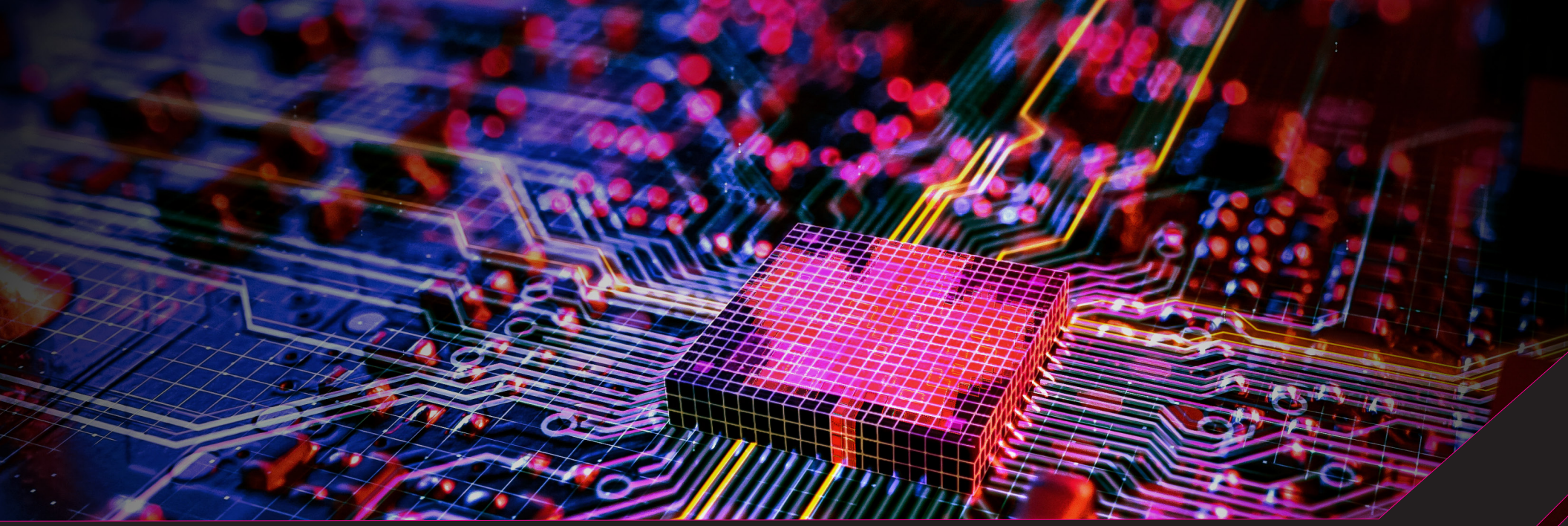


SPECIAL REPORT

Building a Cyber-Resilient Canada

Highlights from the Waterloo Security Dialogue 2024

Shelly Bruce, John Bruce, Kailee Hilt 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 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 continues to be engaged in various projects promoting cyber resilience and is a visiting professor at the University of Ottawa.

John Bruce is a CIGI senior fellow and a cybersecurity expert. Prior to his retirement in September 2022, John was the general counsel for Field Effect Software Inc., a cybersecurity firm in Ottawa. He spent more than two decades with the Canadian Department of Justice, serving as legal counsel and providing strategic policy advice for the Government of Canada's conduct of cyber defence and active cyber operations.

Kailee Hilt is a program manager and research associate at CIGI, where she focuses on public policy issues tied to emerging technology, privacy and cybersecurity. Kailee is presently pursuing her Certified Information Privacy Professional designation.

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.

Table of Contents

Summary

On June 10–11, 2024, the Centre for International Governance Innovation (CIGI) hosted the second annual Waterloo Security Dialogue (WSD), bringing together cybersecurity leaders from across Canada. This event, along with pre-conference consultations, represented a significant effort to merge the concerns and ideas of stakeholders from all sectors — government, private industry, Indigenous communities, academia and civil society. The WSD combines both established and new recommendations, underscoring the need for innovative solutions to tackle Canada's most pressing cybersecurity challenges, such as forming supportive communities of cybersecurity practice, sharing cyberthreat information effectively and bridging the cybersecurity talent gap.

To strengthen Canada's cybersecurity resilience, enhanced cooperation within and across jurisdictions and sectors is essential. A pervasive national culture of cyber resilience can help mitigate cyber risks and result in fewer cybersecurity incidents, with less severe impacts and faster recovery cycles. Continuously improving Canada's national cybersecurity framework can also better prepare the ground for securing emerging technology and inoculating Canadians against other online harms. Engaging the entire Canadian cybersecurity ecosystem is crucial for achieving this vision and fostering greater national prosperity, competitiveness, safety and security.

This special report presents valuable takeaways from various workshops and conference discussions, held under the CIGI Rule,[1] in the lead-up to or during WSD 2024. It is important to note that this report does not reflect the views of any specific individual or organization. Rather, its primary objective is to lay out key ideas and recommendations identified by participants for further exploration.

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.

Key Takeaways

Pathway Forward

Regional Cybersecurity Hubs

Drawing inspiration from Indigenous practices of reciprocity and mutual support, cybersecurity communities of practice or regional hubs have the potential to build Canada's more mature "cyber haves" to support the less mature "cyber-have-nots" in ways that reduce the imbalance of experience, capacity and capability within the cybersecurity ecosystem and, as a result, reduce cyber risk on a national level.

- On a national level, acknowledge and promote the strategic value of cybersecurity partnerships.
- Create conditions for interjurisdictional and cross-sectoral cybersecurity partnering.
- Establish or share new capacity, knowledge, technology and talent within and across hubs.
- Improve coordination and communication across the national cybersecurity ecosystem.

Cyberthreat Information Sharing

Sharing cyberthreat information on a community-wide basis (i.e., beyond those who are actively managing a specific compromise) can help identify other Canadian organizations that may have been victimized or that are at risk. A national framework that supports broad cyberthreat information sharing can help network defenders better protect their systems and information from similar threats.

- Provide a legal mechanism to account for privacy and data protection obligations.
- Establish a clear value proposition and trust in processes to anonymize sensitive information and standardize language and instruments.
- Make cyberthreat sharing easy and cost-efficient with clear information, shared architecture and common protocols.

Cybersecurity Talent

The demand for cybersecurity talent is pervasive and evolving across a spectrum, starting with raising awareness to keep Canadians secure online, and training for students and employees; to education for cybersecurity professionals designing, deploying and maintaining secure systems; to advanced researchers and support for executives and decision makers. At its core, cybersecurity talent is the foundation for securing new and emerging technologies.

