2018-2019 Canadian Cyber Dialogue

Summary Report #2
February 2020

We would like to extend a special thanks to the sponsor of the 2018-2019 Canadian Cyber Dialogue

With generous support from

Main organizer of the 2018-2019 Canadian Cyber Dialogue

Message from the Organizers

February 2020

Turn to any news feed and one cannot help but be struck by the rising importance of cyber security issues for Canadian security and politics. From privacy breaches to cyber espionage and disinformation campaigns, nearly every day brings news of a critical and highly concerning development. The Government of Canada has sought to address these concerns in recent years, most notably through the passage of new omnibus national security legislation and major overhauls to oversight and other agencies involved in the cybersecurity space. Yet rare are the opportunities for all stakeholders—including government, the private sector, academia, as well as civil society—to consult about the best path forward as a country.

When we launched the Canadian Cyber Dialogue in 2018, our aim was to help fill the void and create a single forum where these issues could be addressed across silos, in a comfortable setting for all concerned. The first annual Dialogue proved highly successful, with participants recommending it be continued. Based on the feedback we received, we made some adjustments to the second annual Canadian Cyber Dialogue, including narrowing the focus to discussions around the newly implemented Bill C-59 and the *CSE Act* in particular.

Whether or not a third annual Canadian Cyber Dialogue will be organized remains to be determined, but one thing is certain: we have demonstrated both a need and a desire for there to be some means

of dialogue across the various stakeholder communities. Canada faces enormous risks, but has a wealth of individuals who are committed to mitigating such risks. Events such as the Canadian Cyber Dialogue offer great opportunities to carve a path forward on cybersecurity that is a model for the rest of the world. Making sure that all parties have a way to engage will be essential to our success as a country.

Ron Deibert
Professor of Political Science, and Director of the Citizen Lab,
Munk School of Global Affairs & Public Policy,
University of Toronto

Louis Vachon
President and Chief Executive Officer,
National Bank

Contents

Executive Summary

The second annual Canadian Cyber Dialogue convened in Ottawa in December 2019, and brought together 78 participants from government, the private sector, academia, and civil society to discuss contemporary cybersecurity issues facing Canada. This year's Dialogue was organized around Bill C-59—a major update to Canadian national security legislation which became law in June 2019—and particularly the cybersecurity components found in the Communications Security Establishment (CSE) Act therein. The forum was comprised of four sessions related to the CSE Act, centred around the following topics:

1. Potential updates or amendments to C-59 that might already be necessary;
2. Questions arising from new powers to conduct cyber operations;
3. Cybersecurity issues not thoroughly addressed in C-59 (including critical infrastructure, supply chains, and encryption); and
4. Cyber foreign policy.

Additionally, a short session at the day's end discussed the value of such a forum, ways to improve and spread it, and what the Dialogue might look like in the future. The event was held under strict Chatham House rule and participants were selected to ensure an appropriate representation of subject matter experts and leaders.

A concise explanatory briefing document was prepared for each topic and circulated among participants ahead of the event to support and inform the Dialogue's high-level discussion. The briefings, which were partly created with participants' input, outlined the four

topics, examined recent Canadian developments in these areas, posed questions for discussion, and suggested readings relevant to the respective issues. These briefings may be made available upon request.

The Canadian Cyber Dialogue is Canada's only independent national cybersecurity forum and feedback indicated strong support for its multi-stakeholder format.

The following summaries briefly outline the discussions from the Cyber Dialogue's four sessions and note their respective highlights. The final section of this report provides a summary of the feedback from participants and thoughts on how to continue, alter, promote, or amend the Dialogue concept. The Munk School of Global Affairs & Public Policy invites all interested parties to contact the organizers for further information; we would be happy to share experiences and best practices to inform similar initiatives.

Session 1

C-59 is Here. Now What?

