SPECIAL REPORT

Waterloo Security Dialogue 2025
Fostering a National Culture of Cybersecurity

Shelly Bruce, John Bruce, Reanne Cayenne and Aaron Shull

67 Erb Street West
Waterloo, ON, Canada N2L 6C2
www.cigionline.org

About the Authors

Shelly Bruce is a CIGI distinguished fellow. She is 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 continues to be engaged in various projects promoting cyber resilience and is a visiting professor at the University of Ottawa and a fellow at Vanderbilt University in Nashville.

John Bruce is a CIGI senior fellow. He spent more than two decades with the Canadian Department of Justice, serving as legal counsel and providing strategic policy advice on the conduct of cybersecurity and active cyber operations. John teaches at Carleton University's Norman Paterson School of International Affairs, at the University of Ottawa and at the University of Calgary Law School.

Reanne Cayenne is a program manager at CIGI, where she oversees the operations of projects focused on national security, cybersecurity and responsible technology. Her role also involves policy research and analysis related to CIGI's research priorities. Prior to joining CIGI, Reanne worked as a researcher and consultant in the public, private and non-profit sectors, providing diverse clientele with analytical insights to inform their decision making.

Aaron Shull is research director of digitalization, security and democracy at CIGI. He is recognized as a leading expert on complex issues at the intersection of public policy, emerging technology, cybersecurity, privacy and data protection, and democratic resilience.

Table of Contents

Summary

We live in an increasingly interconnected world where emerging technology is rapidly expanding, amplifying and accelerating economic opportunities and scientific discovery. For all the optimism that comes with these advances, there is the expectation that threat actors will seek — and too readily find — ways to create new capabilities to exploit growing technical and human vulnerabilities. Cybersecurity only grows in importance.

Since 2023, the Waterloo Security Dialogue (WSD) has been designed to connect Canadian cybersecurity practitioners and decision makers — from all levels of government, Indigenous communities, industry sectors, business and civil society — keen to build a national culture of cybersecurity that can meet most cyberthreats head on. Participants have explored the common challenges affecting the majority of Canada's cybersecurity ecosystem and have been establishing new channels of communication to foster unexpected collaboration and ideas that benefit the greater community.

The Centre for International Governance Innovation (CIGI) hosted the third annual WSD on October 20, 2025. Senior officials from the federal government opened the event, updating the group on cybersecurity collaboration and investments, sharing highlights from the new National Cyber Security Strategy and the current Canadian cyberthreat landscape.

WSD participants then explored parts of the cyber ecosystem that have been routinely underserved, providing a contrast to the maturity of Canada's world-class national capabilities: local organizations that often lack experience and resources, but that bear direct, daily and disproportionate responsibilities for the citizens they serve. Conference panels focused on the power of local grassroots movements capable of providing cybersecurity support through expert volunteers, community engagement and reciprocity, together with clinics that match cybersecurity graduates with cyber-vulnerable organizations, and platforms that offer help to those experiencing cybercrime incidents. The practical value of cyberthreat information and intelligence (CTII) sharing within local communities of interest was also explored.

This special report shares insights gathered from WSD 2025, with a nod to connected themes and recommendations from past dialogues. Please note that all WSD events are held under the CIGI Rule,[1] and the content of this report does not reflect the views of any specific individual or organization.

