



CIRANO
Knowledge into action



DIGITAL SOVEREIGNTY AND
ARTIFICIAL INTELLIGENCE
IN CANADA:
FROM SYSTEM FRAGMENTATION
TO INTEGRATED STRATEGIC
CAPACITY IN THE PUBLIC SECTOR

ALAIN DUDOIT

PR

2026PR-05
FOR REFLECTION

Les documents **Pour Réflexion** sont des documents publiés pour susciter échanges et commentaires et s'appuient sur des résultats de recherche. Ces documents sont sous la seule responsabilité des auteurs.

Reflection Papers are documents published to stimulate discussion and commentary, based on research findings. These documents are the sole responsibility of their authors.

Le CIRANO est un organisme sans but lucratif constitué en vertu de la Loi des compagnies du Québec. Le financement de son infrastructure et de ses activités de recherche provient des cotisations de ses organisations-membres, d'une subvention d'infrastructure du gouvernement du Québec, de même que des subventions et mandats obtenus par ses équipes de recherche.

CIRANO is a private non-profit organization incorporated under the Quebec Companies Act. Its infrastructure and research activities are funded through fees paid by member organizations, an infrastructure grant from the government of Quebec, and grants and research mandates obtained by its research teams.

Les partenaires du CIRANO – CIRANO Partners

Partenaires Corporatifs - Corporate Partners

Autorité des marchés financiers
Banque de développement du Canada
Banque du Canada
Banque Nationale du Canada
Bell Canada
BMO Groupe financier
La Caisse
Énergir
Hydro-Québec
Intact Corporation Financière
Mouvement Desjardins
Power Corporation du Canada
Pratt & Whitney Canada
VIA Rail Canada

Partenaires gouvernementaux - Governmental partners

Ministère des Finances du Québec
Ministère de l'Économie, de l'Innovation et de l'Énergie
Innovation, Sciences et Développement Économique
Canada
Ville de Montréal

Partenaires universitaires - University Partners

École de technologie supérieure
École nationale d'administration publique
HEC Montréal
Institut national de la recherche scientifique
Polytechnique Montréal
Université Concordia
Université de Montréal
Université de Sherbrooke
Université du Québec
Université du Québec à Montréal
Université Laval
Université McGill

Le CIRANO collabore avec de nombreux centres et chaires de recherche universitaires dont on peut consulter la liste sur son site web. *CIRANO collaborates with many centers and university research chairs; list available on its website.*

© April 2026. Alain Dudoit. Tous droits réservés. *All rights reserved.* Reproduction partielle permise avec citation du document source, incluant la notice ©. *Short sections may be quoted without explicit permission, if full credit, including © notice, is given to the source.*

Les idées et les opinions émises dans cette publication sont sous l'unique responsabilité des auteurs et ne représentent pas les positions du CIRANO ou de ses partenaires. *The observations and viewpoints expressed in this publication are the sole responsibility of the authors; they do not represent the positions of CIRANO or its partners.*

**Digital Sovereignty and Artificial Intelligence in Canada:
From System Fragmentation to Integrated Strategic Capacity in the Public Sector**

Alain Dudoit

Ambassador of Canada (ret.)

CIRANO Invited Fellow

Strategic Advisor, Global Advantage Consulting Group

April 20, 2026

Pour citer ce document / To quote this document

Dudoit, A. (2026). Digital Sovereignty and Artificial Intelligence in Canada: From System Fragmentation to Integrated Strategic Capacity in the Public Sector (2026PR-05, CIRANO).

<https://doi.org/10.54932/VKRW5383>

Acknowledgments

I would like to thank my colleagues **Anne Marie Hubert**, CIRANO Visiting Fellow and Chair of the Board of the Canadian branch of the Institute for Human Technology, and **Tony Labillois**, Consultant on accessibility, public policy, leadership, and data; former Executive Director at Statistics Canada; and elected member of the International Statistical Institute. I am also grateful to **Alexis Bouffioux**, Communications Coordinator, for verifying and formatting this document in accordance with CIRANO's publication standards.

Their comments and contributions have enhanced the quality and relevance of this work; however, I remain solely responsible for the content, interpretations, and presentation of the final report.

