TRIPLE HELIX

Charting Canada's Digital Ambition

By Abigail Dyer and Érika Dupuis

November 2025

CONFERENCE REPORT

CHARTING CANADA'S DIGITAL AMBITION

by Abigail Dyer and Érika Dupuis

November 2025

Prepared for Triple Helix for the Canadian Global Affairs Institute
Suite 2720, 700 – 9th Avenue SW., Calgary, AB T3P 3V4
www.cgai.ca/triple_helix

On September 16, 2025 the Triple Helix Minds Collaborative Network – a partnership between the Canadian Global Affairs Institute, NPSIA at Carleton University, and industry organized a conference on Canada's digital ambitions. This report provides a summary of the discussions held throughout the day.

Introduction

Canada stands at an emerging technologies crossroads, and the next decision our government makes will determine our ability to leverage these technologies to deliver world class citizen services in addition to better enabling our national security objectives. Around the world, the private sector is embracing digital transformation at an unprecedented pace. For Canada, achieving this same momentum demands not only modern capabilities, but also broad and coordinated government change. With new government leadership, the time for action is not just approaching—it has arrived. Change must happen, but more importantly, conditions are aligned for it to succeed. This conference examined the barriers to this much needed change but also charted the way forward for Canada to harness advanced technologies to realize the government's digital ambitions. The goal of the day was to identify concrete, actionable policy recommendations that can transform this momentum into measurable progress. We were honoured to welcome high-level government and defence officials, as well as thought leaders from academia and industry, who guided us through the day's discussions.

Keynote 1 – Canada's Digital Ambition

The conference started with The Honourable Jenna Sudds, Parliamentary Secretary to the Minister of Government Transformation, Public Works and Procurement and to the Secretary of State for Defence Procurement.

She recognized of the important role that digital will have in the realization of our nation's full potential. Specifically, the Government of Canada has made it clear that digital transformation—redefining the culture of government in partnership with the public sector—is a central priority. To succeed, Canada must ensure that the necessary skills and processes are firmly in place. Our systems must be modern, secure, and fully operable. Public servants must be equipped with appropriate training, and the ethical management of data, and its communication, must remain paramount. At the Edmonton meeting of the Liberal Party of Canada's caucus, Prime Minister Carney had announced a major step forward: the development of a sovereign cloud. This is more than an infrastructure project; it represents a reclaiming of control over Canada's data in order to safeguard both citizens and corporations against escalating cyber threats.

Realizing this vision will require a collective effort from researchers, public leaders, policymakers, and decision-makers. Canadians have expressed strong support for investments in digital resilience, cyber defence, and national security. Yet despite the government's ambition, important

challenges remain. Legacy systems must be modernized or replaced, and public servants must be retrained and recruited to meet new demands. Industry partnerships will be essential in bridging gaps and accelerating progress. At the same time, the digital divide across Canada must be addressed to ensure equitable access for all citizens. Breaking down interdepartmental silos will be crucial, and issues of privacy and ethics must remain at the forefront.

Panel 1: Assessing Canada's Government Digital Posture

Moderator: Vice Admiral (Ret'd) Ron Lloyd

Panelists: Marc Brouillard, PSPC; Derek Dobson, IBM; Lieutenant-Colonel Amanda Whalen, RCAF.

With the digital destination clearly articulated in the opening keynote, this panel examined Canada's current digital posture. The consensus was that there are numerous structural and cultural barriers preventing effective modernization, starting with "small p" policies (which are distinct from "Capital P" policies). "Capital P" policy refers to the high-level frameworks and strategies such as NATO targets and sovereign cloud initiatives. "Small p" policy, by contrast, exists in the form of thousands of non-legislated policies, guidelines, tools and directives within which government departments are required to deliver their mandates. It was noted that these policies were created under very different circumstances and often do not reflect the real-world risks Canada faces today. Because culture and policy are deeply intertwined, efforts to modernize frequently become stalled. Policies reinforce outdated cultures, and cultures resist policy changes. This dynamic creates a cycle of stagnation that has become increasingly dangerous in an era where adversaries are advancing rapidly in leveraging digital across the spectrum of national power including economic, diplomatic and defence and security initiatives.

