



SPECIAL REPORT

Waterloo Security Dialogue Fostering Nationwide Cybersecurity Collaboration

Shelly Bruce, John Bruce,
Aaron Shull and Kailee Hilt

About the Authors

Shelly Bruce is a CIGI distinguished fellow and the former chief (deputy minister) of the Communications Security Establishment. She was appointed chief in June 2018 and retired in September 2022, 33 years after she began her career in Canada's cryptologic agency. Shelly is a visiting professor at the University of Ottawa on cybersecurity issues.

John Bruce is a CIGI senior fellow and a cybersecurity expert. Prior to his retirement in September 2022, John was the general counsel for a cybersecurity firm in Ottawa. He spent more than two decades with the Canadian Department of Justice and now teaches graduate courses in cybersecurity and cyber operations law and policy at Carleton University's Norman Paterson School of International Affairs and at the University of Ottawa.

Aaron Shull is the managing director and general counsel at CIGI. He is a senior legal executive and is recognized as a leading expert on complex issues at the intersection of public policy, emerging technology, cybersecurity, privacy and data protection.

Kailee Hilt is a program manager and research associate at CIGI. She focuses on public policy issues tied to emerging technology, privacy and cybersecurity.

Copyright © 2023 by the Centre for International Governance Innovation

The opinions expressed in this publication are those of the authors and do not necessarily reflect the views of the Centre for International Governance Innovation or its Board of Directors.

For publications enquiries, please contact publications@cigionline.org.



This work is licensed under a Creative Commons Attribution — Non-commercial — No Derivatives License. To view this license, visit (www.creativecommons.org/licenses/by-nc-nd/3.0/). For re-use or distribution, please include this copyright notice.

Centre for International Governance Innovation and CIGI are registered trademarks.

67 Erb Street West
Waterloo, ON, Canada N2L 6C2

www.cigionline.org



Table of Contents

3	Context
4	Main Takeaways
10	Conclusion
11	Next Steps



Group photo at the Waterloo Security Dialogue conference hosted by CIGI in June 2023.

Context

On June 27 and 28, 2023, the Centre for International Governance Innovation (CIGI) hosted the Waterloo Security Dialogue (WSD). The conference brought together leaders and experts to establish connections across jurisdictions with the objective of improving cybersecurity information sharing and incident response in ways that will contribute to a stronger national culture of cybersecurity resilience. Technical experts, practitioners, and senior decision makers from federal and provincial governments, Indigenous groups, municipalities and the private sector participated in discussions to confront pressing cybersecurity challenges and inspire innovative solutions and new ways to collaborate for improved cyber resilience.


The conference revolved around three key themes: cyberthreat information sharing; cyber incident collaboration and coordination practices; and initiatives to enhance cyber resilience in Canada. These themes were explored through engaging panel discussions, keynote presentations and interactive sessions.

The discussions highlighted the role of cyberthreat information sharing in strengthening Canada's incident response capabilities and effectively countering ever-emerging threats targeting the national ecosystem. Participants also shared valuable insights on managing cyber incidents, addressing coordination challenges, managing legal risks, and fulfilling workforce requirements between the public and private sectors. These discussions laid the foundation for constructive dialogue, new connections and novel ideas.

Prior to the conference, a select group of participants engaged in a stimulating tabletop exercise that explored a plausible

cyber incident threatening the operation of power distribution companies (one municipal and one territorial). This interactive scenario allowed participants to investigate the challenges of cyberthreat information sharing across sectors and harness the power of collaboration during cyber incident responses. The insights gained from this exercise informed and enriched subsequent conversations throughout the event.

This report presents key takeaways from the conference discussions held under the CIGI Rule.¹ It is important to note that this report does not aim to present a unanimous consensus among participants or reflect the views of any specific individual or organization. Rather, its primary objective is to lay out key challenges and ideas identified by participants — these will be explored further through CIGI-led workshops and subsequent WSDs.



The conference revolved around three key themes: cyberthreat information sharing; cyber incident collaboration and coordination practices; and initiatives to enhance cyber resilience in Canada.