Table of Contents

Acknowledgments	3
Abstract	5
Résumé	6
Introduction	8
Part One: Recent Developments and Strategic Foundations	11
A geopolitical cycle in flux	11
AI as systemic infrastructure	11
Canada as a middle power	12
Lessons from Quebec	12
The St. Lawrence–Great Lakes Corridor	13
The federal institutional architecture	13
Interoperability and National Security	14
Public trust and the legitimacy of the data ecosystem	15
Part Two: Material and systemic dimensions	16
AI as physical infrastructure	16
The Stargate project and the reshaping of power dynamics	16
Energy and physical constraints	18
Critical dependencies and national security	18
Part Three: Canadian Architecture and Moving to Action	19
Interoperability as strategic infrastructure	19
Data quality and metadata infrastructures	19
Distributed governance and systemic integration	19
Institutional architecture	20
Roadmap for the next 12–24 months	21
Conclusion	23
Annotated bibliography	25

Abstract

Background and issues

This publication offers an up-to-date analysis of public data interoperability in Canada. It incorporates recent developments in federal and provincial policies (notably Quebec's 2026 Digital Sovereignty Statement and two relevant 2026–2027 departmental plans). It also reflects on the acceleration of transformations linked to artificial intelligence (AI). This study builds on the strategic overview and call to action of 2 February 2026. It adds a physical and systemic dimension: AI is no longer merely a software technology, but a physical infrastructure dependent on energy resources, data centres and networks ([McKinsey & Company, 2026](#); [Barbet, IRIS, 2026](#)). FPT+ interoperability (= federal-provincial-territorial, municipal and First Nations) is therefore no longer merely an administrative modernisation project, but a central lever of Canada's strategic capacity, on a par with energy networks or telecommunications.

Three geopolitical and technological dynamics are shaping this context: the fragmentation of supply chains and their reconfiguration around economic security and resilience ([Chatham House, 2026](#)); the industrialisation of AI, marked by a concentration of computing power ([Stargate project](#)) and increased reliance on physical infrastructure ([Beaumier & Cadieux, IRPP, 2026](#)); digital sovereignty, redefined as the ability to structure dependencies rather than seek absolute technological autonomy ([Munk School, 2026](#)).

Key proposals

1. The Canadian domestic market (30–32% of GDP) must be treated as a strategic infrastructure for resilience, whose performance depends on data integration (the St. Lawrence–Great Lakes corridor as a demonstrator).
2. FPT+ interoperability is no longer a technical project, but the prerequisite for an integrated domestic market and predictable economic governance ([Dudoit et al., CIRANO, 2026](#)).
3. Strategic AI acts as a performance multiplier in key sectors (supply chains, critical minerals, the Arctic), provided that the underlying data is interoperable ([Goldfarb, CSA, 2026](#)).

Institutional architecture and roadmap

The coordination between the Treasury Board Secretariat (TBS), Shared Services Canada (SSC) and the Office of Digital Transformation (ODT) is analysed as a structural issue to prevent fragmentation. Our roadmap for 2026–2028 proposes: Flagship use cases (St. Lawrence–Great Lakes corridor); an effective FPT+ strategic data network (supply chains, infrastructure, finance; health, etc.); an FPT+ governance framework with coordination mechanisms and safeguards for data protection and institutional capacity building (innovation labs, training for human resources in the public sector and civil society).

Conclusion

Contemporary sovereignty is no longer measured by the possession of physical resources but by the capacity to integrate data, infrastructure, and decisions. FPT+ interoperability is the key lever for transforming fragmentation into a strategic capability, strengthening Canada's decision-making autonomy in a globalised environment (Centre for Data Innovation, 2026). Without coordinated action by 2028, the country's room for manoeuvre will diminish in the face of the consolidation of technological architectures dominated by a few players.

Résumé

Contexte et enjeux

Cette publication propose une analyse actualisée de l'interopérabilité des données publiques au Canada. Elle intègre les développements récents en matière de politiques fédérales et provinciales (notamment l'énoncé québécois de souveraineté numérique de 2026 et les plans ministériels 2026–2027). Elle se pense aussi sur l'accélération des transformations liées à l'intelligence artificielle (IA). Cette étude s'inscrit dans la continuité de la synthèse stratégique et appel de l'action du 2 février 2026. Elle y ajoute une dimension matérielle et systémique : l'IA n'est plus seulement une technologie logicielle, mais une infrastructure physique dépendant de ressources énergétiques, de centres de données et de réseaux ([McKinsey & Company, 2026](#) ; [Barbet, IRIS, 2026](#)). L'interopérabilité FPT+ (= fédérale-provinciale-territoriale, municipale et Premières Nations) n'est donc plus un simple projet de modernisation administrative, mais un levier central de la capacité stratégique du Canada, au même titre que les réseaux énergétiques ou les télécommunications.