- Implement a national cybersecurity talent and education strategy.
- Evolve a cybersecurity talent pipeline fit for the future, including a formal program for primary, secondary and post-secondary students.
- Increase private sector-academic partnerships in the skills ecosystem.

Context

Imagine a future where the shared responsibility of cybersecurity in Canada is understood and supported by a conducive national framework. Where the right cyberthreat information is shared or available to those who need it, when they need it. Where Canadians default to good cyber hygiene, making them less susceptible to other online harms, such as disinformation and fraud. Where free or affordable cybersecurity training is available in schools and workplaces, and where public-private incubators and apprenticeship programs underpin the practical education of cybersecurity professionals.

Canada's jurisdictions and sectors are united and guided by a co-created, inclusive national strategy, and its most mature organizations set the example of modern, world-class defences for critical Canadian systems and information — all of which have been designed and maintained with security front of mind. Government and private sector leaders also routinely and publicly prioritize, invest in and support cybersecurity partnerships that drive continuous improvements to Canada's cyber resilience.

Canadian organizations, both public and private, experience the fewest cybersecurity incidents per capita globally. When incidents do inevitably occur, they are addressed swiftly and capably managed with minimal downtime and without lingering impact.

On the international stage, Canada is viewed as a best-in-class domestic model for cybersecurity. This confidence attracts investment, foreign businesses, digital trade, innovators and researchers. In its enforcement of the law and through cyber operations, Canada counters foreign threats and manages national risks with proportionate and responsible actions that respect international law.

With genuine dedication and a whole-of-society approach, this vision is achievable. In fact, some of it is already true. Some parts are inconsistently implemented; other parts are aspirational. But there is no argument — more needs to be done.

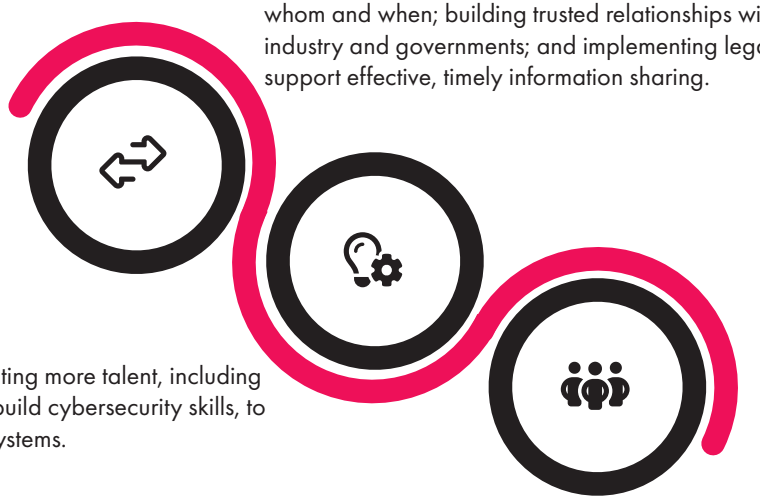
This is why CIGI hosted the second annual WSD on June 10–11, 2024. The event brought together representatives from all levels of government, Indigenous communities, the private sector, academia and key civil society members. The WSD reminds us that there are leaders and experts eager and energized to get us closer to that vision — largely through the power of collaboration.

Despite notable examples of strong partnerships and interjurisdictional collaboration across the country, most agree that these successes are often isolated and lack a cohesive framework. The pre-conference consultations and discussions during the event aimed to promote some of these encouraging partnerships, deconstruct specific challenges, identify recommendations and solutions, and create opportunities for greater collaboration across jurisdictions and sectors.

Focus Areas

WSD 2023 established a solid foundation by examining the state of cybersecurity in Canada. WSD 2024 expanded on this by diving deeper into addressing some of the nation's most persistent cybersecurity concerns. The 2024 agenda concentrated on three themes:

Information sharing: Clarifying what should be shared, with whom and when; building trusted relationships within and among industry and governments; and implementing legal authorities that support effective, timely information sharing.



Talent: In the near term, generating more talent, including innovative new approaches to build cybersecurity skills, to design and protect defensible systems.

Regional interjurisdictional teaming: Building and implementing a national blueprint for local public-private cybersecurity support and collaboration, starting with pilots in regional hubs.

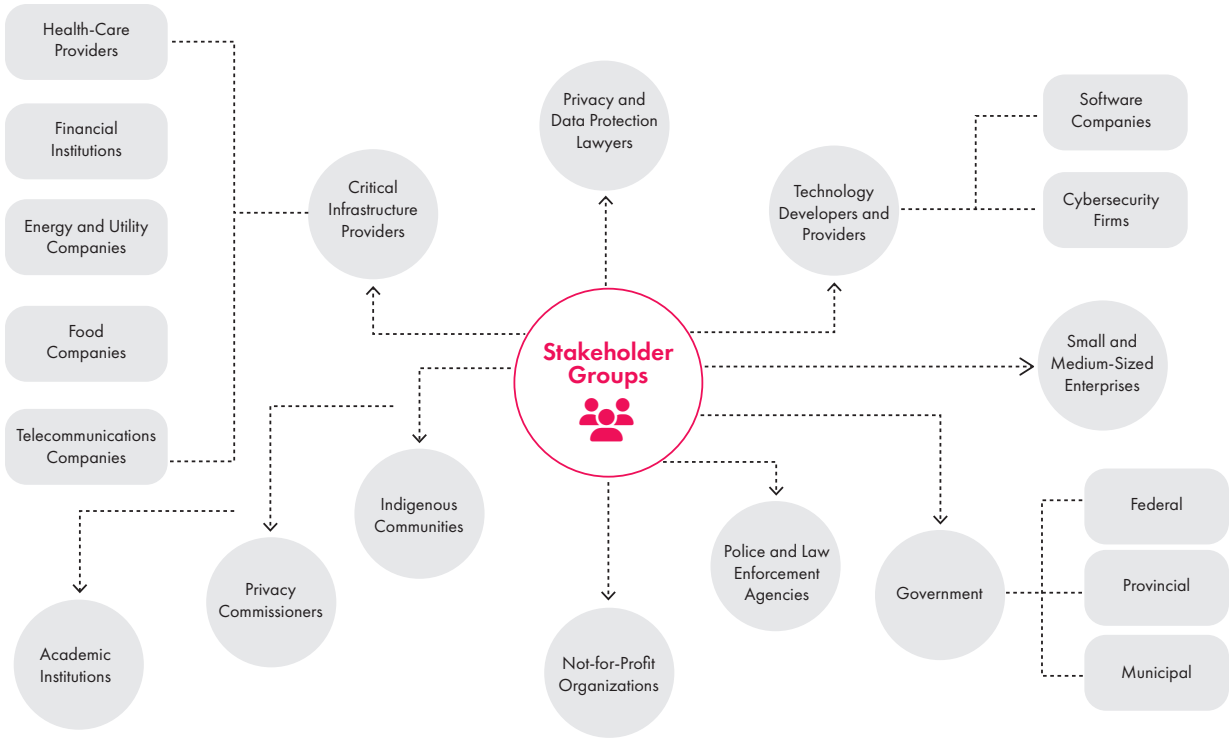
By concentrating on these horizontal themes as force multipliers, the intention was that participants would be able to make serious, thoughtful recommendations as strong cornerstones for the evolving national cybersecurity agenda, inspiring the potential development of future initiatives and partnerships.