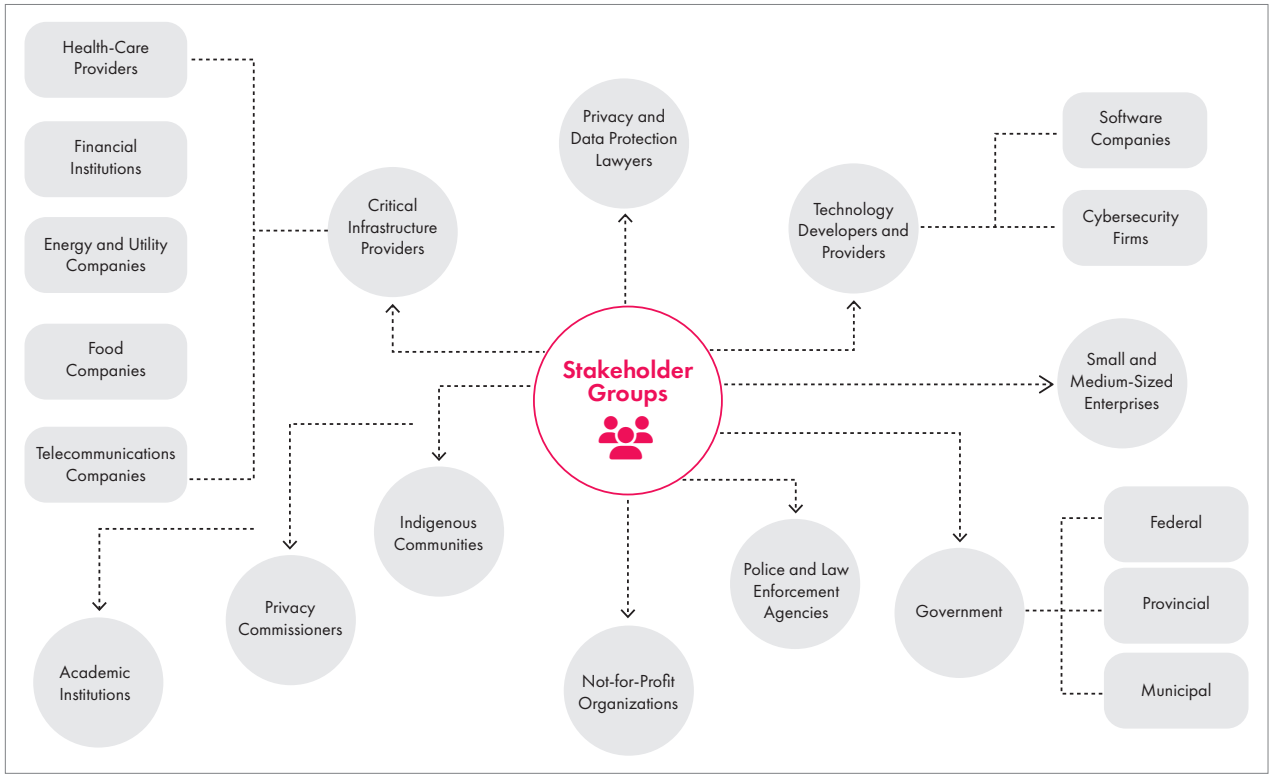
WSD 2025 attendees pose for a group photo.
Photo credit: Luke McKee, CIGI.

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.

Methodology

The unique selling point of the WSD is its broad and representative participation, coming from across Canadian jurisdictions, sectors and geography. Although the event is predominantly Canadian in focus, leading authorities and respected experts have been invited to various sessions to share their allied perspectives, experiences and lessons learned on themes being explored. Including this breadth of insight has allowed the WSD to better triangulate issues of priority concern across the Canadian cybersecurity ecosystem (see Figure 1).

Figure 1: WSD Key Stakeholder Groups



Source: Bruce et al. (2024, 7).

The Road to WSD 2025

Over the past three years, WSD delegates have matured their conversation from identifying the key, common cybersecurity challenges and priorities to exploring possible solutions or activities that can draw down risk through specific recommendations and actions.

2023

The inaugural WSD in 2023 welcomed representatives from municipal, provincial, territorial and federal governments, the private sector and civil society at the CIGI Campus in Waterloo, Ontario, Canada, to better understand channels of communication in the cybersecurity community, perceived hurdles to information sharing, and cyber-incident response silos and impediments in the country. Key takeaways that arose from interactive sessions, presentations and panels, as captured in the WSD 2023 special report (Bruce et al. 2023), included the need to:

- improve cybersecurity knowledge dissemination;
- clarify and communicate cyber-incident response protocols; and
- build a more robust pipeline to generate the cybersecurity talent Canada needs.

Attendees gather for a group photo at WSD 2023.
Photo credit: Julie Baxter, CIGI.

2024

The key findings from WSD 2023 became the starting points for focused consultations and workshops throughout the following year, culminating in WSD 2024. Through exploring persistent concerns with a broadly representative group of stakeholders, a comprehensive and mature set of recommendations was produced in the WSD 2024 special report (Bruce et al. 2024) around several more specific themes:

- real and perceived obstacles to community-wide cyberthreat intelligence and information sharing;
- coherent strategies for building cybersecurity talent and skills for practitioners, the workforce, executives and the Canadian public; and
- the potential for regional cybersecurity hubs to build confidence and capability among Canada's least-resourced and least-experienced cyber defenders.