Given the focus on bill C-59, the opening session assessed and evaluated the *CSE Act*, and identified the legislation's strengths and weaknesses. Informed by a briefing document that outlined the *Act*'s most significant elements, a diverse set of experts discussed the legislation from their respective viewpoints. Broad consensus was reached that new cybersecurity tools and capabilities were much needed to deter threats, and many of C-59's omnibus updates followed demands from the Canadian private sector and practices of our democratic allies. At the same time, there was united recognition that new powers had to be accompanied by an appropriate legal framework and clear safeguards, as was intended by the creation of the Intelligence Commissioner role and the National Security Intelligence Review Agency (NSIRA); no agencies should be exempt from strong and ongoing oversight. While all agreed that C-59 constituted a watershed moment for Canadian national security, concerns were raised around privacy, transparency, necessity, data retention, and the bill's drafting process. Yet many participants, particularly from stakeholders associated with the government, military, and intelligence communities, advocated for patience to "wait and see" how the capabilities contained in C-59, and its new oversight mechanisms, function in practice. The new bill is slated to undergo a parliamentary review by 2022 to evaluate many of the same questions raised in this session.

Highlights:

> Prior to C-59, Canada's security agencies could not meaningfully mitigate cyber incidents **until after they had been committed**, according to security officials.

- Several participants stressed the importance of **public trust** in the legality of security measures. Intelligence representatives spoke of improved openness and declared that Canadians have a right to be informed of who Canadian intelligence agencies are and what they do. Intelligence officials admitted that the review process should hurt a little.

- Review and oversight agencies could further **collaborate and coordinate** with one another, similar to how intelligence agencies do.

- Some key terms and concepts in the Act are not adequately understood, such as what constitutes **"publicly available information"** or a **"reasonable expectation of privacy."** Civil society representatives stressed the importance of public discourse in informing the understandings of such concepts and intelligence representatives noted the importance to their personnel/operators of understanding such terms.

- Participants from civil society and with legal backgrounds raised concerns associated with the degree of discretion (and opacity) given to security agencies in **interpreting national security law**. In a democracy, it is important for security agencies to have a social license to operate, which requires clarity for all parties concerned.

- Participants discussed that clear legal thresholds of **necessity and proportionality** should be embedded into the new intrusive powers available to security services. Cyber operations must be reasonable given their potential foreign policy and defence implications; this is why the foreign affairs minister ought to be involved in key authorizations.

- Defence and security officials supported the CSE's new ability to **support the military's** cyber operations.

Session 2

Cyber Operations: New Powers, New Questions

This session examined how Canada can, and should, exercise its capabilities in cyberspace—and the potential challenges of doing so. Security officials noted the many steps that private sector actors can take to defend their networks. But, as military participants argued, there is a need to push the fight out of Canadian networks and into adversary space. Canada's military views cyberspace as a domain of warfare, through which adversaries might attack Canadian organizations. Thus the military must be able to engage in combat in this domain. Yet the military also sees "cyber" as just one element of warfare; it is only useful when integrated with other capabilities. C-59's new powers mean that instead of building parallel capabilities to the CSE, the military can 'borrow' these from the CSE as needed. Many questions remained unresolved, particularly on building trust with the private sector, including on Vulnerabilities Equities Processes (VEPs). Despite new risks and uncertainties, participants largely accepted that focusing solely on defending networks and remediating them post-compromise is neither adequate nor sustainable. Some ability to hit back, including preemptively, is needed.

Highlights:

> Military officials suggested that offensive capabilities are as much for **deterrent effect** as for anything; it is important that Canada's adversaries anticipate **consequences** for exercising their power through cyberspace. In September 2019, 27 countries—including Canada—signed a resolution agreeing

that they reserve the right to take action to exact consequences, implying that norms alone are inadequate.

> Industry representatives raised the need to develop greater **coordination and collaboration** within the Canadian cybersecurity ecosystem. This includes the public-private, and the federal-provincial-municipal spheres.

> **Deterrence in cyberspace** is poorly understood and discussion on how Canada should engage in 'defend-forward' classes of activities remained unresolved.

> C-59 allows for purely offensive operations—not just those in response to a threat. Such operations may conflict with **international law** insofar as C-59 does not authorize Canadian agencies to violate such law. Yet Canada has not articulated its views of how international law applies in cyberspace and what it means when/if rules are broken. Further, some stakeholders maintained that it is unclear whether the *Charter of Rights and Freedoms* applies for cyberspace conduct.