Methodology

Consulting Key Stakeholder Groups

Leading up to WSD 2024, CIGI hosted a series of workshops that convened professionals from diverse public and private sector organizations. These sessions provided an opportunity for participants to reflect on the challenges in the current cybersecurity landscape and explore strategies for more effective interaction and potential collaboration with other regional and national groups.

The discussions included the following stakeholders:



The workshops and the conference sparked a wide range of perspectives and insights through several key processes:

- **Initial inputs:** Building on the foundational views and information shared during the first conference established the context for the ongoing dialogue and areas of focus.
- **Workshop consultations:** To ensure a diversity of perspectives, consultations were conducted with a targeted sample of stakeholder groups to narrow in on specific issues and proposals.
- **Workshop discussion papers:** Short background papers with discussion questions were distributed to participants prior to the meetings to lay the foundation for the conversations. These papers also included highlights from international and allied initiatives that could serve or be customized to fill a specific gap.
- **Conference presentations:** For the larger conference, speakers were carefully selected, and participants were personally invited to the event. It was important to limit the number of conference participants to ensure that everyone had the opportunity to contribute their views. The presentations and discussions addressed the three horizontal themes, enriching the dialogue with international perspectives and innovative approaches from key allies, including the United States and the United Kingdom. This laid the groundwork for validating, debating and refining both the identified challenges and proposed solutions.
- **Conference breakout sessions:** During the conference, participants separated into small groups to discuss, debate and refine proposals related to cybersecurity information sharing, skills training and regional hubs. This comprehensive approach produced robust and well-informed recommendations, as participants engaged in detailed discussions and contributed diverse experiences.

Challenges and Recommendations

The following sections detail the discussion related to the challenge space and the recommendations that emerged from the consultation sessions held throughout the year.

Regional Cybersecurity Hubs

Of the three WSD 2024 themes, regional cybersecurity hubs represent the most “blue sky” thinking. They are also perhaps the most uniquely Canadian and most promising approach to building up confidence and capability among Canada’s least-experienced frontline cyber defenders.

Inspired by the Indigenous practice of reciprocity, a form of pro-social generosity, participants leaned into a Canadian approach to regional cybersecurity hubs that emphasized mutual support and shared benefits. This philosophy underscores the importance of collective responsibility and interdependence in achieving a more resilient and balanced cybersecurity ecosystem.

Value Proposition

Every day, Canadians expect ready access to the critical services and information they rely on. Organizations delivering these services and safeguarding information understand that, while it is impossible to eliminate all risk, applying robust cybersecurity policies and practices can significantly reduce the likelihood of serious cyberthreats and enhance recovery. However, Canadian organizations vary in their preparedness. Those at the more mature end of the spectrum possess valuable experience and are eager to collaborate with those struggling to implement effective cybersecurity measures in the interest of collective defence.

Establishing models to support these connections and address the imbalance of capacity and capability within our ecosystem can help offset national cyber risk and cultivate the culture of cyber resilience needed to counter the expanding global threat landscape. Over time, a stronger Canadian network of more cyber-mature organizations will yield significant benefits in terms of collaboration, innovation and resilience.

Challenges

Certain members of Canada's cybersecurity ecosystem, in particular the federal government, technology vendors and national critical infrastructure owners, have achieved a level of cybersecurity maturity and are very seized with the importance of secure partners in their immediate circle and extended supply chain. Working as a collective, they have the potential to draw down more national cybersecurity risk and support ecosystem members who are less experienced and have fewer resources for cybersecurity, in particular municipalities, Indigenous communities and territorial governments, each of which bears a direct, daily and disproportionate load in safeguarding local services and information.

Ultimately, the challenge is to create opportunities for the "cyber-haves" to support the "cyber-have-nots" regionally and nationally through advice and guidance, coaching, assistance, and the transfer of technology and knowledge to improve their cybersecurity postures. A secondary challenge is to ensure that examples of excellent, innovative or novel collaboration and support are quickly recognized, promoted and, where possible, scaled to more national levels.

Consultation Takeaways

Participants in various CIGI consultation sessions[2] expressed strong interest in exploring regional cybersecurity hubs and trust-based communities to react to the most pressing local gaps and pressures. They called for better partnerships between the government and the private sector to help those who are struggling to implement baseline cybersecurity practices and controls. Levelling this playing field was seen as a necessary foundational step toward stronger partnerships, more creative and innovative collaboration, and, ultimately, fewer, less severe cybersecurity incidents.

2 Workshop discussions in British Columbia included representatives from federal and provincial governments, critical infrastructure, small and medium-sized businesses, academia, Indigenous organizations and law enforcement; separate consultations with partners, including privacy commissioners, law enforcement, legal and insurance experts, and not-for-profit organizations; discussions and briefings from UK leaders managing their national program of regional cyber and technology clusters; and hands-on workshops and discussions among WSD participants at the conference in Waterloo.

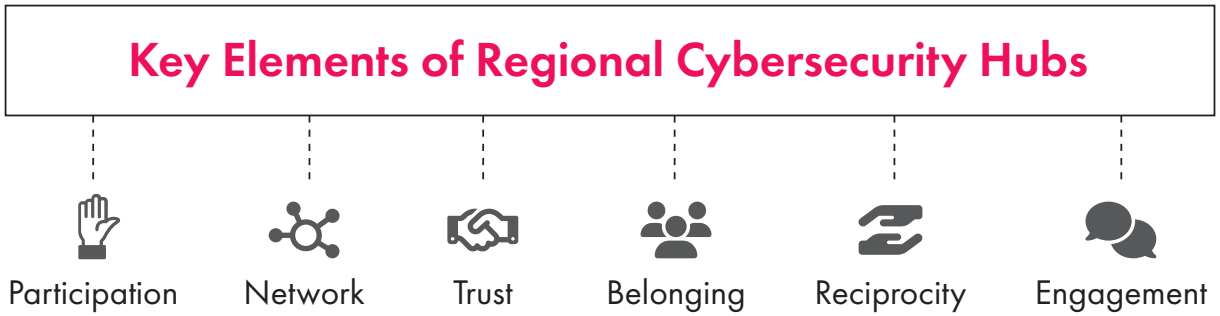
IN FOCUS: British Columbia

In March 2024, cybersecurity leads from different jurisdictions and sectors gathered around a table in Vancouver, British Columbia, to explore the potential value of regional cybersecurity hubs. Participants discussed benefits and challenges, emphasizing the need for broad inclusivity, including federal, provincial and municipal governments; Indigenous communities; as well as academic institutions and small and medium-sized enterprises.