2025

Following the 2024 dialogue, certain aspects of the WSD report recommendations were further explored. Specifically, a regional cybersecurity hub was piloted in British Columbia by volunteers looking to stress test the collaborative concept promoted in the WSD workshops. The British Columbia Cyber Security Hub (BC Cyber Hub) was also used as a platform to explore practical implications of CTII sharing and talent/skills recommendations from a local perspective.

Over the past three years, WSD delegates have matured their conversation from identifying the key, common cybersecurity challenges and priorities to exploring possible solutions or activities that can draw down risk.

WSD 2025: Building a Cyber-Resilient Canada

Canada aspires to a national culture of cybersecurity. The more attuned Canadian organizations and Canadians are to online risk, the more likely they are to practise good cybersecurity hygiene that can, in turn, help them avoid preventable cyber incidents that have the potential to inflict productivity, security, privacy and recovery costs. Determining what this looks like closest to the ground was the focus of this year's dialogue.

Building a national culture of cybersecurity relies on the different parts of Canada's cyber ecosystem playing to their potential and strengths. For example:

- federal government authorities generating strategic vision while mustering cybersecurity experts to build national capability and provide timely, useful advice and guidance;
- national critical infrastructure owners and operators protecting the systems running vital services Canadians rely on daily;
- technology vendors adopting "defence by design and default" principles to create more secure software across its life cycle; and,
- more generally, the rest of the ecosystem — organizations and individuals — being prepared and able to take on the responsibility of continuously improving their cybersecurity hygiene.

Each member of this ecosystem carries a degree — some more, some less — of cybersecurity risk for the broader community. Every one of these constituent groups would say their challenge is great and their cybersecurity work is incomplete, regardless of how experienced or resourced they are.

Federal Programs

WSD participants heard about important and constructive work at the federal level to draw down national risk, including fortifying and formalizing cybersecurity cooperation at the federal-provincial-territorial level. Recent efforts include ministerial cooperation on national digital resilience and official cybersecurity information-sharing agreements. A revised defence industrial strategy prominently features Canadian-led investments, and work is under way to reinforce cyber protections for the infrastructure required to sustain Canadian society and economy.

Together with industry and academia, panellists noted ongoing government support to close critical gaps within and across critical infrastructure sectors and in the safe and secure application of emerging technologies, including artificial intelligence (AI) and quantum. Federal officials reiterated the scope of the challenge and stressed that a whole-of-society approach was needed to address gaps. In their view, public-private engagement that is coherent, purpose-driven and nonduplicative could best help address cybersecurity risk by capitalizing on the strengths of both government and industry.

To reinforce the call for collaboration, WSD participants heard more about the 2025 National Cyber Security Strategy and its two overarching principles: whole-of-society engagement and agile leadership, coupled with a commitment to tackle issue-specific problem-solving. As part of the whole-of-society approach, participants heard that the strategy's Canadian Cyber Defence Collective Strategic Forum (CCDC-SF) aims to formalize collaboration and information sharing between the federal government and other private and public sector members of the Canadian cybersecurity ecosystem, including municipalities, Indigenous communities and not-for-profits.

The WSD 2025 panel "The Evolving Government of Canada Cybersecurity Agenda" featured (from left) Aaron Shull, managing director and general counsel, CIGI; Mark Schaan, deputy secretary to the Cabinet (artificial intelligence), Privy Council Office; Dan Rogers, director, Canadian Security Intelligence Service; and Caroline Xavier, chief, Communications Security Establishment.
Photo credit: Luke McKee, CIGI.

The Rest of the Ecosystem

The federal cybersecurity program and its capabilities are world-class but cannot sustain relationships with every Canadian organization needing tailored assistance, advice or guidance. This means that many of Canada's smallest and most vulnerable organizations struggle because:

- they lack dedicated information technology and security staff;
- the security advice available to them does not fit their needs (often too dense, too technical, too vague or too jargon-heavy);
- they are wary of cybersecurity vendors but are nervous about making security improvements on their own for fear of affecting their bottom line; or
- they are not aware of resources that can provide fit-for-purpose advice and guidance.

Together with industry and academia, panellists noted ongoing government support to close critical gaps within and across critical infrastructure sectors and in the safe and secure application of emerging technologies, including AI and quantum.

The Role of Grassroots Movements in Fortifying a National Culture of Cybersecurity

In the context of cybersecurity, partnership and cooperation are often key considerations, but there is little focus on exploring the specific models and permutations of collaboration within and across sectors, jurisdictions and civil society. In particular, more attention needs to be directed toward the value or impact of volunteer and not-for-profit initiatives that have been mobilizing to work with specific communities in an effort to draw down the level of risk they carry in Canada's collective cyber defence.

