2018-2019

Canadian Cyber Dialogue

Summary report

January 2019

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

NATIONAL BANK

Powering your ideas™

Main organizer of the 2018-2019 Canadian Cyber Dialogue

munk school
OF GLOBAL AFFAIRS & PUBLIC POLICY

UNIVERSITY OF TORONTO

Message from the Organizers

January 2019

Open any feed these days and one cannot help but be struck by the prominence of cyber security related news. Whether it is disinformation around elections, major data breaches of companies, or cyber espionage against high-value targets, there can be no doubt that cyber security has vaulted to the top of the global political agenda.

Canada is not immune to these concerns. Indeed, as an open, democratic, highly-connected, and advanced economic nation, Canada is exceptionally vulnerable to the full range of cybersecurity threats. But how well prepared as a country are we to address them?

In early 2018, the two of us first met to discuss our shared concerns around cyber security. While we come from highly different backgrounds – one of us, a CEO of a major Canadian financial institution; the other, an academic director of a Canadian digital security and human rights centre – we shared a common concern: there was no single forum to bring together all of the relevant Canadian stakeholders across government, private sector, academia, and civil society to discuss cybersecurity issues in Canada. If an "odd couple" like us could agree on the merits of such a forum, perhaps others would as well, we thought. We decided to take a shot and invest our resources and time.

This report provides a summary of the discussion held at the first annual Canadian Cyber Dialogue, convened in Ottawa on November 2018. To encourage a free-flowing and uninhibited discussion, the Dialogue was held under Chatham House rule. As a consequence, this report does not include any names of participants. Instead, we have captured the main "takeaways" of the discussion.

A survey after the event demonstrated that the Dialogue's participants agreed with us on the merits of such a forum. We are, therefore, committed to not only organizing a second annual Cyber Dialogue in 2019, but also a series of side events and workshops as well. If you are interested in joining or supporting us, please get in touch. Meanwhile, we hope this summary provides some useful insights on the state of thinking about cyber security among a cross section of Canadian stakeholders.

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

Louis Vachon
President and Chief Executive Officer, National Bank

Contents

Executive Summary

The first annual Canadian Cyber Dialogue convened in Ottawa in November 2018, bringing together 71 participants from government, the private sector, civil society, and academia to discuss pressing cybersecurity issues facing this country. Under Chatham House rules, the forum addressed preparedness; private sector-government coordination; cybersecurity foreign policy; and disinformation, fake news, and violent extremism. Possible topics and format for the next Cyber Dialogue and mid-year working groups were also discussed. Several overarching themes and issues emerged during these conversations that call for ongoing action from cybersecurity stakeholders in Canada.

Themes

Build trust among stakeholders

Trust is key to effective collaboration on information sharing, developing best practices, and incident response. Trust can be built through routine cooperation (e.g., cyber simulation exercises) so that Canada's network of cybersecurity stakeholders is robust and ready for crisis.

Develop a coherent Canadian foreign policy for cyberspace

Canada needs a coherent and clearly articulated cyber foreign policy tied to core values. Liberal democratic values and human rights should be the defining features of our foreign policy if we claim that they define us as a country. Support to universities for research into a "made-in-Canada" approach could help support this goal.

Protect human rights and empower civil society watchdogs

Activities undertaken in the name of securing cyberspace implicate basic human rights, such as freedom of expression and association. Civil society provides a crucial independent accountability mechanism. Yet, these groups are often under resourced and not included in inter-organizational discussions concerning cyber security, nor part of institutional decision-making bodies.

Work with all levels of government, and small and medium-sized enterprises

Cybersecurity expertise and collaboration is most robust at the federal level and among many of the country's largest corporations. Yet, many key public services and a large portion of the economy rely on other levels of government and sizes of businesses; these stakeholders must be accounted for in a comprehensive cybersecurity policy process.

Define the role of the Canadian Centre for Cyber Security

It is an encouraging development that the Government of Canada has established the Canadian Centre for Cyber Security. At present, however, there is confusion over how it will operate, what will be its mandate, and what coordination mechanisms will be employed to connect the Centre to outside stakeholders. The Centre should clearly define and communicate its role, and address concerns that its connection to intelligence agencies will act as a barrier to trust among some stakeholders.

Engage the public

The Canadian public should be seen as an important stakeholder in cyber security. How can we better engage the public through digital literacy education, conduct meaningful debates on key issues in comprehensible terms, and place the public at the centre of a cybersecurity policy?

