP


NSICOP has a broad mandate to review legislation and government activities related to national security and intelligence. Put differently, foreign cyber operations encompass only a small part of NSICOP's work. Even so, NSICOP has looked at Canada's overall cyber defence with a *Special Report on the Government of Canada's Framework and Activities to Defend its Systems and Networks from Cyber Attack*.<sup>[44]</sup> In 2023, NSICOP and NSIRA signed a Memorandum of Understanding to avoid duplication in their work and improve information sharing to support each other's work.<sup>[45]</sup>

These review mechanisms were established in the same overarching legislation that provided CSE with its foreign cyber operations mandate. As such, these organizations have matured in their own right at the same time CSE's own internal mechanisms for reporting about foreign cyber operations have evolved. While there have been improvements in annual reporting from the CSE's initial reports, there are areas for improvement – in particular, with respect to the way CSE and the CAF (through CAF Cyber Command (CAFCYBERCOM)) are increasingly cooperating on activities, including in activities that would normally be considered foreign cyber operations, but which are neither classified nor reported as such.

## Transparency Deficits Remain

Since CSE received its overarching legislative framework in 2019 (and even prior to that), the organization has had an uneven relationship with transparency. On the one hand, the creation of the CCCS gave CSE a more public-facing arm that routinely engages in advertising, education, guidance, and support. However, CCCS remains governed by the same legislation as CSE; and, as one can see in disclosure practices in CSE's annual reports as well as the information package obtained through the *Access to Information Act* discussed here, CSE's historical proclivity for secrecy remains embedded. With one arm pulled towards publicity while the other is struggling to determine when to stay in and step out of the shadows, the last few years have witnessed CSE wrestling with a well-known challenge of cyber resilience: striking the right balance between secrecy and publicity.<sup>[46]</sup>

CSE still needs to make progress. At present, CSE does not engage in proactive disclosure of records relating to ministerial authorizations. This lack of disclosure mirrors shortcomings in other areas, including CSE's regular invocation of time extensions when responding to records under the *Access to Information Act* – currently, the only way to obtain such records.<sup>[47]</sup> Other types of documents that could be proactively disclosed include many materials classified as "Amber Light."<sup>[48]</sup>

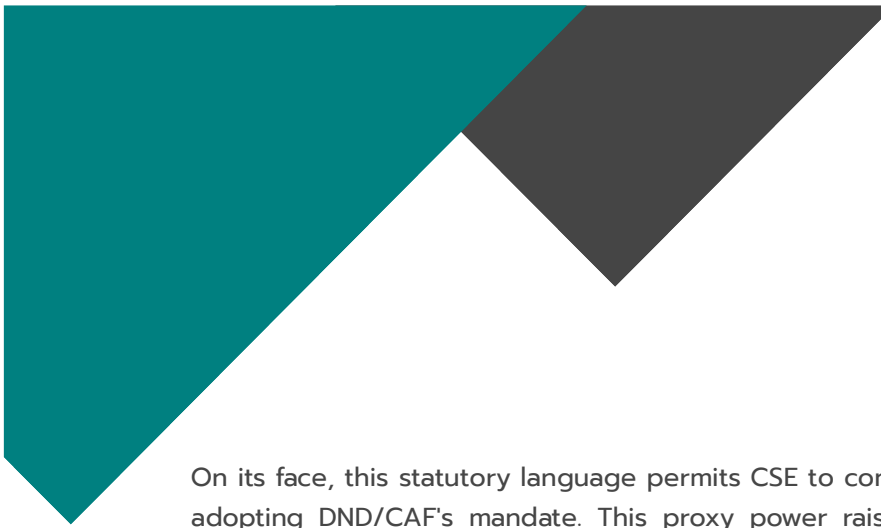


The heavily redacted records we obtained under the *Access to Information Act* present other important questions about the nature of the ministerial authorizations being granted. Although heavily redacted, the End of Authorization reports suggest that many, if not all, of these authorizations have been reinstated for years now. Based on this and existing information, at least one federal infrastructure under CSIA and one DCO authorization are likely comprehensive authorizations that are reinstated yearly to cover ongoing activities to defend federal infrastructure. ACOs are less predictable in purpose, but the ongoing authorization of ACOs and the language of reinstatement and reauthorization suggest that some CSE ACOs have been ongoing for years. As a single authorization can include multiple operations, this could suggest that there might be currently ongoing multi-faceted active operations. Unfortunately, CSE's ability to invoke sweeping national security exemptions in the *Access to Information Act* bars further insight.