Several participants acknowledged that their smaller organizations were struggling to implement basic cybersecurity standards and respond to serious incidents. They noted they would benefit from the support of local partners to navigate the abundance of publicly available advice, guidance and tools, as well as assess the growing slate of commercial vendors promoting their products and services. These organizations expressed a need for assistance in the form of templates and checklists for internal cybersecurity policies, response planning, training materials, and other non-proprietary information such as tools for assessing risk and privacy impact. There was also a strong desire to use the hub community's connections to close gaps, make introductions, and tap into or leverage existing centres of excellence, trusted partnerships and associations.

Some key themes emerged across the conversations:

- **Organic:** A regional hub should serve its community and evolve organically to address member demands that cannot be met by existing relationships and groups.
- **Coherent:** At the same time, WSD participants envisioned the establishment of multiple regional cybersecurity hubs across the country. To increase national coherence, they agreed on the need for an overarching statement of strategic intent. There was consensus that some initial agreement on the allocation of hubs to specific regions might be necessary.
- **Function over form:** Participants stressed the importance of ensuring that membership in a regional hub remains voluntary rather than mandated. They preferred virtual constructs and online access to information and resources over physical organizations. Simplified processes and transparent arrangements with minimal bureaucracy would encourage more organizations to participate. There is still a strong need for face-to-face introductions and networking opportunities.



- **Joint buy-in and endorsement:** With success driven from the top, participants felt the concept as well as any hub pilots needed endorsement from both public and private sector leaders, along with clear support from sponsors of networking, mentoring and knowledge-sharing events. They underscored that both government and the private sector bring unique strengths in terms of knowledge, guidance and financial support, but each also has different drivers and limitations. Combining efforts expands the pool of mandates, capabilities and expertise that hub members can access.

- **Leverage existing strengths:** There was no appetite to reinvent or duplicate work; rather, there was a desire to use the hub community's connections to close gaps, make introductions, and tap into or leverage existing centres of excellence, trusted partnerships and associations. For example, organizations needing support may be unaware of the products, services and training already offered by the federal Canadian Centre for Cyber Security (CCCS), or they may benefit from consulting national sector-specific associations, such as the Canadian Security Telecommunications Advisory Committee or the Energy Security Technical Advisory Committee, for specific cybersecurity expertise in the telecommunications or energy sectors, respectively.

- **Replicate collaboration successes:** There are excellent Canadian examples of collaboration to develop capability and talent, such as business- and university-sponsored cyber ranges serving a region, or municipalities within a district saving by combining security operations centres. Successful pilot projects and initiatives can serve as blueprints for others, with the best ideas scaled across the country. These opportunities range from federating a network of cyber ranges to time-sharing experts (for example, using fractional employment models to deploy employees with specific skills to work on urgent problems across a region), and more.

- **Developing and sharing talent:** Tighter connections might also encourage business investments, such as in cyber ranges, and increase integration and apprenticeship opportunities for on-the-job experience and training. For organizations seeking skilled professionals, this approach could create more opportunities to hire locally. Participants also noted that the trend for remote work might reduce enthusiasm for relocation within Canada, making it even more important to match talent with local co-op and apprenticeship programs.

- **Push-and-pull information network:** Hubs could use their inherent network to disseminate useful or urgent information broadly and more consistently (for example, cyberthreat advisories) across the country, or be used to consult or survey members regarding important issues and initiatives (for example, national strategies or policies). Cybersecurity hub members could use the hub network to communicate common concerns to those who can help (for example, highlight legal and policy impediments with federal or provincial

authorities). In addition, organizations could benefit from access to shared resources, such as templates and checklists for internal cybersecurity policies, response planning, training materials and other non-proprietary information (for example, tools for assessing risk and privacy impact), as well as assistance in evaluating the increasing number of commercial vendors promoting their products and services.

- **Regional priorities and national resilience:** While regional hubs would operate under common foundational principles (for example, to be equitable and diverse, act with transparency, move at the "speed of the fastest"), they could also build depth and expertise (for example, to address specific regional challenges or reflect socio-economic and cultural perspectives). A trusted community of regional partners would be more easily mustered to test readiness and build resilience through cybersecurity exercises.
- **National network of regional hubs:** Each region could also tap into the technical, operational or policy expertise developed naturally in other regional hubs.

Moving Forward: Recommendations Related to Regional Cybersecurity Hubs

Acknowledge and promote the strategic value of cybersecurity partnerships:

- Deliver national-level statements about the importance of Canada's cyber resilience and regularly promote examples of successful public-private partnering and collaboration.
- Secure business and political support, with public endorsement and encouragement of cybersecurity partnerships from the most senior ranks in the public and private sectors (for example, government ministers, CEOs, senior business executives and academic leaders).
- Promote partnerships within and across sectors as a key evolving theme in national cybersecurity strategies.
- Exchange best practices with other nations exploring similar regional constructs, such as European or UK clusters.

Create conditions for interjurisdictional partnering within the broader ecosystem:

- Co-create principles for regional cybersecurity hubs where industry, government and civil society voluntarily but more routinely collaborate and exchange knowledge in ways that strengthen regional and, by extension, national cybersecurity ecosystems.

- Co-create an inventory of basic activities (for example, making connections with centres of excellence for advice and guidance, networking and educational events, and sourcing and sharing [non-proprietary] resources, such as internal cybersecurity policy templates, exercises and workforce training materials, matching skills with needs and so forth).
- Capture a basic "blueprint" for a hub in not-for-profit entities' articles of incorporation to administer regional cybersecurity hubs and actively promote partnerships and collaboration opportunities within and across jurisdictions/sectors.
- Seek public and private sector funding to support regional cybersecurity hubs. Establish incentives and recognition schemes to encourage private sector organizations to invest in these hubs and support new partnerships.

Generate new cybersecurity capacity through new partnerships:

- Encourage each hub to also focus on partnerships and grow cybersecurity knowledge aligned with the academic research strengths of its local universities, uniquely regional cybersecurity challenges, and/or cultural considerations (for example, Indigenous approaches, multilingual resources). Individual hubs would share the unique expertise and experiences they have developed with other regional hubs when requested.
- Build a regional corps of cybersecurity reservists and experts who can be mustered in response to urgent needs, work surges or for fractional ("time-shared") employment on specific issues.
- Encourage each hub to adopt principles of reciprocity, promoting an equitable exchange of cybersecurity knowledge and resources. By integrating Indigenous approaches, including the philosophy of reciprocity, hubs can create culturally relevant and effective partnerships that respect and leverage the strengths of all participants.