Panel 1

Canada's Cybersecurity Situation: Ready for Crisis?

The aim of this panel was to assess Canada's overall approach to, and preparedness for, cybersecurity crises. Preparedness is a multifaceted problem that requires stakeholders to consider their own needs and to collaborate on collective challenges. The military continues to focus on building its internal IT capacity and has begun to undertake detailed planning for crisis scenarios. Electoral authorities have identified the Internet as a threat vector for electoral infrastructure, electoral participants, and for public discourse surrounding elections. Elections Canada has made some progress in coordinating with government agencies such as the Communications Security Establishment (CSE) to prepare for upcoming elections, but substantial challenges remain — especially regarding the preparedness of smaller jurisdictions and political parties. Civil society groups approach preparedness with an eye to prevention: questioning the necessity of mass data stores that present a target to adversaries or abuse from government. Private enterprise continues to build its capacity for incident response but lacks clarity on its role in a national approach to preparedness and coordinated crisis response.

Highlights:

> The role that the Canadian Centre for Cyber Security would play in the event of a crisis was not clearly understood. Should corporations contact the Centre for assistance with incident response? What role would the Centre play in coordinating the response to large-scale crises?

> Civil society groups feel themselves to be 'on the outside looking in,' partly because their approach to many key issues diverges sharply from the government and industry consensus. They advocate for data minimization to reduce potential targets as opposed to thinking about how to use "big data."

> The threats to privacy and other rights in the realm of preparedness can be understood as having two parts: What harms may bad actors cause? And what harms may good actors cause as they work to prevent harms from bad actors?

> Trusted links between institutions are key to preparedness because they facilitate rapid and coordinated responses when crises arise. The public should also be considered in this paradigm. Failure to set public expectations about threats may result in disproportionate or counterproductive public responses in the event of a crisis.

> What is the role of "active cyber measures" or cyber offense in support of defensive missions as envisioned in Bill C-59? What are the risks or consequences of such a posture? How does this fit in with Canada's broader international standing?

Panel 2

Government and Industry: Working in Silos or as Partners?

Trust was a key theme in the discussion during this panel, which addressed long-standing issues around sharing information between the government and private sector, and considered the privacy concerns associated with sharing protocols. There has been progress in building trust amongst corporations and between the private sector and the government to facilitate increasingly meaningful information sharing. The creation of information sharing structures, such as the Canadian Cyber Threat Exchange, was noted by many as a positive development. Engaging different sizes of enterprises and levels of government — and ensuring that information is shared in a useful form, rather than being shared in bulk to defer liabilities associated with a lack of sharing — remain as challenges in the private sector-government realm. More serious problems exist regarding civil society engagement. Specifically, civil society stakeholders are not included in sharing structures and often lack the access and technical expertise to provide a watchdog function.

Highlights:

> ‘Information sharing’ should be defined to extend beyond reporting on particular breaches and threats to include collaboration on preparation and developing best practices. Sharing must be a meaningful engagement rather than serving as a checkbox activity.

> Excessive data sharing can compromise the usefulness of the data, especially for smaller partners who lack the capacity to parse it. Lack of trust can lead parties to withhold their most important data.

> Juxtapose the situation in Canada to that in China, where there is little distinction between public and private, where state authorities have limitless access to information, and where checks — such as civil society — largely do not exist. How do we compete with such an adversary while holding true to Canadian values?

> There is an established process for sharing information about vulnerabilities between the Communications Security Establishment (CSE) and major private enterprises. The CSE has recently started to disclose some vulnerabilities to software vendors. Serious concerns were raised about the lack of transparency and oversight in how these decision are made, despite reassurances that there is a rigorous process within the government.

> Civil society groups argue that sharing should be assessed based on balancing the benefits to the public and the potential harms to rights. Sometimes sharing is minimally intrusive and has profound public benefits. At other times, sharing is too intrusive and not justified by the benefits. There should be a public debate around these issues in comprehensible terms.

Panel 3

Canada's Foreign Cybersecurity Policy

"Does Canada have a foreign policy on cyberspace?" This question was the subject of robust disagreement during this panel, which focused on the state of law and policy on Canadian cybersecurity interest beyond our national borders. Government representatives argued that Canada's policy has been clearly articulated in speeches and statements, and that it includes strong support for human rights. Others, notably from academia, pointed to the lack of a policy document and questioned the extent and consistency of the government's concern for human rights. There were calls for greater public debate on how to defend and project Canadian values in cyberspace. The role of Canadian values in foreign policy was also central to a discussion of whether these values create an inherent disadvantage in cyber security for liberal states vis-a-vis authoritarian rivals who have more central control and fewer internal constraints.