From an industry perspective, it was emphasized the importance of adopting technological solutions not simply for efficiency, but for outcomes that enhance Canada's defence posture. Yet, it was also noted the hesitation within government to embrace decision-making at speed. This hesitation often results in missed opportunities, with benefits lost the risk of change is avoided. A vivid operational perspective was provided as one of the many examples where public service and defence leaders are trying to deliver digital outcomes but are constrained from outdated manual, waterfall, and numerous approval processes internal and external to their departments.

The panel highlighted systemic inefficiencies. For example, whereas allied nations are completing tasks in hours the CAF are taking months. The key takeaway being that for "Every single one of those days that we're spending navigating the bureaucratic process and waiting for someone to review something is a day that our allies and enemies are getting ahead of us."

Examples from the COVID-19 pandemic and Afghanistan illustrated both the potential and the limitations of Canada's current approach. During both of these crises, the government was able to demonstrate short-term successes. However, this agility was only possible because of the

emergency context. Without changing the underlying "small p" policy foundations, these successes are best described as false positives. Looking forward, the panelists agreed that policy changes are needed first and then once defined, organizational change should follow– embracing an adherence to the principle of "form follows function." Without reform, the government risks adhering to a status quo posture characterized by a culture of slow, compliance-driven processes that hinder the Canadian Armed Forces and the public service alike.

Another area of focus was procurement and innovation. Smaller Canadian firms often face significant barriers when bidding for government contracts. Large corporations frequently win contracts, only to subcontract to smaller players, shifting legal and financial burdens onto them. This practice stifles innovation, discourages new entrants, and undermines domestic competitiveness. The panel stressed the importance of creating clearer pathways for small companies to participate in procurement and scale their solutions. Aligning key performance indicators with mission-driven objectives, rather than compliance checklists, was proposed as one way to ensure procurement serves Canada's strategic needs. One of the major obstacles for smaller Canadian companies was Canada's overly risk adverse Contract Security Program requirements for unclassified procurements which are unique amongst our Five Eyes Partners.

Privacy and sovereignty also featured prominently in the discussion. It was noted that while Canadians already share sensitive data with banks and healthcare providers, government systems still rely on outdated methods such as fax and hand-delivered documents to transfer information. It was assessed that dated "small p" policies adopted in the pre-digital era constrain the government from leveraging modern digital technologies that Canadians use in their day to day lives. It was recognized that there has been much discussion about sovereignty very recently, however, panelists cautioned that not everything can be made sovereign; trade-offs are inevitable, and Canada must be prepared to operate with "sovereign autonomy" while ensuring its core objectives are never compromised.

Throughout this panel, trust was a recurring theme. For true transformation, trust must exist between government and the private sector, between policymakers and the armed forces, and between citizens and their institutions. Trust does not mean blind faith but rather the creation of frameworks that clearly define authorities, responsibilities, accountabilities, and ethical boundaries. It was reinforced that moving at the speed of trust is fundamentally a human endeavour, and that should not be confused with trusting the process, which is anything but.

Panel 2 - How Other No Fail Organizations Are Leveraging Digital

Moderator: Marc Watters, CADSI

Panelists: Caroline Cameron, Deloitte; Tim Gibel, SAP Canada; Robert Percy, CoLab

This panel explored how private sector organizations with "no-fail" missions—such as healthcare, supply chains, and critical infrastructure—are leveraging digital transformation, and what lessons government can draw from them.

Looking at key challenges and some misconceptions, they addressed how adopting digital systems in government differs sharply from the private sector. Panelists highlighted that misperceptions and rigid procurement processes often slow innovation. Private companies are more likely and need to accept risk more often as part of survival. The government, on the other hand, tends to eliminate and/or avoid risk, creating bottlenecks. This contrast makes it difficult for public institutions to adopt flexible and mission-driven digital strategies.