Trois dynamiques géopolitiques et technologiques façonnent ce contexte : La fragmentation des chaînes d'approvisionnement et leur reconfiguration autour de la sécurité économique et de la résilience ([Chatham House, 2026](#)) ; l'industrialisation de l'IA, marquée par une concentration des capacités de calcul ([projet Stargate](#)) et une dépendance accrue aux infrastructures matérielles ([Beaumier & Cadieux, IRPP, 2026](#)) ; la souveraineté numérique, redéfinie comme la capacité à structurer des dépendances plutôt qu'à rechercher une autonomie technologique absolue ([Munk School, 2026](#)).

Propositions clés

1. Le marché intérieur canadien (30–32 % du PIB) doit être traité comme une infrastructure stratégique de résilience, dont la performance dépend de l'intégration des données (corridor Saint-Laurent–Grands Lacs comme démonstrateur).
2. L'interopérabilité FPT+ n'est plus un projet technique, mais la condition d'un marché intérieur intégré et d'une gouvernance économique prévisible ([Dudoit et al., CIRANO, 2026](#)).
3. L'IA stratégique agit comme un multiplicateur de performance dans les secteurs clés (chaînes d'approvisionnement, minéraux critiques, Arctique), à condition que les données sous-jacentes soient interopérables ([Goldfarb, CSA, 2026](#)).

Architecture institutionnelle et feuille de route

L'articulation entre le Secrétariat du Conseil du Trésor (SCT), Services partagés Canada (SPC) et le Bureau de la transformation numérique (BTN) est analysée comme un enjeu structurel pour éviter la fragmentation. Notre feuille de route pour 2026–2028 propose : Des cas d'usage emblématiques (corridor Saint-Laurent–Grands Lacs) ; un réseau FPT+ performant de données stratégiques (chaînes d'approvisionnement, infrastructures, finances ; santé...) ; un cadre de gouvernance FPT+ avec des mécanismes de coordination et des garanties pour la protection des données ; le renforcement des capacités institutionnelles (laboratoires d'innovation, formation des ressources humaines dans le secteur publique et dans la société civile).

Conclusion

La souveraineté contemporaine ne se mesure plus par la possession de ressources physiques mais par la capacité d'intégration des données, des infrastructures et des décisions. L'interopérabilité FPT+ est le levier central pour transformer la fragmentation en une capacité stratégique, renforçant l'autonomie décisionnelle du Canada dans un environnement globalisé (Center for Data Innovation, 2026). Sans action coordonnée d'ici 2028, les marges de manœuvre du pays se réduiront face à la consolidation des architectures technologiques dominées par quelques acteurs.

Introduction

Three recent events have highlighted the urgency of strategic public data integration in Canada. [The CIRANO panel](#) on 19 January 2026 highlighted persistent gaps in interoperability. The resulting call to action proposed concrete steps to address these issues. Finally, the [fourth annual GVCdtLab conference](#), held on 26 March, highlighted the key role of the St. Lawrence–Great Lakes corridor as a lever for economic integration. These discussions converge on an unequivocal conclusion: Canada’s main strategic asset lies in its domestic market.

This market accounts for 30 to 32 per cent of GDP, and five out of six jobs depend directly on it. Yet it does not yet function as a unified economic space. Several obstacles hinder its effectiveness. Interprovincial barriers persist, complicating the movement of goods and services. Rules and practices vary from one province to another, creating distortions of competition. Administrative processes overlap, making procedures cumbersome for businesses. Above all, data is collected according to different methodologies, and systems do not communicate with one another. As a result, in many sectors, coordination costs remain abnormally high, holding back the productivity of an advanced and innovative country.

This update marks a turning point in how we approach the digital transformation of the public sector. It is no longer a matter of gradual administrative modernisation, but of a structural shift that redefines the conditions under which public authority is exercised. Three elements are profoundly transforming this landscape. Data, having become a strategic asset, enables us to understand economic and social dynamics with unprecedented precision.