> Intelligence community representatives stressed the importance they (now) place on **public transparency**, with the CSE committing to publishing at least some of its cyber threat assessments in unclassified formats.

> There was a general agreement in favour of strong **vulnerabilities disclosure**, balanced with an understanding that some vulnerabilities may be used offensively. But Computer Emergency Response Teams (CERTs) must be trusted intermediaries; the housing of the Canadian Centre for Cyber Security (CCCS), which operates as Canada's CERT, within CSE might lead to tension with international norms against involving CERTs in malicious activity and with maintaining trust between CERTs and governments.

Session 3

Slipping Through the Cracks

This third session examined cybersecurity issues that are less prominently addressed in C-59. The discussion was broader than in other sessions and some early speakers mentioned emerging challenges from new technologies. Yet most of the discussion revolved around equities concerning critical infrastructure (CI), supply chains, and encryption. Several participants argued that C-59 inadequately addresses CI and, when it does, is vague on details; participants raised both pros and cons of such ambiguity. Private sector stakeholders noted the lack of attention paid to the supply chain that keeps businesses operational; for example, a truck firm delivering parts to a plant. Participants broadly agreed on the need to promote strong encryption and its importance as an enabler of trust, with some suggesting secure communications should not be a choice for people to make, but a default. Some stakeholders asserted that the encryption debate has become overly dogmatic, with sharp and irreconcilable differences between stakeholders. To remedy this, participants expressed a need to develop a more mature, responsible, and productive dialogue amongst all concerned.

Highlights:

> Some industry participants called for a **clearer definition of CI** in a digital context and noted that 40% of Canada's population is employed in sectors recognized under the government's current definition of CI. At the same time, the government's definition excludes important elements, such as Canadian universities and their research. Defining CI more clearly could frame

organizational responsibilities and help set expectations, including where the private sector should independently take on threats. That said, participants recognized that too much specificity might have strategic and security drawbacks.

> C-59 mentions information on **infrastructures "of importance"** to the government of Canada; the difference between infrastructure that is "critical" versus that which is "of importance" is unclear.

> Some major CI threats come not from adversaries, but from threats affecting the underlying **physical infrastructures** required by digital systems to operate. Threats associated with climate change or energy, for example, risk being overlooked if too much focus is placed on infrastructure's digital and security dimensions.

> On supply chains and particularly 5G, some participants called for increased **digital sovereignty** to ensure some part of our CI is manufactured in Canada or like-minded states. Stakeholders' opinions were mixed regarding the feasibility of relying on certification programmes and software assurance assessments.

> The government, particularly Public Safety Canada and the Canadian Centre for Cyber Security (CCCS), are developing and acquiring various **measures for assessment**, training, awareness, and assurance. They aim to do so through a whole-of-government approach. But it is unclear what these measures, as well as new CI security-focused public-private partnerships, will look like.

Session 4

Cyber Foreign Policy

The new powers enabled by C-59 affect how Canada may conduct its foreign policy agenda and this final session explored some of these effects. More broadly, discussion centred around whether Canada should have an international strategy for cyberspace and, if so, what this should look like. Participants agreed that the Internet and cyberspace must be understood in a global context, and that international action is needed to safeguard Canadian interests in democracy, human rights, and a rules-based order. Canada has been slow to engage with an international cybersecurity strategy; while Global Affairs Canada was slated to ready such a strategy in 2019, the work remains in progress and details are scarce. The room agreed that any international cyber strategy should be at least shared with the Canadian public, if not created in consultation with the public and various stakeholders. The session concluded with recognition of the importance for Canada to maintain a moral high-ground to boost legitimacy among those who support liberal democracy and human rights, trust, and thereby Canada's international position.

Highlights:

> Before developing a cyberspace strategy, the Canadian government should first **articulate what Canadian interests are** and what they mean. By defining such interests, the government can focus on what must be protected and secured and how best to do so—including how to promote these interests globally and in multilateral fora. While technology and the realities of the cybersecurity landscape change rapidly each year, fundamental Canadian values and interests do not.