Compounding these issues requires reckoning with the broader question of when and how CAF and CSE should be required to share information about the targets of their operations. As noted above, some of this information can be inferred from publicly reported information about threats. Publication of specific information, though, would help assure accountability in the conduct of CAF and CSE in carrying out their mandates (and potentially have a deterrent effect on foreign adversaries, too).

The federal government has also stretched existing norms and legal vacuums that support the withholding of information when special operations are deployed by the military to deployments of CAF/CYBERCOM and the CAF Cyber Forces. That is unlikely to change unless there is a reform in the law. This absence of a disclosure requirement when CAF conducts offensive military cyber operations leaves Canadians reliant on "soft" transparency norms to obtain disclosure about important parts of both CAF and CSE's operations – such as a recent disclosure in the Department of National Defence and Canadian Armed Forces 2022-23 Department Results noting the CAF conducted an offensive military cyber operation with CSE's support.<sup>[49]</sup>

Even if the targets of these operations are unknown, there is a pressing need to ensure that when such operations are authorized, they remain aligned with broader Canadian policy interests, particularly as the federal government deploys CSE's foreign cyber operations as national security and defence tools. This is particularly important in the context of CSE's TOA mandate, which allows the organization to have "the same authority to carry out any activity as would ... the Canadian Forces or the Department of National Defence" and to "benefit from the same exemptions, protections and immunities as would persons authorized to act on behalf of ... the Canadian Forces or the Department of National Defence."<sup>[50]</sup>



On its face, this statutory language permits CSE to conduct additional foreign cyber operations by adopting DND/CAF's mandate. This proxy power raises important questions when it comes to transparency, since the prohibitions on CSE causing "death or bodily harm" or "obstruct[ing], pervert[ing] or defeat[ing] the course of justice or democracy" apply only in the context of CSE's foreign cyber operations.<sup>[51]</sup> These prohibitions do not apply to activities carried out in furtherance of the TOA aspect of its mandate. This enables CSE to support the CAF directly in CAF cyber operations that would normally be prohibited as CSE foreign cyber operations. Such practices may require better oversight (by the Information Commissioner) and review (by the Information Commissioner and NSIRA). Although the CAF have stated the military directly handles all military cyber operations, this gap in the reporting and review mechanisms leaves Canadians and parliamentarians in the dark.

In addition, the *Communications Security Establishment Act* states that an End of Authorization report must be provided to the Minister of National Defence within 90 days of the last day of the period of validity of each foreign cyber operation authorization and that the Minister must provide a copy of this report to NSIRA. When CSE assists CAF/CYBERCOM with operations that would normally be classified as a DCO or ACO (but through the TOA aspect of its mandate), an End of Authorization report is not required. In addition, another factor that makes the reporting and transparency of military cyber operations difficult is that, under Canadian law, they are considered the same as any other military operation. These gaps in the statutory framework require further review by review bodies like NSIRA and NSICOP.

## Recommendations

Since 2019, when the *Communications Security Establishment Act* entered into force and provided the CSE its foreign cyber operations mandate, Canada's use of cyber operations as a national security and defence tool has only grown. While transparency has steadily improved, it remains inconsistent. There remain areas of improvement to make the work of oversight and review organizations easier, increase the federal government's reporting on cyber operations, and improve the public's understanding on cyber threats to Canada and how Canada is responding to them.

*First*, the federal government should develop a protocol for the eventual declassification of the End of Authorization reports for ministerial authorizations. Further, the federal government should enact specific content requirements for CSE's annual reports, which include, at a minimum, high-level information concerning ministerial authorizations. Additionally, CSE itself should increase disclosure of its reporting of materials designated "Amber Light."