One risk mentioned as a central theme for the government was the adoption of cloud. Many businesses are already deeply integrated into the cloud, including mission-critical operations such as organ transplant logistics. For the Canadian government, however, issues with respect to security considerations and recently, conversations about sovereignty complicate cloud adoption. One framework discussed was measuring cloud sovereignty across four dimensions: data, technical, legal, and operational. Canada, once a leader in digital transformation, has fallen behind due to risk aversion and slow investment. Panelists argued that sovereignty *can* be achieved in Canada, provided there is clarity in expectations and frameworks that balance security, privacy, and innovation.

Drawing back on the previous panelists and the discussion around the relationship between "small p" policy (operational frameworks) and "Capital P" Policy (government-level direction), it was related to risk and the different ways "Capital P" and "small p" policy play a role. In government, "small p" policies are often rigid and risk-averse, whereas the private sector treats risk as unavoidable. This cultural divide creates delays; thousands of compliance checks, lengthy procurement processes, and legacy system dependence all prevent timely innovation. Panelists suggested reducing unnecessary "gates" in approval systems and focusing instead on outcome-driven assessments.

Trust emerged as another key factor. In the private sector, certifications and self-vetting often suffice to establish confidence. Governments, however, struggle with balancing trust and control. Panelists noted that Canada should leverage existing models, such as the U.K.'s cloud adoption strategy, to accelerate progress. Stronger collaboration between public and private actors, particularly in setting standards and experimenting with pilot projects, could help bridge the current divide.

Technology will continue to reshape the workforce, particularly with the rise of AI. To succeed, the government must align policy and culture with innovation. Without cultural change, new

policies will stall, and without updated policies, innovation cannot take root. The panel concluded with cautious optimism: while Canada faces barriers of bureaucracy, sovereignty, and risk aversion, these challenges can be overcome by embracing innovation, clarifying goals, and fostering partnerships that prioritize outcomes for citizens over rigid processes.

Keynote 2 - Digital Transformation: Operational Advantage in a Complex World

Lieutenant-General Steve Boivin, Commander, CJOC

LGen Steve Boivin emphasized the critical role of digital transformation in shaping the future of the Canadian Armed Forces (CAF) and enhancing operational effectiveness across multiple domains. Collaboration with industry partners, including from the Five Eyes, is essential to achieve mission outcomes, accelerate decision-making, and maintain strategic advantage. Speed, agility, and digital fluency were highlighted as core priorities, particularly in high-risk and congested operational environments.

CAF operations rely on robust C4ISR systems—integrated networks that support command, control, communications, computers, intelligence, surveillance, and reconnaissance. These systems enable real-time situational awareness, improved decision-making, and resilience across five domains: space, cyberspace, air, land, and maritime. Digital technology is leveraged to counter domain-specific threats such as cyberattacks, satellite disruption, disinformation, and adversarial military advancements.

Key operational priorities include the defence of North America (particularly the Arctic), Europe (including NATO commitments), the Indo-Pacific region, and global contingencies. At home, CAF supports domestic operations like forest fire response (Operation LENTUS) and Search and Rescue missions. Internationally, CAF contributes to NATO missions, multinational brigades, and training for allied forces such as Ukraine, enhancing self-defence capabilities and interoperability.

He specifically identified three conditions for success for the CAF to succeed in their digital journey:

1. *Leadership, Unified Understanding and Vision*. A clearly articulated CAF vision to all stakeholders to set the conditions to move the force from analogue to digital by design. The efforts must be command-led, and they must encourage their subordinates to operate at pace and scale noting it will be uncomfortable for some. Finally, to achieve these outcomes authorities should be delegated to the lowest level possible.