Improve coordination and communication across the national cybersecurity ecosystem:

- Implement light-touch, overarching governance for national coherence; advise regional hubs; track metrics and progress nationally; and promote inter-hub collaboration while encouraging each hub to develop organically to meet the needs of its region.
- Encourage federal, provincial and territorial authorities to use regional hubs to communicate or push urgent messages, poll or survey, and/or conduct exercises with a nationally representative network of hub members.

- Conversely, encourage regional hub members to use the local or national networks to compare or raise issues and escalate concerns to those best placed to address them.

Community-Wide Cyberthreat Intelligence and Information Sharing

There is broad consensus on the need for enhanced sharing of cyberthreat information and intelligence (CTII) to strengthen Canada's national cyber defence. Regular, timely exchange of relevant, useful and actionable information can offer organizations insights they may not generate independently, enabling more informed cybersecurity decisions. Harnessing the collective knowledge, experience and analytical capabilities of the community can help close the gap between attackers and defenders.

Value Proposition

Canadian networks will never be impervious to all cyberthreat activity, but we can make it more costly for threat actors to do their worst. Most of these perpetrators are looking for quick, easy wins using tried-and-tested techniques that involve minimal adaptation and maximum results. Our objective is to make Canadian networks sufficiently hard targets so that the growing cloud of cyber locusts choose to pass over Canada's domestic cyberspace. Sharing CTII from even a single incident with the broader community can have immediate and longer-term impact in achieving that objective.

In a tactical sense, cyberthreat actors can be halted when an organization promptly shares relevant and actionable threat indicators of compromise (IOCs) with other defenders who can integrate them into their network defences. These shared IOCs also enable national defenders to analyze the attack and its perpetrators, helping to identify other potential victims in Canada. This allows officials to alert affected organizations and take follow-up actions within their own mandates, such as hunting, blocking or disrupting the capabilities of specific threat actors targeting Canadians.

On a strategic level, shared IOCs, when combined with other cyberthreat intelligence detailing the tactics, techniques and procedures used by threat actors, can equip network defenders with the tools to counter some of the most persistent and evolving threats. Regular, constructive sharing of CTII is believed to enhance collective defence, enabling more effective responses to emerging cyberthreats.

Challenges

Creating cyber defence coherence across Canada's numerous individual networks through community-wide CTII sharing presents a significant challenge. Considerable time and effort have already been invested in developing CTII-sharing mechanisms in the country. The CCCS, part of the Communications Security Establishment, plays a key role in this effort by sharing CTII with a diverse range of network defenders. As Canada's national technical authority for cybersecurity and cybersecurity emergency response teams, the CCCS is tasked with protecting the country's critical networks.

Additionally, a growing number of Canada's critical infrastructure sectors have established their own information-sharing mechanisms to distribute timely CTII among their members. The Canadian Cyber Threat Exchange (CCTX), a not-for-profit, cross-sectoral CTII-sharing hub operational since 2017, provides its members with detailed insights into cyber events affecting Canadian businesses and offers tools for threat mitigation. Major cybersecurity service providers, such as Microsoft, Palo Alto and Cisco, also contribute advanced CTII sharing.

Despite these efforts, gaps and limitations in CTII sharing persist, in particular for communities such as municipalities, small and medium-sized businesses, and Indigenous groups. Addressing these challenges is central for enhancing Canada's national cyber-defence capabilities. This issue was a key focus of the workshop and discussions at WSD 2024.

Despite these efforts, gaps and limitations in CTII sharing persist, in particular for communities such as municipalities, small and medium-sized businesses, and Indigenous groups.

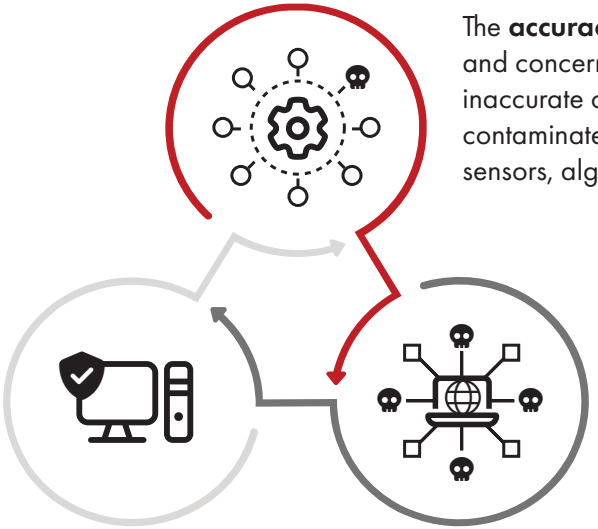
Consultation Takeaways

Drawing on the consultation sessions, participants agreed that Canada would benefit from a more effective and efficient CTII-sharing framework that includes all network defenders across the country. They identified several obstacles that may hinder broader CTII sharing:

- **Trust in the CTII-sharing process:** Participants noted that one of the most pressing concerns related to sharing CTII is about maintaining confidentiality around specific aspects of a cyber incident and the risk of losing control over the compromise narrative.

  Participants expressed varying degrees of trust in:

The **accuracy** of the CTII shared and concerns that the distribution of inaccurate or incomplete CTII will contaminate or mislead defence sensors, algorithms and analysis.



The ability to **protect** CTII containing sensitive and proprietary information, leading to misuse and harm (for example, privacy breaches, lost competitive advantage) throughout the sharing cycle.

The **security** of the channels used to share CTII being sufficiently resistant to external interference and tampering.

- **Ease of engagement and cost-efficiency:** Federal and provincial governments are well placed to facilitate community-wide sharing (subject to having the appropriate legal authority to do so), but private sector organizations are often reluctant to share CTII with federal partners because the process is unclear or cumbersome — there is no single window to report incidents or share CTII. In addition, government agency requests to victim organizations are poorly coordinated and often duplicative, creating fatigue and resentment within victim organizations.

  Adding to the difficulty in collaborating on CTII-sharing opportunities is the fact that non-disclosure agreements (NDAs) and information-sharing agreements (ISAs) are challenging to construct and difficult to

harmonize. Concerns about being unable to establish clear rights and obligations that will protect their interests around the information that others would benefit from accessing, make organizations reluctant to share CTII beyond the circle of those involved in mitigating an incident. Sometimes, the sharing of CTII relevant to an incident is expressly precluded in cyber insurance and managed service provider (MSP) contracts, unless victims obtain pre-approval to share the information from those hired to manage the incident before sharing the CTII.