*Second*, CSE should indicate, publicly and in its ministerial authorizations, that its ministerial authorizations align with its other public material on identified threats. In particular, CSE should clarify that only cyber threats identified in the *National Cyber Threat Assessment* are being targeted. This would increase transparency of authorizations, provide greater accountability over the use and exercise of these exceptional powers, and simultaneously serve as a deterrent by more explicitly showing that Canada is using foreign cyber operations to stop threats against Canada.

*Third*, mandate more comprehensive reporting by CSE to the Intelligence Commissioner and NSIRA on the activity conducted in furtherance of CSE's TOA mandate, in particular to partners such as the DND/CAF (and, in particular, in the context of military cyber operations). We also encourage NSIRA and NSICOP to review CSE's use of its TOA aspect of its mandate and how it is used to support CAF cyber operations and ways to improve transparency.

## Conclusion

When the authorizing legislation of CSE came into force on August 1, 2019,<sup>[52]</sup> there was significant promise about the potential for clear direction, strong guardrails, and better oversight and review of the organization through the establishment of this new authoritative legal framework.<sup>[53]</sup> As the findings of this policy brief show, there remain several areas for improvement, in particular in striking a better balance with transparency. The existing mechanisms for review and transparency through the Intelligence Commissioner, NSIRA, and NSICOP have contributed to improvements in guardrails, transparency, and oversight, but important gaps and areas for improvement remain.