2. *Culture and Prioritization*. Innovation should not be seen as a risk but a requirement for operational relevance. Digital transformation must be owned by the chain of command in the CAF and the senior executives in Defence. Accountabilities and risk acceptance must be with commanders and not staffs. At all echelons digital training and education must evolve to raise the levels of digital literacy in the CAF.

3. *Policies*. Traditional process-based procurement models are too slow for the pace of digital innovation required and there is a requirement to transition to more outcome-based models that enable continuous capability evolution. "Small p" policies put in place decades ago in some cases must be reviewed to ensure Canada has the right security classification framework, up-to-date IT security risk management policies and procurement policies.

LGen Boivin concluded that the CAF's digital transformation is framed not as a buzzword, but as an imperative to achieve operational effectiveness, enhance interoperability, and build a future-ready military. This is our moment to align on economy, sovereignty, and defence. Canada has the talent, the technology, and the ambition. Our government ought to bring them together in order to generate the unity of digital thought, purpose, and action needed to put the CAF and Canada at the forefront of other modern digital nations.

Panel 3 - Setting the Conditions for Success

Moderator: Brigadier-General (Ret'd) Chris Ayotte, AWS

Panelists: Nutan Behki, SSC; Mel Crocker, Air Canada; Jody Thomas, former National Security and Intelligence Advisor to the Prime Minister.

The session emphasized the critical steps necessary for Canada to achieve its digital ambition, particularly in the government and defence sectors. Speakers highlighted that while the path to digital transformation is clear, implementation is complex and requires strong leadership, accountability, and strategic partnerships. Canada faces a digital lag due to historical reliance on analog systems, fragmented governance across multiple departments, and insufficient investment in both technology and defence infrastructure.

Panelists emphasized that the speed and effectiveness of modern operations depend on information flow. Canada must prioritize digital readiness to catch up with global peers, requiring investment in technology, infrastructure, and defence spending. It was also noted that while Canada possesses talented personnel, obstacles such as bureaucratic procurement requirements and a lack of government-business partnerships hinder progress. It was also noted that agility is essential: organizations must move quickly, make sound decisions, and avoid breaking critical systems.

Key strategies include enhancing digital literacy among leaders, clarifying accountability, and fostering a culture that embraces risk responsibly. Effective digital transformation requires understanding the problems to be solved, leveraging individual strengths, and flattening hierarchical structures to improve communication and accountability. Political, operational, and technological risks must be recognized and managed, rather than ignored or oversimplified.

Panelists stressed the importance of honesty and transparency in project management. Acknowledging failures and being truthful about progress allow organizations to adapt and improve. Incentive structures and hiring practices should reward success, innovation, and risk-taking. Flattening organizational hierarchies, appointing specialists as leaders, and prioritizing mission-critical objectives were highlighted as essential for sustainable digital transformation. Overall, achieving digital success requires a clear vision, empowered leadership, strategic risk management, and a willingness to challenge the status quo across both government and industry.

Fireside Chat- Seizing the Opportunity

Moderator: Dave Perry, CGAI

Panelist: Bill Matthews, Secretary of the Treasury Board

The session explored how Canada's government, under Prime Minister Carney's leadership, is approaching defence procurement, fiscal management, and digital transformation. With new ministers and clerks alongside returning officials, the government is in the early stages of setting priorities, but a clear interest in acting quickly is evident. However, the longstanding bias toward "figuring everything out before launch" often slows progress. An approach of launching with the minimum necessary and adjusting along the way to accelerate results and tackle problems as they arise is the current orientation.

A key theme was risk management. Government often delegates tasks or reduces back-office functions to limit risk, yet this conservative approach can also hinder innovation. Treasury Board policies were highlighted as both a tool and an obstacle; while policies are preapproved, changes or exceptions—particularly in areas like cyber and AI—require quicker, more flexible decision-making. Departments are experimenting with AI, but current registries lack clarity on scope, goals, and outcomes, raising concerns about oversight and efficiency.