Highlights:

> There is an emerging norm among states that international law applies to cyber activities, but how this functions in practice remains largely unclear. Many cyber operations currently occur in the "grey zone" of potentially hostile acts—the severity of which fall short of armed conflict.

> Criticism was directed particularly at the Government of Canada's response to the activities of Canadian companies abroad that raise human rights and corporate social responsibility questions (e.g., the export to authoritarian regimes of Netsweeper's Internet filtering technology). Some argued that the government has neither been vocal enough on these issues nor taken meaningful action.

> Some major corporations have been active in advancing a values-driven approach to cyber policy through initiatives such as the Digital Geneva Convention. These steps were generally welcomed, but questions were raised about whether their implementation would be effective and would lead to real change in the normative landscape.

> The current international context makes it very challenging to build international consensus and to reach meaningful agreements on cyber policy issues. Liberal democratic norms and structures are perceived to be under pressure, or even collapsing. Canada has been an advocate for the rules-based global order, but has perhaps been less vocal on cyber as compared to other issues.

Panel 4

Disinformation, Fake News, and Violent Extremism

This panel considered how stakeholders like the government, private sector, technical communities, and civil society can collaborate to counter violent extremist content and disinformation campaigns online. While disinformation is nothing new, the complexity and novelty of online campaigns raise challenges that Canada has only begun to confront. The government has pushed for, and received, a G20 commitment to create a multilateral response mechanism for disinformation; this mechanism is being developed. However, the corporations that own major social media platforms remain the front line of combatting disinformation and extremist content. While platforms have devoted more resources to these efforts, questions were raised about the timeliness and adequacy of companies' response. Both government and private sector efforts to counter disinformation also implicate the right to free expression and, thus, raise concerns about the transparency and oversight of decision-making processes.

Highlights:

> Questions raised include: Is disinformation an impossible problem to solve when the current business model of social platforms rewards the most engaging content, even when that content is false? Are platforms such as YouTube, Facebook, and Twitter not merely the venue where disinformation spreads, but one of the key causes of its proliferation?

> Disinformation has become a major focus of inquiry in academia, civil society, and government, but this body of research is not yet mature. There is no commonly-accepted definition of disinformation, nor is there rigorous evidence as to which means of combating disinformation are most effective.

> Disinformation is expected to get worse with the increasing sophistication of so-called “deep fakes.” Participants anticipated that artificial intelligence will create bots that are much harder to detect. Image, video, and audio editing technology may advance faster than techniques for detecting fakes.

> What is the role of the citizens in combatting disinformation? Governments and corporations often seem to regard users as passive participants whose only role is to be protected. There were calls for more public education and engagement.

Panel 5

Next Steps for the Canadian Cyber Dialogue

This panel engaged participants in a discussion about the 2019 Canadian Cyber Dialogue, including possible invitees, topics, logistics, and format changes. A consensus emerged that having a forum focused on Canada was useful, especially since venues for international discussion already exist. Participants brought forward many suggestions on how to broaden and deepen the dialogue on Canadian issues, both in person and through a feedback survey that was circulated after the conference. These suggestions mentioned other stakeholders who could be included and new topics that could be addressed. It was also suggested to organize working groups on subjects of particular interest throughout the year, which would report back at the annual Dialogue. Based on participants' comments, the next Dialogue will endeavour to move on from discussions of broad issues to frame more specific problems and focus on actionable outcomes. The format will be adjusted to further encourage ongoing participation from all attendees. It was agreed that the second annual Dialogue should be held in Ottawa.

Suggested future working groups and discussion topics:

> Supply chain: security and resilience
> Critical infrastructure: preparedness and modernization
> Updating arms controls for the digital age
> Regulating dual-use technologies
> Deterrence: forestalling influence operations and disinformation
> Engaging the public in cyber dialogues: education, communication, and digital literacy

Suggested future participants:

> Canadian Centre for Cyber Security
> Communications Security Establishment
> Increased participation from telecom companies
> Increased participation from judiciary and law firms
> Small and medium sized enterprises and trade associations
> Municipal and provincial governments

If you or your organization is interested in becoming a partner for the 2019 Canadian Cyber Dialogue, please reach out to us at r.deibert@utoronto.ca