August 2026 – Issue 7

Policy Forum

What security benefits or risks should the Government of Canada consider when thinking about AI?

Policy Forum Politique is a publication format that aims to stimulate debate by presenting a wide range of expert opinion on a topic of national security significance to Canada. For this seventh edition, we ask four experts for their perspectives on the following question: *In June 2026, Canada unveiled its new artificial intelligence (AI) strategy. Although the strategy makes much mention of the economic benefits that come with adopting AI, it is silent when it comes to security or military considerations despite calling for certain sovereign capabilities. What security benefits or risks should the Government of Canada consider when thinking about AI?*

Matthew da Mota | Canadian Shield Institute

Matthew is Research Director, Emerging Technology and National Security at the Canadian Shield Institute. His research examines how emerging technologies and shifting geopolitical dynamics reshape governance, knowledge, and sovereignty — with a particular focus on the national security implications of AI and digital infrastructure.

Canada's new AI strategy promises opportunity and calls for sovereign capabilities, but it treats sovereignty as an industrial question with focus on compute, chips, models, and data centres. That perspective mistakes ownership for control. The sovereignty that matters is epistemic, and it rests on governance: the capacity to set terms on how AI enters the institutions that hold Canada's knowledge, and to preserve the human judgment that verifies the quality of that knowledge.

Generative AI erodes both. Disinformation and deepfakes are cheap to produce, individuals can retreat to private sycophantic feedback machines, and poisoning a widely used AI model takes startlingly few malicious inputs. Trust in information itself is at stake. An adversary need not defeat Canada on some AI-enabled battlefield; it need only make Canadians distrust their own knowledge. Yet the models upon which this environment depends with a few foreign, private firms, outside of Canadian governance. More sovereign compute would not change that.

The military is not exempt. As AI is introduced into the decision loop, it has the potential to degrade the judgment it is meant to support through bias, skills atrophy, and blurred accountability when decisions are informed, or made, by non-human actors.

An even deeper danger is succumbing to the temptation to replace hard-won, tested knowledge systems with automated ones before we grasp what we are trading away. Compounding this problem is how we do not understand how AI will reshape the battlespace. We thus cannot judge how far to lean on it. Over-commit and Canada invites these risks; under-commit and it cedes strategic ground.

The greatest security risk, and opportunity, from AI is its potential to irreversibly transform the knowledge environment. Sovereign capability must mean governing the knowledge pipeline and deliberately preserving independent human judgment—a knowledge infrastructure that is resilient enough to support AI and thus would not be undermined by it. Concretely, Ottawa should invest in trusted public research and data infrastructure—secure repositories with verifiable provenance and integrity safeguards—and set governance terms for how AI is procured and admitted into public institutions, balancing research security against open science. Building that foundation first lets AI be layered onto a knowledge base Canadians can trust, rather than adopting AI and only afterward trying to make sense of the hybrid human-AI systems it creates."

Balkan Devlen | Montreal Institute for Global Security

Balkan Devlen is Senior Fellow for Strategic Foresight at the Montreal Institute for Global Security (MIGS), Senior Fellow at the Macdonald-Laurier Institute (MLI), and Adjunct Research Professor at Carleton University.

Ottawa's new AI strategy is a competent document about a narrow problem. It wants more firms adopting AI, more compute on Canadian soil, fewer dependencies running through foreign clouds. However, its notion of exposure stops at data centres and supply chains, and its notion of protecting Canadians stops at privacy and online harms. Surely, those are all real concerns but they are not the ones keeping the security and intelligence communities, in Canada and among our allies, awake.

The risks that make advanced AI a national security question rather than an industrial policy file are the ones that may prove irreversible. The Institute for AI Policy and Strategy groups them into three: loss of control, where capable systems slip human oversight; extreme concentration of power, where whoever first commands such systems entrenches an advantage no rival or electorate can later contest; and great power war, where the race itself — through miscalculation, pre-emption, or arms-race instability — turns kinetic. Others add a fourth concern; catastrophic or malicious misuse - think AI-enabled bioweapons or mass subversion via hyper-individualized political warfare at scale.

These are not science fiction stories imported into policy. Three out of four of these risks (with the exception of loss of control) can become reality even before AI systems supersede human-level intelligence. The Privy Council Office co-hosted a scenario exercise with CIGI that walked officials through such risks and concluded governments must prepare now for human-level or superhuman systems within five years. More than thirty MPs and senators across party lines have called superintelligence a national security priority.

The obvious objection — Canada will not build Artificial General Intelligence (AGI), so why plan for it? — has the logic backwards. Precisely because we will not build it, we have every reason to

shape the rules and the outcomes while we still can. A 360-degree strategy would have named these four risks as Canadian security interests and assigned them a mandate and a budget. States that treat advanced AI solely as an adoption file will be governed by decisions made elsewhere. Let's hope the long-awaited National Security Strategy addresses these issues.

Jennifer Irish | Pendulum Geopolitical Advisory

Jennifer Irish is Adjunct Professor, University of Ottawa (Telfer) and Principal, Pendulum Geopolitical Advisory. She is a former Canadian diplomat and was the Founding Director of the University of Ottawa's Information Integrity Lab.

Dave McMahon | Clairvoyance Corp

Dave McMahon is CEO Clairvoyance Corp and Chief Intelligence Officer at Sapper Labs. Dave also served in various leadership positions with the Canadian Armed Forces, Canadian Security Intelligence Service (CSIS) and the Communications Security Establishment (CSE).

The rapid advancement of AI is transforming Canada's security, intelligence and defence enterprise. AI is both an enabler and a disruptor, and Canada's ability to maximize its benefits while reducing risks will depend not only on its AI strategy, but also on complementary investments in security, information integrity, resilience and trusted partnerships.

AI offers significant opportunities to advance further in big data analytics, intelligence curation and assessment, cybersecurity, defence operations, and risk-informed decision-making.

At the same time, Canada faces an increasingly complex threat environment where technology is a defining feature of geopolitical competition and conflict. Generative AI enables deepfakes, synthetic media, and large-scale disinformation campaigns that undermine public trust. It can also facilitate transnational repression, online exploitation, financial manipulation, and increasingly sophisticated cyberattacks. There is considerable untapped potential to leverage AI to detect cyber threats, counter foreign information manipulation and interference, strengthen critical infrastructure resilience and improve Canada's ability to respond to these emerging threats. A credible AI strategy must balance innovation with measures to counter AI-enabled disinformation and information manipulation.

A first priority is for Canada to build a secure, sovereign AI capabilities by expanding trusted domestic data, compute capacity and digital infrastructure, along with a sovereign intelligence collection capacity. These investments will reduce reliance on foreign technologies for critical national security applications while strengthening resilience and economic competitiveness. International collaboration, including federated approaches with trusted partners such as those in Europe, can be of benefit in complementing (not replacing) Canadian sovereign capability as long as internet openness is not sacrificed.

Success also depends on close collaboration to counter cyber and information attacks among governments, industry, academia, civil society and allies, supported by common threat methodologies and standards, shared secure information-sharing platforms and harmonized mitigation strategies and playbooks. We should continue to pursue options to regulate the development of AI without stifling innovation.

Canada's AI strategy provides a good foundation. The next challenge is translating strategic objectives into operational capability through sustained investment, dedicated counter-disinformation initiatives, stronger research security, coordinated cyber defence, and enduring partnerships that ensure AI enhances both Canada's security and long-term prosperity.