> While government representatives emphasized multilateral cooperation with like-minded states, others in the room questioned how and to what extent Canada should **engage with states that do not share our interests**, including developing states and adversarial ones. It is unclear what, if anything, Canada is doing to engage with the "swing states," or countries with undecided policy positions, in order to promote democratic and human rights-based cybersecurity policy and capacity building, as a way to counter the narrative and policies of authoritarian control that are promoted by other states.

> When the Canadian Forces decided to engage in "active cyber operations" there was **no reference to foreign policy**, national security, or consequences of the militarization of cyberspace. Some military and intelligence powers might contradict Canadian diplomatic efforts.

> Canada is aligning itself with US cybersecurity approaches, including offensive capabilities and so-called "persistent engagement" approaches to deterring cyber threats. Participants raised questions as to whether or not Canada should **consider independent approaches** or approaches bearing more resemblance to those adopted by the EU, UK, or Australia. Participants also raised questions as to the role of the **private sector** in these new cybersecurity operations and asked whether Canada should adopt new rules, informed by transparency and human rights, to govern private sector partnerships.

> Canada aims to be a leader in the development and deployment of **artificial intelligence (AI)** and other emerging technologies. However, Canada has not articulated clear positions on international human rights issues related to AI, such as how Canada will support international efforts to ban lethal autonomous weapons. Participants suggested that the government should do so urgently.

> Unlike key allies, Canada has not clearly outlined how it believes that **international law** applies, or should apply, in cyberspace. Participants broadly agreed that further clarity and transparency are required.

Session 5

What's Next for the Canadian Cyber Dialogue?

This session heard suggestions on future directions, outputs, policy, and other engagements that should flow from the Canadian Cyber Dialogue process, as well as critical feedback on the Dialogue itself. Participants expressed broad satisfaction with the event, its sessions, and its format—both together at the Dialogue's closing session and also via a subsequent survey.

Responding to comments from the 2018 Cyber Dialogue, the topic of this year's event was designed to be narrower and more focused, hence the theme of the *CSE Act*. This was generally well-received, though it was agreed that topics within this theme were still too broad to be fully covered in just one day.

Feedback on Format

One shared comment for future Cyber Dialogues stressed the importance of a relaxed and informal environment designed to generate group discussion; this might involve a more circular seating arrangement.

Several participants supported the possibility of holding smaller working groups, or tabletop exercises, throughout the year. The outcomes of such meetings could then inform a full Cyber Dialogue event.

Some felt that some participants' introductory remarks were too long; it was agreed that the real value of the event was in back-and-forth dialogue among participants and the informal tête-à-tête

discussions. Moreover, questions sometimes went unanswered given time restraints.

The challenge of keeping topics relevant to all stakeholders was also raised. For example, focus on review and oversight of government may not be of substantive relevance to private sector stakeholders.

Feedback on Participants

This year's Dialogue enjoyed wide representation from various sectors, including leaders from relevant government, intelligence, and defence institutions. It was agreed that a voice from Canadian Security Intelligence Service (CSIS) was noticeably absent and that future dialogue on this topic would benefit from representatives of the Treasury Board, Intelligence Commissioner, and key justice figures.

Representatives of some of the major social media and tech firms cancelled at the last minute, or found this year's topic less relevant to them, though they expressed interest in future events.

Some attendees expressed a desire to include participants of the highest level, i.e., from ministerial or deputy-ministerial levels. Yet others felt this might make speakers nervous and stated a preference for subject-matter experts. For future events, one of the aforementioned smaller workshops might include a discussion with such decision makers, perhaps to review the Dialogue's conclusions.

Please Feel Free to Reach Out!

This year's participants found the Cyber Dialogue event to be valuable. Moving forward, it remains to be seen in what form, and to what extent, the Dialogue will continue. If your organization would like to hold a Cyber Dialogue-style event, or review our agenda and prepared material for the 2019 Cyber Dialogue, feel free to get in touch.

To get in touch with us, please write to inquiries@citizenlab.ca with the subject line ‘Canadian Cyber Dialogue.’

2018-2019

Summary
Report #2