¹ The CIGI Rule is a variation of the Chatham House Rule. When a meeting is held under the CIGI Rule, participants are free to use the information received and the identity and affiliation of participants may be revealed, but no views expressed, or other information received, may be attributed to any participant.

Main Takeaways

The realm of cybersecurity² is expansive, with a multitude of topics and themes being deliberated across different fora. This dialogue was designed specifically to explore practical issues related to how cyberthreat information is shared in Canada, and how cyber incidents are managed in Canada.

Key takeaways from the conference discussions included the following:

- Participants expressed the importance and urgency of an inclusive, whole-of-nation approach to cybersecurity.
- The various jurisdictions represented reflected the wide spectrum of Canada's cybersecurity partnerships.
- There is a drive to build on good, current initiatives and create clear, practical and national frameworks, especially for information sharing.
- There is an imperative for unprecedented levels of and renewed leadership in public-private partnering.

Conference participants discussed constructive initiatives that could serve as strong cornerstones for Canada's evolving national approach to cyber resilience:

- Well-defended federal systems form the foundation of security best practices for Government of Canada online services and information holdings, and effective management of federal cybersecurity events are informing the development of a national cyber incident response plan.
- Declassified cyberthreat intelligence, along with targeted alerts and advisories, are routinely shared with relevant audiences and the broader public.
- When discovered, compromised organizations are directly notified by the national Cyber Security Incident Response Team.
- Federal experts and tools have been deployed to assist in managing serious cybersecurity incidents in important Canadian systems.
- Canadian law enforcement and security mandates have been successfully used to dismantle cybercrime infrastructure and tools.
- Critical infrastructure leaders, such as telecommunications, have worked to set cybersecurity best practices and commit to continuous improvement in their sectors.

² Cybersecurity is defined as the "prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation" (see <https://csrc.nist.gov/glossary/term/cybersecurity>).

- Private sector-sponsored training initiatives and other post-secondary education programs have helped generate new cybersecurity talent in Canada.
- Cybersecurity awareness campaigns have been gaining more traction among Canadians.

These are just a few instances showcasing Canada's current leadership and innovation in cybersecurity. However, those involved acknowledged during conference discussions the ongoing challenges posed by the constantly evolving technology and threat landscape, as well as constraints related to policy, capacity and resources.

Building on several existing areas of strength, the WSD concentrated its efforts on enhancing inter-jurisdictional information sharing and incident response, aiming to establish a foundation for long-term national cyber resilience.

The group discussions emphasized six themes that warrant further exploration to establish favourable conditions for the future.

This dialogue was designed specifically to explore practical issues related to how cyberthreat information is shared in Canada, and how cyber incidents are managed in Canada.

Continuous, Inclusive Engagement on a National Scale

Participants engaged with federal leads for an update on the Canadian government's cybersecurity efforts related to the conference themes, specifically in sharing advice, guidance, threat assessments, alerts and victim notifications, as well as the types of assistance available during incident response. They also heard about federal mandates leveraged to reduce foreign cyberthreats before they strike Canadian victims.


It is encouraging that the many departments and agencies that are implicated in the federal cybersecurity agenda are working together; however, outside of government circles, there is low visibility of these efforts and confusion surrounding the various roles and responsibilities. Many Canadian victims remain uncertain about whether and how to engage the appropriate federal authority when experiencing a serious cyber incident.

In the end, many participants expressed their preference for a designated federal central point of contact. They favoured regular and focused national dialogue and co-development of national cybersecurity strategies and plans and clear explanations about roles and responsibilities. Participants pointed to a requirement for more priority attention to public dialogue on these and other cybersecurity issues, specifically at the national level and involving senior officials.

Unprecedented, Radical and Innovative Public-Private Teaming

Conference participants underscored the unique cybersecurity considerations they each face in delivering their services, information and products to the citizens in their jurisdictions. The phrase “only as strong as our weakest link” was frequently used to emphasize the importance of collaboration across all sectors.