Secondly, digital infrastructure now underpins all institutional activities, from service delivery to national security. Finally, artificial intelligence is no longer merely a tool for innovation: it constitutes a systemic infrastructure that shapes economic, industrial, and institutional dynamics, as highlighted by McKinsey & Company (2026).

In this context, advanced economies are no longer distinguished solely by their physical resources or institutions. Their ability to integrate complex systems and organise the interdependencies that run through them is becoming a decisive factor in their power. Canada, as a middle power, embodies this paradox. On the one hand, it possesses major assets: a world-class scientific ecosystem, stable institutions, and abundant natural and energy resources. On the other hand, these assets do not translate into an integrated strategic capability. Three factors explain this disconnect. The fragmentation of data across the FPT+ public sector prevents a coherent analysis of national issues. The segmentation of institutional structures limits coordination between stakeholders. The lack of interoperability mechanisms delays decision-making in crisis situations.

A paradigm shift is therefore required. It is no longer a question of modernising sectors in silos, but of building a unified strategic capability. The interoperability of FPT+ public data is the central lever for this. As McKinsey & Company (2026) highlights, the challenge goes beyond technology: it is about transforming a set of fragmented systems into an architecture capable of supporting public decision-making, anticipating disruptions, and acting in a global environment marked by increased uncertainty and rivalries.

Why an update

Since January 2026, the strategic context has been changing profoundly and at an ever-increasing pace, necessitating an urgent update to our analysis. Three major dynamics explain this acceleration.

Firstly, artificial intelligence has entered a phase of industrialisation. This transition is characterised by a concentration of capabilities in the hands of a limited number of players, mainly American and Chinese, and an increased reliance on physical infrastructure, such as data centres and energy networks. This transformation is not neutral: it redefines power dynamics and exposes Canada to new vulnerabilities, particularly in terms of national security and economic resilience.

Secondly, analytical frameworks have evolved. Digital sovereignty is no longer synonymous with technological autonomy. As demonstrated by the Munk School (2026) and Chatham House (2026), it now refers to a state's ability to structure its dependencies within a globalised environment. For a middle power such as Canada, this means organising partnerships, diversifying supply sources and securing critical infrastructure, rather than seeking an impossible self-sufficiency.

Thirdly, Canadian initiatives reveal a paradox. On the one hand, the federal and provincial governments have recognised the strategic importance of data and AI. Quebec's Digital Sovereignty Statement (2026), federal departmental plans, and recent adjustments within the public sector bear witness to this. On the other hand, these initiatives remain fragmented. The lack of coordination between levels of government risks even exacerbating the silo mentality that Canada is specifically seeking to overcome.

These transformations are accompanied by institutional awareness, but also by persistent challenges. Operating models are evolving, at both federal and provincial levels. Public actors now recognise the urgency of action but are struggling to achieve overall coherence. The most recent research, coupled with strategic reflections conducted at CIRANO and elsewhere, confirms the systemic nature of this pivotal moment. Canada stands at a crossroads: either it integrates its initiatives into a coherent framework, or it risks seeing its investments in infrastructure and technology reinforce existing fragmentation.

There is therefore a pressing need for concerted action among FPT+ governments. Two scenarios lie ahead for the country. Without systemic integration, investments risk deepening divisions, weakening resilience in the face of external shocks. Conversely, a coordinated approach could transform scattered initiatives into a unified ecosystem, capable of producing systemic effects and strengthening Canada's competitiveness and sovereignty.

This publication draws on a cross-analysis of international strategic reports, federal and provincial government frameworks, and recent academic work on digital sovereignty, data interoperability, and AI. Its objective is clear: to provide an integrated understanding of the transformations underway and to derive concrete implications for Canada's institutional architecture. The focus is no longer on diagnosing problems, but on proposing actionable solutions for the next 12 to 24 months.

Part One: Recent Developments and Strategic Foundations

A geopolitical cycle in flux

The world is entering a phase of accelerated breakdown of the international order. We are witnessing the end of one historical cycle and the beginning of another – a geopolitical cycle which, unlike economic cycles, spans several decades. This transition is not neutral: it is redefining the balance of power between the major powers. The United States, faced with the rise of China, is reconfiguring its alliances, trade, and value chains to serve its strategic interests above all else. Europe and other regional players are following this trend, marking the end of an era in which economic efficiency took precedence over geopolitical considerations.