# References

- [1] The authors thank Bill Robinson and Wesley Wark for their feedback on earlier drafts.
- [2] A-2024-00062, received from the Communications Security Establishment. Original language of request: "All reports made under section 52 of the CSE Act (timeline: 2024)."
- [3] Communications Security Establishment Act, SC 2019, c 13, s 76, s 15(1). [CSE Act].
- [4] CSE Act, s 15(2).
- [5] CSE Act, s 16.
- [6] CSE Act, s 17.
- [7] CSE Act, s 18.
- [8] CSE Act, s 19.
- [9] CSE Act, s 20.
- [10] CSE Act, s 22(1).
- [11] CSE Act, s 22(1).
- [12] CSE Act, ss 26(1), 29(1), and 30(1).
- [13] CSE Act, ss 26(1), 27(1), 27(2), 29(1), and 30(1).
- [14] CSE itself has made public a helpful – but incomplete – overview of the *ex ante* and *ex post* obligations. See Communications Security Establishment, "A Quick Guide to the CSE Act," online at: <https://www.cse-cst.gc.ca/sites/default/files/2022-03/binder-oct-2021-quick-guide-cse-act-e.pdf>.
- [15] CSE Act, s 36(1). When the ministerial authorization for such activity furthers the FI and CSIA aspects of its mandate, those authorizations may be extended one time for one year, with a requirement to notify – but not to obtain approval from – the Intelligence Commissioner. See CSE Act, ss 36(2), 36(3), and 36(4).
- [16] CSE Act, ss 40(1) and 42.
- [17] CSE Act, s 52(1).
- [18] National Security and Intelligence Review Agency Act, SC 2019, c 13, s 2, s 8. See also CSE Act, ss 52(2) and 52(3).
- [19] Communications Security Establishment, "Communications Security Establishment Annual Report, 2022-2023," pg. 44, online at: <https://www.cse-cst.gc.ca/sites/default/files/2324-0034-cse-annual-report-2022-2023-e-web.pdf>; NSICOP, "National Security and Intelligence Committee of Parliamentarians Special Report on the Government of Canada's Framework and Activities to Defend its Systems and Networks from Cyber Attack (Feb 2022)," pgs. 76-77, online at: <https://nsicop-cpsnr.ca/reports/rp-2022-02-14/2022-cyber-attack-framework-report-en.pdf>; Intelligence Commissioner, "Annual Report 2023," online at: <https://www.canada.ca/en/intelligence-commissioner/annualreport.html>.
- [20] CSE Act, s 20.
- [21] Communications Security Establishment, "Communications Security Establishment Annual Report, 2022-2023," online at: <https://www.cse-cst.gc.ca/sites/default/files/2324-0034-cse-annual-report-2022-2023-e-web.pdf>; Communications Security Establishment, "Communications Security Establishment Annual Report 2023-2024," online at: <https://www.cse-cst.gc.ca/sites/default/files/cse-annual-report-2024-v3-e.pdf>.
- [22] CSE Act, s 59.
- [23] CSE Act, s 59.
- [24] Communications Security Establishment, "Communications Security Establishment Annual Report 2019-20" (date modified: June 4, 2021), online at: <https://www.cse-cst.gc.ca/en/accountability/transparency/reports/communications-security-establishment-annual-report-2019-20> and Communications Security Establishment, "Communications Security Establishment Annual Report 2020-2021" (date modified: June 28, 2021), online at: <https://www.cse-cst.gc.ca/en/accountability/transparency/reports/communications-security-establishment-annual-report-2020-2021>.
- [25] Christopher Parsons, "Don't give more powers to CSE until it submits to effective review," Policy Options (Nov. 29, 2022), online at: <https://policyoptions.irpp.org/magazines/november-2022/communications-security-establishment-review/>.
- [26] National Security and Intelligence Review Agency, "Review of CSE's Active and Defensive Cyber Operations" (Sept. 2021), online at: [https://nsira-ossnr.gc.ca/wp-content/uploads/CSE-ACODCO-2\\_EN-55612.pdf](https://nsira-ossnr.gc.ca/wp-content/uploads/CSE-ACODCO-2_EN-55612.pdf).
- [27] Communications Security Establishment, "Communications Security Establishment: Annual Report 2021-22," online at: [https://www.cse-cst.gc.ca/sites/default/files/2022-06/cse-annual-report-2021-2022-e\\_0.pdf](https://www.cse-cst.gc.ca/sites/default/files/2022-06/cse-annual-report-2021-2022-e_0.pdf).
- [28] Communications Security Establishment, "Cyber operations" (date modified: April 6, 2023), online at: <https://www.cse-cst.gc.ca/en/mission/cyber-operations>.
- [29] CSE Act, s 16.
- [30] Government of Canada, "Canada's Intelligence Priorities - September 2024" (Sept. 19, 2024), online at: <https://www.canada.ca/en/privy-council/services/publications/canada-intelligence-priorities.html>.
- [31] Canadian Centre for Cyber Security, "National Cyber Threat Assessment," online at: <https://www.cyber.gc.ca/sites/default/files/national-cyber-threat-assessment-2025-2026-e.pdf>.
- [32] Communications Security Establishment, "Communications Security Establishment Annual Report 2020-2021" (date modified: June 28, 2021), online at: <https://www.cse-cst.gc.ca/en/accountability/transparency/reports/communications-security-establishment-annual-report-2020-2021>.