Opportunity and Intent

In 2024, WSD participants were enthusiastic about grassroots and volunteer efforts in promoting and fortifying regional cybersecurity. They highlighted key considerations and a set of recommended actions for local efforts that specifically addressed the growing divide between a region's most and least cyber-mature organizations. They singled out the needs of this latter group as a priority while still encouraging work in parallel to evolve the regional cybersecurity collaboration concept into a broader and more ambitious vision of sustainable, trusted support structures that could address other pressing cybersecurity gaps and challenges well into the future.

WSD 2024 participants stressed the critical value of broad representation in these regional initiatives. They sought opportunities for federal and provincial governments, municipalities, businesses, Indigenous communities, academia and non-profits to team up in new ways to:

- increase cybersecurity capacity and capability, aligned with the strengths of local universities and talent incubators;
- create new proving grounds, such as widely accessible cyber ranges and organized regional cybersecurity exercises;
- muster technical and operational support in times of urgent need (for example, with a regional corps of expert reservists or fractionally employed cybersecurity professionals); and
- consistently disseminate important cybersecurity information from federal and provincial authorities or, in the reverse, gather local perspectives and inputs for national strategies and plans.

Flowing from the 2024 dialogue, CIGI committed to explore some of these recommendations in 2025, in line with its approach of representative, multi-stakeholder engagement. The research team looked at how other countries were exploring regional cybersecurity models to inform a made-for-Canada pilot.

Example: The UK Approach

Probably the most developed model has been in the United Kingdom, with local, organic, voluntary networks distributed across 17 regional cyber clusters. Each cluster leverages public, private and academic cybersecurity leadership in its area, with an emphasis on promoting business development for cybersecurity firms based in the cluster. Membership models vary, but each is a volunteer group relying on public and private sector contributions to support small back-office functions, maintain a website with useful content and contact information, and organize awareness and networking events.

More recently, a centralized "umbrella" cluster — the UK Cyber Cluster Collaboration (UKC3)[2] — has been taking on the role of coordinating UK government connections to the 17 clusters (for example, in the distribution of grants and contributions). It is expected that the UKC3, although incorporated after most clusters were established, will promote more national coherence with agreed measures of success.

A Model for Canada

There are already some excellent volunteer cybersecurity initiatives and partnerships in Canada, but, given the vast nature of the country, they are often isolated or distributed in pockets around Canada. The vast majority have not yet been scaled or integrated with formal programs in a way that has created a pervasive national culture of cybersecurity. Given the decentralized approach, many currently support local cybersecurity start-ups or professional development and have few formal or informal connections among them.

While these initiatives should be celebrated for addressing important needs, relatively few are focused on the many, many small organizations that have little experience and few resources to deal with cybersecurity incidents.

2 See https://ukc3.co.uk/.

A Canadian Pilot: Why in British Columbia?

British Columbia faces a dynamic and growing cyberthreat landscape due to its high-value economic sectors — 98 percent of BC businesses are small and medium enterprises, contributing 35 percent of the province's GDP. With British Columbia recognized as Canada's Pacific gateway to global trade, cybercrime remains the most pervasive and persistent risk, specifically ransomware and other financially motivated crime. At the same time, state-sponsored cyberthreat actors have geopolitical interest in British Columbia and pose more of a strategic threat. In 2025, British Columbia — although representing 13 percent of the Canadian population — reported 20 percent of Canada's cyber breaches, primarily against health-care, education, energy, transport and community-based organizations.

Those consulted in British Columbia acknowledge that major BC operators often have the resources and knowledge to protect themselves against most cyberthreats; however, they remain concerned about levelling the cybersecurity risk in the region by helping the smaller, more vulnerable organizations in the BC cyber ecosystem improve cybersecurity hygiene.

The WSD 2025 panel "Regional Cybersecurity Communities of Practice" featured (from left) Nick Maltchev, Don Costello and Earl Maynard.
Photo credit: Luke McKee, CIGI.

As an additional consideration, BC participants were committed to addressing these needs through the Indigenous practice of reciprocity, a form of pro-social generosity based on collective responsibility, interdependence and resilience. This would require mature organizations to generously share their experience and expertise with those who most need assistance. BC participants in WSD's regional hub consultations were also determined that hub evolution be organic, voluntary, light touch in administration and governance, and with its priorities driven by the demands/needs of hub members.