The [CIRANO GVCdtLab](#) conference on 26 March identified three key findings that shed light on the challenges facing Canada. Firstly, national security now takes precedence over the mere pursuit of economic efficiency. States now prioritise resilience and technological sovereignty, even if this entails additional costs or longer lead times. Secondly, businesses and investors must navigate an increasingly complex environment. Protectionism is becoming widespread, sanctions are multiplying, and state intervention in the economy is becoming the norm rather than the exception. Finally, the investment landscape is undergoing a profound transformation. Certain sectors, once considered purely commercial, are becoming strategic, with digital technologies, critical minerals and energy infrastructure leading the way. Decision-making horizons are shortening as geopolitical risks evolve rapidly. Value chain models based solely on cost optimisation are becoming obsolete, as they ignore the new realities of security and resilience.

AI as systemic infrastructure

Canada is on the front line of this global reconfiguration, as its economy depends significantly on trade with the United States and on the continued technological dominance of its powerful neighbour. Supply chains, once optimised for cost and speed, are now being redesigned around four imperatives: economic security, resilience, technological sovereignty, and strategic competitiveness. As Chatham House (2026) points out, economic performance no longer relies solely on access to external markets or the reduction of trade barriers. It now depends on a country's ability to function as an integrated system, capable of coordinating its physical infrastructure, information flows, governance mechanisms, and analytical tools.

Artificial intelligence perfectly illustrates this transformation. Long regarded as merely a set of techniques, it has become a systemic infrastructure, as critical as energy networks or transport. Its components – computing infrastructure, energy resources, data, models, and platforms – are now deeply interdependent, as demonstrated by McKinsey & Company (2026). The social and economic implications are considerable, as are the human and skills training challenges they raise. This interdependence is a gamechanger: digital sovereignty can no longer be reduced to a quest for technological autonomy. Rather, it must be understood as the ability to manage complex dependencies whilst retaining decision-making flexibility.

Canada as a middle power

Current geo-economic transformations mark a turning point: global value chains are no longer driven solely by the pursuit of efficiency. They have become instruments of power, where economic security, resilience and technological sovereignty take precedence over cost optimisation. For Canada, as a middle power, this change poses a twofold challenge. On the international stage, the country must contend with the dominance of the major powers and a structural dependence on global infrastructure.

Within its borders, it faces another obstacle: data fragmentation, interprovincial barriers, and a lack of collaboration between public and private sector actors.

In an increasingly protectionist world, a strong domestic market becomes a strategic asset. It fulfils three essential functions. It acts as a buffer against external shocks: when access to export markets is restricted, the ability to rapidly reallocate flows within the country reduces the vulnerability of businesses. It also serves as a platform for SMEs to scale up: for many of them, consolidating their capabilities in the domestic market precedes and facilitates their international expansion. Finally, it provides a space for standardisation and learning: businesses can evaluate, certify, and optimise their products there before exporting them.

However, Canada does not yet function as a truly unified domestic market. Several obstacles hinder its effectiveness. Interprovincial barriers persist, complicating the movement of goods and services. Rules and practices vary from one province to another, creating distortions of competition. Administrative processes overlap, making procedures more cumbersome for businesses. Above all, data is collected according to different methodologies, and systems do not communicate with one another.

Lessons from Quebec

[Quebec's Digital Sovereignty Policy Statement](#) (2026) offers valuable lessons, not only for the province but for Canada as a whole. The Quebec government has adopted a resolutely operational approach. Rather than limiting itself to principles or regulatory frameworks, it has made concrete choices: strengthening control over its critical infrastructure, such as its government cloud and data localisation, and reducing its dependence on external suppliers. This approach demonstrates that digital sovereignty is built through tangible actions: directing investment, structuring a technological ecosystem, and aligning public decisions with common objectives.

The Quebec experience also reveals the limitations of a purely infrastructure-based approach. Admittedly, strengthening control over infrastructure and data is necessary. But this is not enough to create an integrated strategic capability if information systems remain fragmented and lack interoperability. Digital sovereignty is not merely about controlling technological assets. It also requires the fluid and secure flow of information, both within Quebec and between the various levels of government in Canada. Without this integration, investments in infrastructure risk reproducing, on a different scale, the very silos we are seeking to eliminate.