A lack of standardized sharing processes and common data formats leaves some network defenders having to "translate" IOCs before ingesting them in their cyber-defence platforms. Many network defenders protecting the information infrastructures of under-resourced municipalities, small businesses and Indigenous communities are not able to afford to benefit from key threat-tracking tools provided by popular commercial cybersecurity platforms.

- **A clear value proposition supporting CTII sharing:** Attention must be paid not just to the benefits of CTII sharing, but also to the cost of not sharing CTII more widely. Many organizations are frustrated by a lack of feedback from those with whom they share CTII. This was particularly a concern among many participants when it came to sharing CTII with federal government organizations. This left many CTII sharers wondering whether the act of sharing creates unwanted business and operational risks without generating much benefit. Victims who feel uncertain about the usefulness of sharing are disincentivized to continue making the effort to share.

  The absence of an agreed-upon value proposition for CTII sharing and a lack of buy-in from private sector C-suites make community-wide CTII sharing a hard sell. There is a pressing need to raise the cyber literacy of those on corporate boards and in C-suites, and this cyber literacy needs to include an understanding of the value of wide CTII sharing. Corporate boards need to understand how community-wide CTII sharing will positively impact their business interests and benefit their customers.

- **There are legal concerns that inhibit community-wide CTII sharing:** All organizations in Canada must carefully manage personal information collected according to requirements set out in the Personal Information Protection and Electronic Documents Act or the Privacy Act. Accounting for the sharing of CTII

that contains personal information under data protection legislation in Canada has proven to be challenging given the difficulty in obtaining express, informed consent from all network users and the fact that neither the implied consent construct nor the existing exceptions for sharing without consent are likely to be applicable in most situations.

The unauthorized sharing of privacy-sensitive or identifying information in shared CTII can give rise to allegations that data privacy regulations have been breached or trigger private litigation. Companies operating in Canada and the United States may refrain from sharing critical CTII within Canada due to concerns about civil liability but are prepared to do so in the United States, where legal protections for sharing CTII with government and the private sector have been established.

Moving Forward: Recommendations Related to Community-Wide CTII Sharing

Provide legal mechanisms to account for privacy and data protection obligations:

- Develop comprehensive legislation to enable community-wide sharing of CTII in Canada. This legislation would authorize CTII sharing under relevant data protection legislation, remove legal liability from sharing CTII, maintain existing legal privileges attached to shared CTII, and exempt shared CTII from relevant access to information and privacy legislation and unfair competition provisions.
- Draw on emerging "privacy-enhancing technologies" to address concerns about protecting privacy-sensitive and personal identifying information in shared CTII.
- Explore the potential for more robust CTII sharing through a draft code of practice for community-wide CTII sharing and consult with Canada's federal and provincial privacy commissioners on how to improve the draft. Although Canada's privacy legislation does not yet recognize codes of practice (such an authority is contemplated in Bill C-27), the process of designing a code of practice for community-wide CTII sharing provides a useful opportunity to explore and better understand current concerns about CTII sharing and how those concerns could be addressed.

Foster trust in the process:

- Standardize the wording of legal CTII-sharing agreements (NDAs and ISAs) to encourage CTII sharing and remove impediments to CTII sharing in MSP and cyber insurance contracts in a way that addresses the interests of all parties involved in mitigating a cyber incident.

- Anonymize or de-identify the source of the CTII being shared to reassure organizations that sharing CTII does not increase the risk of harm to their business and operational interests.
- Develop a clear value proposition for CTII sharing, demonstrating how it benefits the entire community through both reactive sharing of newly identified threats and proactive dissemination of trends and forecasts.
- Create a cybersecurity review body (such as the US Cyber Safety Review Board or Canada's Transportation Safety Board) charged with reviewing significant cyber compromise events and extracting key lessons learned for the community.

Make the process for sharing CTII as easy and cost-efficient as possible:

- Create financial incentives and legal immunities that are capable of encouraging CTII sharing.
- Develop a standardized taxonomy for CTII incidents and a universal data format that will allow network defenders to easily ingest IOCs for use in commercial security platforms such as Microsoft Defender.
- Create a central architecture for sharing CTII that provides streamlined, single-entry processes for sharing CTII with government agencies; establishes formats that are easily ingested and acted upon by the full range of network defenders in Canada; as well as promulgates rules governing further distribution of CTII that has been shared. CCTX's Data Exchange offers a potential model for constructing this kind of centralized architecture.
- Establish a mechanism to assist network defenders in under-resourced municipalities, small businesses and Indigenous communities in meeting the costs involved when enabling the key threat-tracking tools provided by popular commercial cybersecurity platforms.

Cybersecurity Talent and Skills

The cybersecurity talent challenge is urgent and complex, spanning a wide range from enhancing cyber hygiene among Canadians in general, and for students and employees to offering advanced education for cybersecurity professionals and supporting cutting-edge research into modern cyberthreats and solutions. Despite Canada's early and enthusiastic adoption of information technology and the internet, many Canadians still need regular reminders about the importance of robust cybersecurity practices. Implementing even basic measures at an individual or organizational level could prevent or mitigate many of the cybersecurity incidents currently impacting the country.

Value Proposition

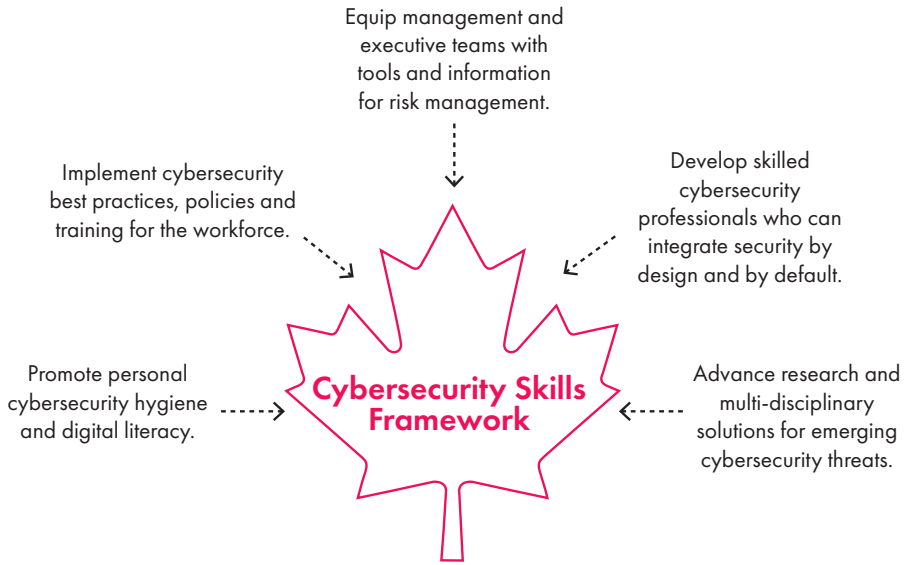
The demand for more and better cybersecurity talent remains intense, starting with preparing Canada's education system to be equipped to produce technical experts skilled in integrating security into systems that are increasingly powered by generative artificial intelligence (AI) and filled with sensitive personal, financial and proprietary information. Additionally, cybersecurity professionals with specialized skills are needed to provide round-the-clock protection against service interruptions, privacy breaches and catastrophic failures.