In this vein, participants acknowledged that larger public and private sector organizations — such as governments and major critical infrastructure providers — are more likely to have mature cybersecurity programs to protect the citizen-facing functions they deliver on a national scale. Smaller entities — such as municipalities, Indigenous groups and remote territorial infrastructure operators — are often less resourced for the cybersecurity challenges they face. Heightening their resource constraints is the direct, daily and disproportionate impact they have on the lives of everyone within their jurisdictions (for example, in areas related to citizen information and basic utilities).



The phrase “only as strong as our weakest link” was frequently used to emphasize the importance of collaboration across all sectors.

In response, WSD participants reflected on current examples and reinforced the need for more routine and innovative teaming among public and private sector partners. Under the leadership of those with

more cybersecurity maturity and experience, smaller organizations can be mentored toward improved cybersecurity; innovative solutions can be shared among the community; and economies of scale can be arranged by championing local or regional cooperation to address common needs (for example, co-managed secure cloud tenancies for a collective of municipalities). While there are important examples of this leadership in place today, there is room to enhance, showcase and institutionalize these lead roles.

This kind of radical teaming, however, requires continuous and highly inclusive engagement with all “team Canada” practitioners, policy makers and decision makers as a group to understand the emerging challenges and new opportunities. Ultimately, a strong culture of public-private partnership can multiply the capacity for problem solving, forensic analysis and co-innovation for future demands, and expand the underlying network for national information exchange and assistance in response and recovery.

National Framework to Optimize Sharing of Cybersecurity Information

Some of the most focused discussions revolved around the necessity of establishing unambiguous expectations for the exchange of cybersecurity information, with a particular emphasis on eliminating existing real or perceived barriers as interpreted within the context of regulations such as the Privacy Act, the Personal Information Protection and Electronic Documents Act, or non-disclosure agreements, among others.

There was a strong desire to create a national information sharing framework with express statutory authority to guide organizations and explicitly permit sharing without penalizing those who share.

At the same time, there was an emphasis on designing appropriate protections for information sharing through constructive approaches (for example, automated tools to anonymize privacy information, more permissive sharing provisions in non-disclosure agreements and prescribing “safe haven” entities as custodians of data).

Federal officials took time to address perceptions that relevant cyberthreat details from classified reporting were not being sufficiently shared with those who needed the information to protect vital systems. Canadian and US security and intelligence officials explained that, while sensitive sources, methods and techniques used to gather classified intelligence may require ongoing protections, unprecedented volumes of cyberthreat intelligence, technical indicators, anticipated threat vectors and other relevant details are routinely extracted from classified intelligence and shared, both through dedicated channels to targeted Canadian and allied entities, as well as publicly, when appropriate. Whether the balance is being struck to fully empower network defenders will be explored further in future CIGI-led workshops and subsequent WSDs.

National Framework to Optimize Cyber Incident Management and Recovery

Improvements in sharing threat intelligence and applying cybersecurity best practices will offset cyber risk, but not eliminate it entirely. It is critical for Canadian entities experiencing serious cyber compromises to know — in advance of any compromise — precisely how, when and where to report the incident and be confident that the recipients of this information are capable and prepared to assist them in responding to and recovering from the breach.

It is certain that sufficient resourcing and skills for cybersecurity and incident response will remain challenging. More coordinated formal and informal teaming among public and private sector incident response experts, including police in different jurisdictions, could increase the national capacity for forensic analysis, provide additional victim support for response and recovery, and increase transparency and information sharing. As time passes and experience and trust grow, this type of collaboration has the potential to encourage more victims to willingly report the incidents they encounter.



It is certain that sufficient resourcing and skills for cybersecurity and incident response will remain challenging.

Clear Expectations, Incentives for Implementing Cybersecurity Best Practices

While many organizations follow the guidance in the US National Institute of Standards and Technology cybersecurity framework, some called for directed baseline standards suitable for specific jurisdictions, such as municipalities or small and medium-sized organizations.