Case Study: BC Cyber Hub Pilot

WSD 2025 panellists who steered the experiment explored early findings with the broader group. Still in its infancy, the BC Cyber Hub pilot project is a volunteer-led community of business, not-for-profit, municipal, provincial and federal experts helping BC organizations become incrementally more secure and resilient.

Since early 2025, the hub's 11 volunteers have met virtually on a biweekly basis. Their goals have been to:

- Draft basic terms of reference to guide expectations and governance.
- Set the vision/mission, starting with a focus on helping the small and most vulnerable organizations in British Columbia.
- Compile a regional inventory of cybersecurity resources and events as a reference.
- Create a website (www.bccyberhub.ca) as a central resource with information about cybersecurity and registration.
- Host in-person and virtual launches, with a call to action and membership drive.
- Survey local demand signal through a short questionnaire.
- Establish a baseline understanding of BC cyberthreat assessment with the help of the Canadian Centre for Cyber Security (Cyber Centre).
- Engage membership through scheduled events and informal connections geared toward raising cybersecurity awareness, answering members' questions and providing networking time that contributes to the region's sense of community.

While there is potential for the hub to contribute to a more mature and capable community of cybersecurity practice in British Columbia, especially in collaboration with other organizations, such as local business councils, the hub will not:

- duplicate any existing BC cybersecurity initiatives;
- take the place of cybersecurity professionals or business services and providers; or
- promote business development — any business support will be as corporate social responsibility only.

Level of Interest

Within the first six months, more than 100 people registered as members of the hub. Most of them had professional accreditations and experience, and were looking for an opportunity to contribute to bolstering British Columbia's culture of cybersecurity. Hub events, to date, have been centred on seeking potential members and offering introductory primers (for example, on identity management).

A recent focus has been exploring a pilot using personalized, AI-powered cybersecurity assistants to help small organizations improve their cyber hygiene. By onboarding through a simple questionnaire to assess their use of technology and preparedness, small organizations can use AI assistants to ask unlimited questions in a "no shame" environment. In return, they can get tailored, implementable guidance translating universal security standards into simple, step-by-step instructions. Emphasis has been on understanding their needs and meeting them where they are with accessible solutions.

In these still early days, the hub is gradually emerging as a safe space for small BC organizations to present their needs and be matched with free, plain-language advice and guidance and tools that can reduce their organization's risk. Interest and support are sufficient for the hub to continue to evolve organically; however, a more sustainable structure may be required.

CTII Sharing

Another WSD 2024 key principle was explored through the BC Cyber Hub perspective: CTII-sharing processes needed to be as straightforward and cost-effective as possible. For community members to feel comfortable sharing CTII within their own community or, more broadly, with others across the country, members would require a clear value proposition and confidence in trusted sharing processes that addressed legal and operational considerations. Recognizing these requirements, the work leading up to WSD 2025 focused on what kind of CTII is of greatest benefit to these communities.

The first step was to create a catalogue of CTII artifacts — ones most likely to be of value to BC Cyber Hub members in the detection and management of phishing, ransomware and supply-chain network attacks. The catalogue has two general classes of CTII: "operational CTII," which are specific indicators of compromise such as email addresses, IP addresses and associated domains; and "tactical CTII," which provide insight into the adversary's tactics, techniques and procedures.

Given the capability disparity within the BC Cyber Hub membership, the initial focus was on sharing the kind of operational CTII that would be the most useful to network defenders having only rudimentary technical capabilities and limited experience in security operations. While some of this operational CTII contains personal information — the disclosure of which (without the data subject's consent) would be prohibited under the personal information protection legislation in place across Canada — in British Columbia, there is a legal mechanism capable of supporting the disclosure of this class of CTII. The process is complex, however, and requires the establishment of a number of legal arrangements among hub members.[3]

During the dialogue, panellists agreed that the complex legal and technical structures needed to support the sharing of operational CTII containing personal information diminished the overall benefits. The panel felt that developing complex sharing frameworks for operational CTII may not represent the best use of the hub's time and resources over the long term.