Defence procurement remains a pressing challenge. Canada must balance industrial strategy, trade diversification, and military readiness while ensuring transparency in spending. The discussion emphasized that procurement issues are complex and cannot be reduced to a single problem. Overly rigid processes, technical merit dilution, and insufficient human resources strain the system, with staff often overworked to meet ambitious timelines. Greater flexibility, earlier involvement of multiple departments, and a willingness to prioritize key needs over exhaustive details were discussed as considerations for the way forward.

Fiscal accountability and transparency remain priorities, but questions persist about whether government spending reports and classifications—such as definitions of capital investment—are serving their purpose effectively. While transparency to Parliament is necessary, current processes consume extensive resources and may require modernization.

Ultimately, Canada must embrace a more flexible, risk-tolerant approach to procurement and spending, particularly in defence. By streamlining processes, adopting best practices, and enabling quicker decision-making, the government can better support national defence and economic priorities while delivering value to Canadians.

Recommendations

Across all discussions, one theme was clear: Canada cannot afford to delay digital transformation. The following recommendations are provided to accelerate the realization of that outcome.

1. **Modernize Risk Management Frameworks:** Canada should shift from a risk-avoidance to a risk-balanced model by reforming policies. Conduct a full "small p" policy review (non-legislated policies, directives, guidelines, security guidance, etc.) to enable a transition from pre-digital manual, paper-based, waterfall processes to modern digital enabled processes and procedures. The three policies that would need to be amended to enable this outcome are amending the classification framework to reflect the same level of injury of our NATO and Five Eyes Partners, rescinding the Harmonized Threat and Risk Assessment Methodology (TRA-1) and consolidating IT Security Guidance into a single document to replace IT Security Risk Management: A Lifecycle Approach.

2. **Initiate a Government–Industry Digital Partnership:** Canadian sovereignty across the digital enterprise is unrealistic. However, there are key aspects of the digital enterprise such as in cloud and AI where Canada would be wise to achieve Sovereign Autonomy. The AI sprint kicked off by Minister Solomon is an important first step to understanding the end-state. It is recommended that a government-industry working group be stood up and given a work plan that reports progress quarterly to inform key aspects such as IP, enabling Canadian SMEs, and specific aspects of the digital ecosystem. Organizations such as CADSI would be ideal to represent the interests of Canadian industry.

3. **Enabling Defence:** The fact that the Canadian Armed Forces' command and control of operations has not fundamentally changed in the last 20 years, and the numerous internal and external processes required to implement simple yet extremely relevant mission applications for the Services reflects a lack of enablement of the Defence digital enterprise. It was understood that Shared Services Canada was created to more cost effectively manage the government's IT portfolio. However, the unintended consequences of putting at risk the force generation and force employment of the CAF on missions assigned by the Government of Canada are untenable. As the CDS/Deputy Minister of Defence own this risk they should be empowered with the authorities and accountabilities to manage all aspects of their digital portfolio. The only dependencies that Defence should have on SSC are those that they choose to have.

4. **Strengthen Trust and Accountability Frameworks:** Develop clear, transparent frameworks that define responsibility and accountability for digital and security initiatives shifting to *speed of trust*; from focusing on process speed to empowering decision-makers and reducing reliance on rigid compliance checks. To achieve this outcome treating all government departments the same is not helpful as their requirements are different. Digital policies need to be tailored to recognize these differences. National security and defence departments, academia and research departments, and citizen service departments have unique digital requirements that need to be reflected in the government's digital policy suite. The current plan to update Canada's Digital Service Policy would be the ideal time to highlight these important differences.

5. **Institutionalize Continuous Learning and Cultural Change:** It was highlighted that there is a lack of digital literacy across government and particularly at the executive level. Making informed decisions about IT has become problematic. With online coursing as sophisticated as it is today and recognizing that in private industry there are requirements for senior executives to keep pace with technological advancements, it is recommended that a course be tailored for all executives in the public sector and completion be a performance management appraisal.