Others felt there was promise in legislative change, such as the recently tabled Bill C-26, the Critical Cyber Systems Protection Act, and were eager for the framework to be extended to other sectors — within both federal and provincial jurisdictions. This would allow regulatory frameworks to be synchronized across jurisdictions and achieve some efficiencies, where possible.

Other legislative proposals could include positive requirements for technology vendors to apply “secure-by-design” principles or risk penalties. Legislation and regulations could require vendors to include a software bill of materials as an inventory of the software modules nested within their offerings and giving network defenders a better view of inherent system vulnerabilities.

Participants considered how small and medium-sized organizations and businesses could benefit from incentives — financial or other — to implement best cybersecurity practices. Similar incentives and recognition could be extended to encourage larger, more experienced organizations to demonstrate their leadership by actively, constructively mentoring less mature organizations to become cyber safe.

Ensure a Dependable Pipeline of Cybersecurity Skills and Foster Adherence to Fundamental Cybersecurity Practices by the Canadian Population

WSD participants acknowledged the overwhelming, unmet demand for traditional cybersecurity skills in Canada and the impact this is having on their operations. They also stressed the pressing need for

cybersecurity education in all Canadian jobs and disciplines, and — given the overwhelming adoption rate of the internet in Canada — to raise the cybersecurity quotient among Canadians more generally.

This presents a challenge that demands the consensus of various stakeholder groups spanning the nation. A national strategy is required that is capable of accommodating the diverse education needs of audiences ranging from elementary and high-school students to senior citizens while expanding existing academic and graduate programs on a nationwide scale. This strategy should establish more sustainable skill pipelines characterized by greater diversity to meet the escalating demand for cybersecurity talent while addressing the specific needs of cyber victims and vulnerable groups. Each aspect of this education and awareness needs to be accessible and easily understood — for practitioners and the public, and available in English, French, Indigenous and other languages, as appropriate.



WSD participants acknowledged the overwhelming, unmet demand for traditional cybersecurity skills in Canada and the impact this is having on their operations.



Conclusion

Cybersecurity has emerged as a global concern, with many countries in pursuit of strategies to protect their technology, systems and data, while safeguarding their economies and upholding the established expectations of their citizens. These expectations include a secure and predictable online environment, characterized by dependable access to vital information and services. There are many lessons and best practices that can be shared, as well as multilateral efforts dedicated to creating international cybersecurity policy and standards.

While Canada examines the approaches taken by others, care must be taken to evolve a made-for-Canada cybersecurity framework that factors in specific Canadian characteristics, strengths and concerns, such as:

- a multi-jurisdictional government structure built on a constitutionally mandated division of powers;
- a shared citizen tax base that relies on funding transfers to support citizen-facing programs and services;
- declining trust in government, and its ability to tackle tough problems alone;
- critical infrastructure that is predominantly private sector-owned and is physically distributed across a vast, but modestly populated, country;
- regional differences in culture, demographics, languages, as well as the availability of basic services and rates of digital access and adoption;

- progressive immigration policies and a national understanding of the value of multicultural perspectives;
- relatively strong international rankings in relevant indicators (for example, in technology adoption, STEM [science, technology, engineering and mathematics], media independence, digital literacy) but low-density population and market for research, innovation and solutions;
- respect for right-sized regulatory frameworks for economic security and setting expectations for both industry and consumers; and
- being a vocal defender of the rules-based international order and a safe, stable, inclusive, predictable cyberspace.

A Canadian approach can incorporate unique national attributes and values, beginning with how to address the trope and indisputable truth that cybersecurity is a team sport. Canada's team must include all levels of government, all regions, Indigenous groups, critical infrastructure operators, businesses, not-for-profit organizations and Canadians themselves. The playbook for this national team must be transparent about the roles and responsibilities that each team member carries and lay out expectations for more experienced and mature team members to show more leadership in supporting others to raise their respective cybersecurity bars.