The St. Lawrence–Great Lakes Corridor

The St. Lawrence–Great Lakes Corridor perfectly embodies the challenges and opportunities of data integration. This strategic economic area, where flows of goods, energy and information intersect, illustrates just how much performance depends on coordination. Yet the data associated with these flows remains fragmented today. It is held by a multitude of stakeholders, produced according to different standards and rarely integrated. This fragmentation has direct consequences: it limits visibility into operations, reduces the ability to anticipate disruptions, and hinders the optimisation of logistics flows.

Data interoperability can transform this situation. By linking the various sources of information, it would enable the creation of a unified view of the corridor. Stakeholders could then anticipate disruptions, improve their coordination, and strengthen resilience in the face of shocks. This is not merely a technical issue: it is a strategic lever for turning the corridor into a genuine economic driver, whilst securing supply chains that are critical to Canada.

The federal institutional architecture

The 2026–2027 departmental plans of [the Treasury Board Secretariat \(TBS\)](#) and [Shared Services Canada \(SSC\)](#) reveal a growing awareness of the challenges of interoperability and digital sovereignty. TBS is positioning itself as the linchpin of this transformation. Its responsibilities cover data governance, the modernisation of public services and coordination between different levels of government. To fully fulfil this role, TBS must broaden its mandate. It must make FPT+ interoperability an explicit strategic priority, create incentives to encourage provinces and territories to participate, and streamline administrative processes to accelerate implementation.

Shared Services Canada (SSC) plays a complementary but equally crucial role. As the operational arm of digital transformation, it is responsible for modernising infrastructure, ensuring secure data hosting and strengthening the cybersecurity of systems. To fully support interoperability, SPC must develop common platforms accessible to all levels of government, harmonise technical protocols to facilitate data exchange, and collaborate closely with the provinces to avoid duplication and optimise the use of resources.

The Office of Digital Transformation (ODT), although still under development, has a pivotal role to play. It must function as the link between the strategy defined by TBS and its implementation by SPC. It must facilitate coordination among all stakeholders and identify high-impact use cases to demonstrate the concrete benefits of interoperability. The positioning of the BTN within the SCT is not a mere organisational detail. It constitutes a structural choice. This configuration allows governance and coordination functions to be concentrated within a single institutional framework, whilst maintaining a clear separation from the operational functions conducted by SPC. This role involves close collaboration with the private sector and research and training institutions. This coordination is essential. It prevents the fragmentation of responsibilities and strengthens the overall coherence of the system. Without this coordination, efforts risk remaining fragmented and interoperability will never become an operational reality.

Interoperability and National Security

In a world marked by geopolitical fragmentation and the militarisation of data, Canada's national security increasingly depends on its ability to integrate, protect and utilise its own data. FPT+ interoperability and digital sovereignty are not merely technical projects: they are critical infrastructure, just like energy or telecommunications networks. They form the foundation of the country's strategic autonomy.

However, the fragmentation of data systems within FPT+ administrations exposes Canada to three major risks. Firstly, it creates blind spots in intelligence, preventing a comprehensive view of threats and opportunities. Secondly, it leads to delays in decision-making during crises, when every second counts. Thirdly, it increases the country's strategic dependence, making it vulnerable to external pressures. Sovereignty is no longer measured solely in terms of territory or military capabilities: it now rests on control of data, digital infrastructure, and information systems.

The real danger is not a sudden event, but a gradual erosion. Canada will not lose its sovereignty overnight: it will see it erode as it becomes dependent on systems it does not control. In this context, the interoperability of public data and digital sovereignty are no longer distant concerns: they are immediate priorities for national security. The state's ability to integrate and utilize its data will determine its resilience in the face of future crises.

The recent restructuring of national security functions marks a turning point in the organization of the Canadian state. Since its creation in 2023 and its reorganization following the 2025 elections, the National Security Council (NSC) has become the central forum within the Cabinet for strategic decision-making. Its remit covers a broad spectrum. It analyzes intelligence to inform government decisions. It manages strategic relations, notably with the United States, a key partner but also a dominant player in the technological sphere. It oversees responses to modern threats, whether foreign interference, cyberattacks or global instability. Finally, it sets annual priorities for intelligence and defence, thereby ensuring long-term coherence.