- [33] Canadian Centre for Cyber Security, "Ransomware" (dated modified Dec. 15, 2021), online at: <https://www.cyber.gc.ca/en/guidance/ransomware>.
- [34] Canada Cyber Threat Exchange, "Traffic Light Protocol (TLP)," online at: <https://cctx.ca/traffic-light-protocol/>.
- [35] Communications Security Establishment, "CSE calls on Canadian organizations and critical infrastructure providers to strengthen defences on third anniversary of Russia's invasion of Ukraine" (dated modified: Feb. 18, 2025), online at: <https://www.cyber.gc.ca/en/news-events/cse-calls-canadian-organizations-critical-infrastructure-providers-strengthen-defences-third-anniversary-russias-invasion-ukraine>; Communications Security Establishment, "Cyber threat bulletin: Cyber Centre urges Canadians to be aware of and protect against PRC cyber threat activity" (dated modified June 3, 2024), online at: <https://www.cyber.gc.ca/en/guidance/cyber-threat-bulletin-cyber-centre-urges-canadians-be-aware-and-protect-against-prc-cyber-threat-activity>.
- [36] Office of the Intelligence Commissioner, "Office of the Intelligence Commissioner" (date modified April 24, 2025), online at: <https://www.canada.ca/en/intelligence-commissioner.html>.
- [37] See e.g., Intelligence Commissioner of Canada, "Annual Report of the Intelligence Commissioner" (2019), online at: <https://www.canada.ca/en/intelligence-commissioner/annualreport.html>; see also, e.g. Intelligence Commissioner of Canada, "Annual Report of the Intelligence Commissioner" (2020), online at: <https://www.canada.ca/en/intelligence-commissioner/annualreport.html>.
- [38] Intelligence Commissioner of Canada, "Annual Report of the Intelligence Commissioner" (2024), online at: <https://www.canada.ca/en/intelligence-commissioner/annualreport.html>.
- [39] Intelligence Commissioner of Canada, "Annual Report of the Intelligence Commissioner" (2024) at 14, online at: <https://www.canada.ca/en/intelligence-commissioner/annualreport.html>. The Commissioner's remarks focused on CSE Act, s 26(2)(e).
- [40] Intelligence Commissioner of Canada, "Annual Report of the Intelligence Commissioner" (2024) at 15, online at: <https://www.canada.ca/en/intelligence-commissioner/annualreport.html>.
- [41] Intelligence Commissioner of Canada, "Annual Report of the Intelligence Commissioner" (2024), online at: <https://www.canada.ca/en/intelligence-commissioner/annualreport.html>.
- [42] Intelligence Commissioner of Canada, "Annual Report of the Intelligence Commissioner" (2024), online at: <https://www.canada.ca/en/intelligence-commissioner/annualreport.html>.
- [43] National Security and Intelligence Review Agency, "Our Mandate" (dated modified Oct. 6, 2023), online at: <https://nsira-ossnr.gc.ca/en/about-nsira/what-we-do/>.
- [44] National Security and Intelligence Committee of Parliamentarians, "National Security and Intelligence Committee of Parliamentarians Special Report on the Government of Canada's Framework and Activities to Defend its Systems and Networks from Cyber Attack" (Feb. 14, 2022), online at: <https://www.nsicop-cpsnr.ca/reports/rp-2022-02-14/intro-en.html>.
- [45] National Security and Intelligence Review Agency, "NSICOP-NSIRA Memorandum of understanding" (Jan. 10, 2024), online at: <https://nsira-ossnr.gc.ca/en/publications/secretariat-operations/nsicop-nsira-memorandum-of-understanding/>.
- [46] DND/CAF, "Pan-Domain Command & Control (PDC2) Concept Paper," online at: [https://publications.gc.ca/collections/collection\\_2025/mdn-dnd/D2-680-2024-eng.pdf](https://publications.gc.ca/collections/collection_2025/mdn-dnd/D2-680-2024-eng.pdf).
- [47] Matt Malone, "Trudeau promised radical transparency. Instead, he has exacerbated closed government," The Hub (Feb. 23, 2024), online at: <https://thehub.ca/2024/02/23/matt-malone-trudeau-promised-radical-transparency-instead-he-has-exacerbated-closed-government/>.
- [48] E.g., see A-2023-00026, received from the Communications Security Establishment. Original language of request: "All unclassified materials that went into the 'Baseline Cyber Threat Assessment: Cybercrime' released by the CCCS in August 2023 pertaining to ransomware," online at: <https://theijf.org/open-by-default/24420226>.
- [49] DND/CAF, "2022-23 Departmental Results," online at: <https://www.canada.ca/en/department-national-defence/corporate/reports-publications/departmental-results-report/2022-23-index.html>.
- [50] CSE Act, s 25.
- [51] CSE Act, s 32.
- [52] Bill C-59, 1st Sess., 42nd Parl., Assented to June 21, 2019.
- [53] Government of Canada, "Enhancing Accountability and Transparency" (July 17, 2019), online at: <https://www.canada.ca/en/services/defence/nationalsecurity/our-security-our-rights/enhancing-accountability-transparency.html>.