Cybersecurity is not the end goal. Rather, incremental improvements in best cybersecurity practices will fortify a more secure digital Canada — one that underwrites Canadians’ daily dependence on internet-enabled services; supports the online needs of Canadian governments, businesses, academics and innovators; helps safeguard citizens against online harms; and is a globally recognized trusted domain for digital trade and commerce.

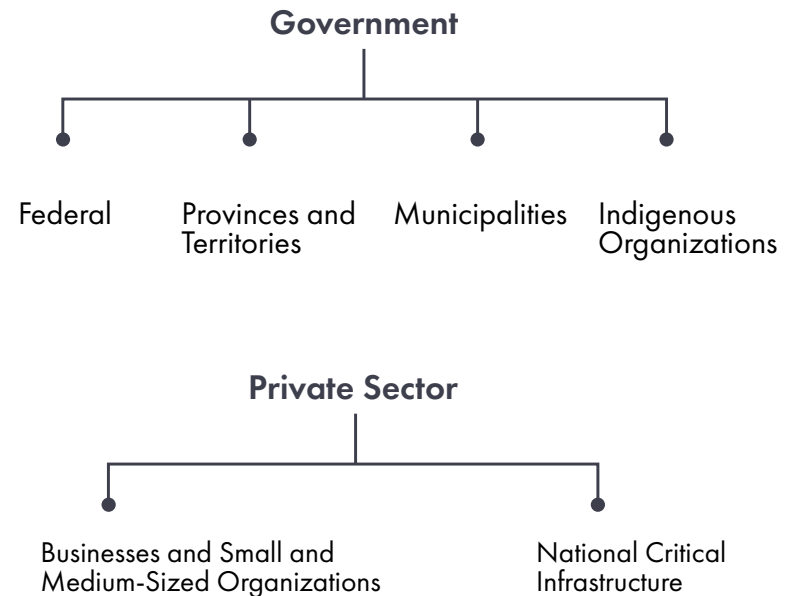
The choice to default to inclusion in addressing information sharing and incident response promises new levels of resilience and new opportunities for economic growth, prosperity, safety and security.

Cybersecurity is not the end goal. Rather, incremental improvements in best cybersecurity practices will fortify a more secure digital Canada.

Next Steps

To promote continuous communication and to enhance comprehension of the fundamental components necessary for shaping a new direction in national cybersecurity cooperation, CIGI will conduct a series of focused workshops. These discussions will be centred on the distinct contributions and needs of each jurisdiction, with the aim of generating progressive ideas that improve national information sharing, incident response capability and cyber resilience.

The workshops will be divided into the following categories:



Following each workshop, a summary report will be written as a contribution to a compendium. The insights generated will be instrumental in framing the agenda for the subsequent round of cybersecurity discussions at the WSD in June 2024, and contribute to Canada's national blueprint for cyber resilience.

Ultimately, reinforcing a high-functioning, reliable national network and routinely sharing information and best practices will, in time, incubate a more robust Canadian culture of cyber resilience — one that reduces cyber risk on a national scale, and where collaboration is commonplace, cyber incidents are fewer and less severe, and recovery from them is swift and less costly for Canadians.

Acknowledgements

We extend our gratitude to our expert planning committee for their role in making the first WSD a success. They worked diligently behind the scenes, offering guidance and oversight throughout the planning process. Additionally, we would like to acknowledge the Canadian Centre for Cyber Security for designing a comprehensive tabletop exercise that engaged practitioners from diverse sectors.



Centre for International Governance Innovation

About CIGI

The Centre for International Governance Innovation (CIGI) is an independent, non-partisan think tank whose peer-reviewed research and trusted analysis influence policy makers to innovate. Our global network of multidisciplinary researchers and strategic partnerships provide policy solutions for the digital era with one goal: to improve people's lives everywhere. Headquartered in Waterloo, Canada, CIGI has received support from the Government of Canada, the Government of Ontario and founder Jim Balsillie.

www.cigionline.org

Printed in Canada on paper containing
30% post-consumer fibre and certified by
the Forest Stewardship Council®