6. **Enabling Third Parties:** A recurring theme during the day was the Government's inability to trust internationally recognized third parties in keeping with our NATO partners. The Canadian government's misplaced belief that they need to be the "authority" for managing low risk activities whether in procurement or security results in government risk managing low- to high- risk activities because of a lack of capacity. Examples include managing all security statuses/clearances and security and accreditation of software solutions that have been certified by third parties in service with our allies yet do not meet the bespoke Canadian requirements. In some instances, Canadian companies are paying literally millions of dollars for independent third-party security and accreditation as directed by the Canadian Cyber Security Centre only to have the certification challenged by a line department. Canada needs to revisit the Contract Security Program and align the Designation Organization Screening (Protected A and B procurements) requirements with our NATO and Five Eyes partners. In addition, a policy identifying independent third-party certifications as the standard for line departments to accelerate the change in culture is recommended.

7. **Informatics Procurement:** To note that procurement challenges were a recurring theme during the day would be an understatement. It was recognized that the ArriveCAN application fallout would only further exacerbate digital procurements. The shortcomings identified by the Office of the Auditor General and attributed to the CBSA, PSPC and the Public Health Agency in the delivery of the ArriveCAN application are indisputable. Unfortunately, their recommendations apply to the existing policy paradigm. PSPC's most recent amendments to the existing procurement vehicles underscore this point.

Although a professional services contract was used in the ArriveCAN application, it is essentially the same format as a Task-Based Informatics Professional Services (TBIPS) contract. What has been lost on most is that when TBIPS was introduced in 2006, the belief was that by leveraging the best practices of large private sector firms $2.5 billion in savings could be realized over five years. This would be accomplished by saving 10% in prices paid by government, realize 10% in procurement efficiencies, and reduce the time to complete procurement by 50%. Although the cost savings were quickly abandoned as not being realistic, TBIPS and eventually SBIPS were and still are the informatic procurement vehicles. If government is to address digital procurement challenges it needs to abandon TBIPS and SBIPS and recognize that the digital landscape has evolved so much that they need to define new digital procurement vehicles that reflect industry and other nation's best practices. Tinkering with decades old approaches to procuring digital services is not what right looks like in 2025.

Canadian Global Affairs Institute

The Canadian Global Affairs Institute focuses on the entire range of Canada's international relations in all its forms including (in partnership with the University of Calgary's School of Public Policy), trade investment and international capacity building. Successor to the Canadian Defence and Foreign Affairs Institute (CDFAI, which was established in 2001), the Institute works to inform Canadians about the importance of having a respected and influential voice in those parts of the globe where Canada has significant interests due to trade and investment, origins of Canada's population, geographic security (and especially security of North America in conjunction with the United States), social development, or the peace and freedom of allied nations. The Institute aims to demonstrate to Canadians the importance of comprehensive foreign, defence and trade policies which both express our values and represent our interests.

The Institute was created to bridge the gap between what Canadians need to know about Canadian international activities and what they do know. Historically Canadians have tended to look abroad out of a search for markets because Canada depends heavily on foreign trade. In the modern post-Cold War world, however, global security and stability have become the bedrocks of global commerce and the free movement of people, goods and ideas across international boundaries. Canada has striven to open the world since the 1930s and was a driving factor behind the adoption of the main structures which underpin globalization such as the International Monetary Fund, the World Bank, the World Trade Organization and emerging free trade networks connecting dozens of international economies. The Canadian Global Affairs Institute recognizes Canada's contribution to a globalized world and aims to inform Canadians about Canada's role in that process and the connection between globalization and security.

In all its activities the Institute is a charitable, non-partisan, non-advocacy organization that provides a platform for a variety of viewpoints. It is supported financially by the contributions of individuals, foundations, and corporations. Conclusions or opinions expressed in Institute publications and programs are those of the author(s) and do not necessarily reflect the views of Institute staff, fellows, directors, advisors or any individuals or organizations that provide financial support to, or collaborate with, the Institute.