---

3 These disclosures could take place under a common program agreement (CPA), which must involve at least one public sector entity as a signatory. The CPA must be reviewed and approved by the information and privacy commissioner for British Columbia. Once approved, the CPA operates as a lawful authority for disclosing personal information without the consent of the data subject under the Freedom of Information and Protection of Privacy Act. The BC information and privacy commissioner also recognizes CPAs as a legal authority for the disclosure of personal information without the consent of the data subject under British Columbia's Personal Information Protection Act, authorizing the registered hub members to share this information with each other.

In comparison, the sharing of tactical CTII and security analytics offers benefits to both less mature network defenders (for example, basic security monitoring) and those that are more advanced (for example, threat hunting). In addition, the distribution of tactical CTII does not give rise to the same legal complications that can arise with sharing personal information found in some operational CTII. The panel felt the hub should focus on the distribution of tactical CTII and take advantage of advances in AI technology to create agents that could help those hub members with minimal technical and resource capabilities to ingest tactical CTII.

The panel agreed that much of the tactical CTII needed to support this approach is already available from existing sources such as the Cyber Centre, CyberBC and the Canadian Cyber Threat Exchange (CCTX). In addition to distributing tactical CTII of interest to its members, the hub could act as a regional translator and amplifier, tailoring national and provincial intelligence to fit the needs of its members while feeding local insights back to partners such as the Cyber Centre, CyberBC and CCTX. This two-way flow will strengthen both regional and national cyber resilience more effectively than focusing on short-lived or ephemeral operational CTII.

The WSD 2025 panel on "Improving Cyber Threat Information Sharing" featured (from left) Bob Gordon, strategic advisor, CCTX; Brent Arnold, founder, Capstan Legal; Emily Laidlaw, Canada Research Chair in Cybersecurity Law, and associate professor, Faculty of Law, University of Calgary; Caitlin Lemiski, director of policy, Office of the Information and Privacy Commissioner, Government of British Columbia; and Dave Whyte, co-founder and chief technical officer, Tidal Point Software. *Photo credit:* Luke McKee, CIGI.

For community members to feel comfortable sharing CTII within their own community or, more broadly, with others across the country, members would require a clear value proposition and confidence in trusted sharing processes that addressed legal and operational considerations.

Talent Dividends from Grassroots Initiatives

One of the key WSD 2024 themes focused on creating a pipeline for developing cybersecurity talent. The BC Cyber Hub pilot explored opportunities for grassroots initiatives to have a "win-win" impact by providing useful support that could also reinforce academic programming and skills. As examples, panellists discussed different models operating in Canada today:

- **The Catalyst Cyber Clinic** at the Rogers Cybersecure Catalyst (Toronto Metropolitan University) where the clinic (similar in concept to legal aid clinics) matches and mentors students graduating from university cybersecurity studies, helping them gain useful, practical experience working with small not-for-profit organizations with limited resources to implement basic security to protect their clients and their mission.

- **La Clinique de cyber-criminologie** (Université de Montréal) where criminology and psychology students gain valuable experience by supporting victims of online scams, but also use the data acquired to build insight into emerging fraud trends, including the use of AI by cybercriminals. Assistance for victims includes guiding clients through administrative tasks on how to file claims for fraud and a personalized action plan for recovery.

- **High-school initiatives** in British Columbia to encourage skilled talent in cybersecurity by the BC chapter of the Information Systems Audit and Control Association.

The dual objectives of these grassroots initiatives embrace the "cyber for all" concept. Those who are cyber vulnerable or cyber victimized get informed support for their needs while the students hone their technical skills and work ethic. This practical experience is increasingly sought by employers onboarding new cybersecurity talent — with a demonstrated hiring interest by financial institutions and law enforcement.

Panellists noted the lack of visibility of grassroots efforts geared toward cybersecurity and stressed that more awareness and information sharing across clinics could also provide opportunities to see who else may be interested in setting up new clinics and/or expanding current ones.

Going Forward: Reflections and Next Steps

In all WSD 2025 discussions, themes of collective defence and national resilience were set against the challenging reality of Canada's vast and varied cybersecurity ecosystem. Participants heard about practical efforts to address such a diverse mix of cybersecurity needs juxtaposed against the priority and urgency of reducing cyber risk at the national level.

Ultimately, the trend of sophisticated cyberthreat actors — both state and criminal — continuing to target Canada's most vulnerable organizations set the backdrop for the WSD 2025 discussions. The threat to small municipalities, local Indigenous communities, schools, hospitals, small businesses or not-for-profit community groups appears only set to grow as emerging technologies help threat actors to refine and amplify their activities.