Simultaneously, enhancing personal cybersecurity training can reduce mistakes in the workforce and improve protection for employer systems and sensitive data, such as medical records and financial information. Early cybersecurity awareness for children can also develop their online instincts and resilience against various online threats, including disinformation, fraud, sexual exploitation and bullying. Cyber-smart children are more likely to grow into cyber-savvy adults who apply their knowledge effectively in higher education, the workplace and executive decision-making roles.

Challenges

As the global cyberthreat landscape grows, it is important to enhance cybersecurity skills across all levels, from young Canadians to seasoned professionals and leaders.

Canada's cybersecurity skills framework must be holistic and include programs to:



WSD 2024 aimed to address the challenge of preparing future cybersecurity professionals while also highlighting the broader need for cybersecurity awareness and talent. It is evident that significant efforts are needed to organize curricula, incentivize study, and recruit students, educators, employers and researchers to meet the growing demand for cybersecurity expertise and address emerging threats.

Consultation Takeaways

Through consultations[3] in recent months, participants were keen to point out promising initiatives geared toward generating cybersecurity talent and onboarding graduates into meaningful employment. There is frustration, however, that these examples are not systemic or do not scale nationally, leaving large parts of the country without the talent needed to design, operate and maintain the security of vital online systems. Much of the feedback from participants was anecdotal and focused on applied skills as there is insufficient data to diagnose most national trends.

Their collective experience highlighted the following:

- **Canada must adopt a more coherent and consistent approach to addressing the cybersecurity talent challenge:** A comprehensive Canadian cybersecurity education and training strategy should establish clear national-level goals. Given the complexity and scale of the issue, it is essential to involve a team of trusted experts and thought leaders from employers, educators and government in both the development and implementation of the strategy. This collaboration will also help assess demand, create programs to generate the necessary talent, and enhance efforts to develop, retain and upskill cybersecurity professionals.
- **Employers are increasingly seeking experienced technical professionals with expertise in specialized areas:** Participants expect this trend to continue, with growing demand for individuals skilled in emerging technologies such as cloud computing and AI. Conversely, automated processes are reducing the need for

3 In May 2024, CIGI and the Rogers Cybersecure Catalyst co-hosted a workshop in Toronto with experts from academia, cyber ranges, government, law enforcement, businesses, not-for-profit organizations as well as other consultations with Indigenous organizations and privacy commissioners. In June 2024, workshops and discussions with WSD participants focused on refining recommendations related to cybersecurity skills.

some entry-level cybersecurity positions, leading to fewer opportunities for those looking to reskill for these roles.

- **Encouraging continuous learning and upskilling in cybersecurity:** Participants emphasized the need for improved skills across the broader Canadian cybersecurity ecosystem, not just for new professionals with advanced technical skills. They stressed the importance of enhancing cybersecurity awareness, especially among C-suite executives, senior decision makers and those managing organizational risk, through national public information campaigns. Additionally, it was discussed that there seems to be insufficient financial or other incentives for individuals to invest in upskilling or cross-training in cybersecurity or other technical fields throughout their careers.
- **Early introduction and continuous development of cybersecurity education:** There is a compelling case for proactively addressing the ongoing cybersecurity talent shortages by introducing national cybersecurity programming in early elementary school. As students advance through their education, the instruction can become increasingly difficult. Implementing nationwide cybersecurity courses in high schools can provide a head start for students pursuing technical post-secondary programs, such as at universities and colleges. Furthermore, work-based apprenticeship programs could be offered to high school graduates, allowing them to gain valuable experience through on-the-job training.

Moving Forward: Recommendations Related to Cybersecurity Talent

Implement a national cybersecurity education strategy:

- Collaborate across jurisdictions and sectors to develop a national cybersecurity talent pipeline that accounts for specialists, business professionals, general workforce, educators, students and the Canadian public.
- In collaboration with provincial apprenticeship authorities, introduce an apprenticeship model that provides opportunities for a broad range of motivated individuals to pursue cybersecurity careers even without post-secondary education.
- In addition to the recommendations listed below, consider:
  - intensifying current federal cybersecurity awareness campaigns (for example, in the manner of Canada's Food Guide campaigns) for the Canadian public;

- creating a corps of “cybersecurity reservists” for acute skills gaps, and the exchange of talent between the private and public sectors, as well as fractional employment models to apply top talent in times of crisis or intractable challenges; and
- aligning cybersecurity research chairs to optimize connections and the potential of their research programs.

Introduce formal cybersecurity education at the earliest opportunity, and throughout primary and secondary education programs:

- Create a national cybersecurity education program for children aimed at improving their understanding of and ability to maintain good cybersecurity hygiene.
- Work with provincial ministries of education to integrate cybersecurity and cyber safety as a life skill into the K–6 curriculum. This may also help generate interest among traditionally under-represented groups and girls in pursuing technical and cybersecurity careers.
- Work with provincial ministries of education to continue development and integration of cybersecurity into high school (grades 9–12) curriculum, introducing more technically sophisticated courses that serve as prerequisites for apprenticeship opportunities or to give a head start to those entering post-secondary streams.
- Increase the number of trained elementary and secondary school educators by incentivizing them to gain the knowledge and experience to teach basic programming or advanced courses.

Evolve a cybersecurity talent pipeline fit for the future:

- Gather statistics regarding current and future competency requirements and projected talent gaps — for both students and educators.
- Set and regularly update a common national curriculum that can be used by primary, secondary and post-secondary instructors.
- Create a framework of grants, contributions and incentives to increase the pool of both students and educators in cybersecurity.

- Set national goals for diversity within the cybersecurity profession and sustainable programs for generating talent by tapping into immigration processes and other representative talent pools.
- Require training on foundational cybersecurity, cyber resilience and “security by design/default” for any academic field of study developing internet-facing technology.
- Promote open-enrolment cybersecurity courses and integrate cybersecurity training into all academic disciplines; encourage interdisciplinary (legal-policy-technology) collaboration for advanced problem solving.
- Stand up a national association of cybersecurity professionals and solicit their ideas on developing talent for future challenges.