While federal and national players continue to produce expert information resources, vulnerable members of Canada's ecosystem can benefit from support networks closer to home translating that knowledge into consumable advice and guidance for them. Grassroots and volunteer movements are filling critical gaps and represent an increasingly important catalyst for a healthy national culture of cybersecurity. They help:

- raise cybersecurity awareness in their community;
- direct volunteer expertise and other contributions to those with need and interest in improving their cybersecurity;
- build trust and confidence among those serving in their community; and,

- ultimately, reduce cybersecurity risk and improve local cyber resilience.

Key takeaways from this year's dialogue include the need to:

- Recognize and promote the role of grassroots cybersecurity movements in administering support that helps the most cyber-vulnerable organizations to adopt basic cyber hygiene and to engage established Canadian resources for continuing advice and guidance.

- In the spirit of the 2025 National Cyber Security Strategy's emphasis on "whole of society," encourage highly effective grassroots cybersecurity models — ones that successfully improve trust and confidence among members and materially raise their cybersecurity bar — to make their "blueprints" available for other Canadian volunteer groups. These can be replicated elsewhere or, alternately, be scaled or "franchised" on a more national basis.

- Seek consistent competency and ethics frameworks to help set expectations and boundaries for the volunteer experts and practitioners supporting these initiatives.

- Ensure the new strategy's federal CCDC-SF consultation construct includes leaders of grassroots initiatives who can help:
  - bring coherence to a national network or pipeline of grassroots groups with cybersecurity goals;
  - provide input regarding local challenges into national cybersecurity strategies or policies;
  - amplify national cybersecurity messaging and advice, and provide recommendations for products to less-experienced, less-resourced organizations; and
  - act as focus groups for any cybersecurity matters of national consultation.

- Encourage private-public partnerships that engage grassroots movements and help the most vulnerable Canadian organizations mature to reduce their cyber risk.

The WSD 2025 panel "Addressing Local Cybersecurity Gaps" featured (from left) Benoît Dupont, Nick Maltchev and Katie Gibson.
Photo credit: Luke McKee, CIGI.

In the end, the key takeaway is that it is in our collective security interest to capitalize on the expertise and generosity of passionate volunteers keen on bolstering a national culture of cybersecurity. If not, we are squandering a powerful opportunity that demands relatively few resources to sustain and offers great dividends. Grassroots initiatives, although local, have far-reaching impacts for the prosperity, safety and security of Canadians, especially considering that the beneficiaries of their support are often organizations carrying great responsibility of care for local populations.

Acknowledgements

CIGI would like to thank the CSE and the Cyber Centre for partnering with us to host the 2025 WSD in Ottawa. It was no easy feat gathering representatives from the public and private sectors, civil society, academia and Indigenous communities; the Cyber Centre welcomed the WSD team and attendees graciously, and their support in facilitating the event directly contributed to its success. It was an honour to host the dialogue during Cybersecurity Awareness Month with a formidable organization dedicated to fostering cyber resilience in Canada.

We also extend our gratitude to the conference speakers, participants and planners. Active engagement and insights shared by the community promote a trusted, informed and committed network geared toward shaping Canada's cybersecurity posture for years to come.

Works Cited

Bruce, Shelly, John Bruce, Aaron Shull and Kailee Hilt. 2023. *Waterloo Security Dialogue: Fostering Nationwide Cybersecurity Collaboration.* Special Report. Waterloo, ON: CIGI. www.cigionline.org/publications/waterloo-security-dialogue-fostering-nationwide-cybersecurity-collaboration/.

———. 2024. *Building a Cyber-Resilient Canada: Highlights from the Waterloo Security Dialogue 2024*. Special Report. Waterloo, ON: CIGI. www.cigionline.org/publications/building-a-cyber-resilient-canada-highlights-from-the-waterloo-security-dialogue-2024/.

Acronyms and Abbreviations

AI	artificial intelligence
BC Cyber Hub	British Columbia Cyber Security Hub
CCDC-SF	Canadian Cyber Defence Collective Strategic Forum
CCTX	Canadian Cyber Threat Exchange
CIGI	Centre for International Governance Innovation
CPA	common program agreement
CSE	Communications Security Establishment
CTII	cyberthreat information and intelligence
Cyber Centre	Canadian Centre for Cyber Security
UKC3	UK Cyber Cluster Collaboration
WSD	Waterloo Security Dialogue

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®

RECYCLED
Paper made from
recycled material
FSC® C023070