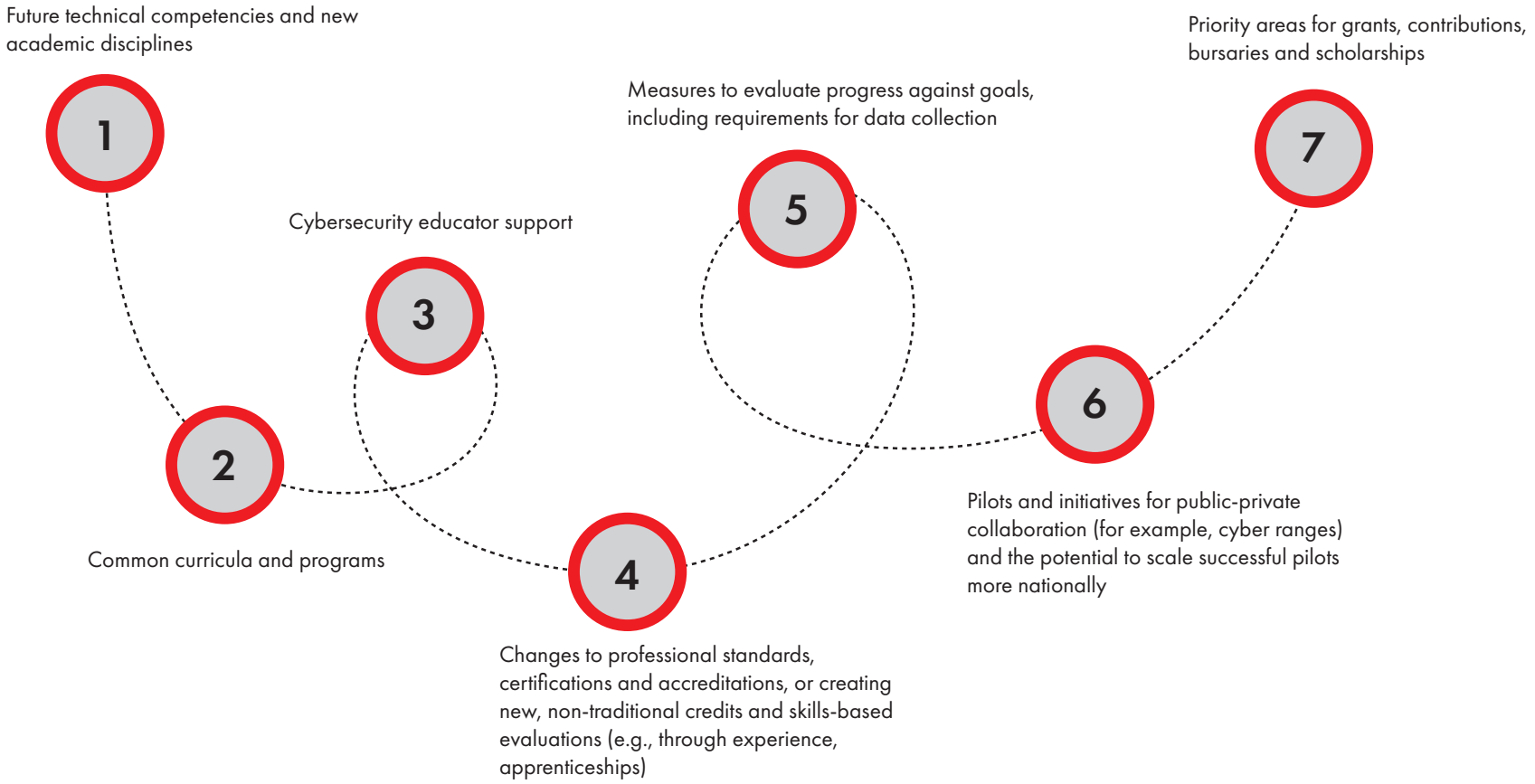
Increase private-sector-academic partnerships in the skills ecosystem:

- Working with professional standards bodies and associations, identify and integrate cybersecurity requirements into Canadian professional and licensing standards where appropriate.
- Use regional hubs to link universities, colleges and schools developing applied cybersecurity talent. Pair with employer organizations that can provide practical experience and/or apprenticeships through on-the-job coaching with cybersecurity professionals.
- Stand up new private-sector-academic partnerships as cyber ranges in key regions to maximize hands-on academic experience, share libraries and research projects, and model threats and exercise plans.
- Provide incentives for private sector organizations that commit to effective onboarding and continuous development of cybersecurity professionals throughout their careers.
- Recognize excellence in cybersecurity education, training and related initiatives through national public-private awards.

Promote open-enrolment cybersecurity courses and integrate cybersecurity training into all academic disciplines.

Enlist a national cybersecurity talent advisory circle:

- Solicit advice and guidance on the implementation of the national talent strategy, in particular on matters requiring national policy coherence, coordination and/or consistency, such as (but not limited to):



- Engage a core team of cybersecurity experts from industry, academia and government who are thought leaders and committed to shaping Canada's future cybersecurity talent landscape.

Next Steps

The conference discussions represented a significant step in gathering and exploring diverse ideas to address the concerns of today's network defender community. There is no easy solution to these cybersecurity challenges, which can, given their scope and scale, feel intractable. Some of these recommendations have been raised before. Others are new. More are needed.

Taken together, and with intensified cooperation and incremental implementation, Canada can continue to evolve an effective framework for cybersecurity and strengthen cyber resilience on local and national scales.

By engaging the entire Canadian cybersecurity ecosystem, Canada comes closer to the vision laid out at the beginning of this report and the greater benefits of enhanced prosperity, competitiveness, security and safety. The WSD serves as an important platform for leaders across Canadian jurisdictions and sectors to collaborate in this iterative solution space.

Much work remains, however, and in the coming months, CIGI will continue to engage with community stakeholders. The focus will be on further exploring some of these recommendations to strengthen Canada's cybersecurity posture and promote collaboration among the various levels of government, the private sector and Indigenous communities on cybersecurity initiatives.

Acknowledgements

We would like to thank everyone who attended this year's WSD and the series of workshops hosted by CIGI before the conference. Your valuable contributions are sincerely appreciated. We also express our gratitude to Brent Weberg, Ian Paterson, Charles Finlay, Emily Laidlaw, Robert Gordon, Adam Kardash and Vern Crawley for their help in preparing this report.

Acronyms and Abbreviations

AI	artificial intelligence
CCCS	Canadian Centre for Cyber Security
CCTX	Canadian Cyber Threat Exchange
CTII	cyberthreat information and intelligence
IOCs	indicators of compromise
ISAs	information-sharing agreements
MSP	managed service provider
NDAs	non-disclosure agreements
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