The promotion, in March 2026, of the Chief Information Officer of the SCT to the post of Under-Secretary of the Cabinet for National Security and Intelligence could represent a major step forward. This change is significant. It offers a unique opportunity to elevate digital governance issues to the strategic level. It also ensures horizontal integration by linking technical, analytical, and decision-making dimensions. Finally, it paves the way for coherent alignment between AI, data, and intelligence—three essential pillars of modern national security.

Data interoperability, digital sovereignty, and AI have moved beyond the realm of administrative modernization. They now lie at the heart of national security and the state's strategic capability. In an environment where hybrid risks are multiplying and information is becoming a weapon, the ability to produce, integrate and utilize data is no longer an option: it is an essential prerequisite for anticipating crises, making informed decisions, and acting effectively.

Sovereignty is no longer measured solely in square kilometres or military capabilities. It is now measured in terms of information integration capacity. The interoperability of FPT+ data has become a critical infrastructure, on a par with energy networks or telecommunications. Its role is just as vital: without it, fragmented systems create major vulnerabilities. Blind spots in intelligence are multiplying. Decision-making delays in crisis response are lengthening. Dependence on external systems is growing, exposing the country to unnecessary risks.

National security and intelligence functions must now play a structuring role. They can no longer be limited to the collection and analysis of information. Their mission is now broader: they must shape the state's information and decision-making architecture. This entails three key responsibilities: 1) integrating data flows to avoid blind spots and redundancies; 2) aligning analytical capabilities to ensure decisions are based on reliable and up-to-date information; 3) ensuring the consistency of the systems that support FPT+ public action.

This evolution goes beyond the scope of digital transformation. The issue at stake is now Canada's operational sovereignty. In an increasingly fragmented international system, where information has become a vector of power in its own right, the ability to integrate, protect and utilize data is no longer an asset: it is a prerequisite for fully exercising sovereignty. The countries that master this integration will be those able to anticipate crises, influence international standards and protect their strategic interests.

Data interoperability and digital sovereignty are no longer merely sector-specific initiatives. They now define the very architecture of contemporary public power. A state that does not control its data does not control its decisions. In a world where information is a resource as critical as energy or physical infrastructure, it is this capacity for integration that will distinguish sovereign nations from those that are subject to the choices of others.

Public trust and the legitimacy of the data ecosystem

The ability to integrate and utilise data at the FPT+ level rests on a condition that is often implicit but decisive: public trust. Without strong social legitimacy, data integration initiatives, even those that are technically robust, face institutional and public resistance that limits their scope. The protection of personal information, transparency of use, and clarity of responsibilities and communications with the public thus become strategic components, on a par with infrastructure or analytical capabilities.

In this context, data governance must explicitly incorporate mechanisms for accountability, auditing and public communication. It is not merely a matter of protecting data, but of continuously demonstrating that its use generates tangible public value. This 'licence to operate' determines the sustainability of interoperability initiatives and their acceptability in an environment where public expectations regarding transparency and ethics are rising sharply.

Part Two: Material and systemic dimensions

AI as physical infrastructure

Artificial intelligence has undergone a radical transformation. It is no longer merely an abstract, dematerialized software technology. It has become embedded in the physical world, now dependent on tangible resources: energy to power its computations, data centres to store and process information, and ultra-high-speed networks to transmit data flows. As McKinsey & Company (2026) points out, this evolution marks a turning point: innovation in AI no longer relies solely on algorithms, but on the physical infrastructure that underpins them.

The latest generation of AI models illustrates this growing dependence. They require massive processing power, distributed storage systems to manage unprecedented volumes of data, and ultra-fast networks to ensure instant communication. This exponential demand for computing power has shifted the centre of gravity of innovation: physical infrastructure has become the limiting factor in AI progress.

The Stargate project and the reshaping of power dynamics

The Stargate project, analyzed by P. Barbet (IRIS 2026), represents a paradigm shift in the field of AI. It is not merely an additional piece of infrastructure, but a paradigm shift: computing capabilities are designed and deployed on a massive scale, responding to both technical and economic imperatives. The economy of scale enables reducing unit costs and optimizing resource utilization. But they also create barriers to entry for actors lacking colossal resources, such as Canada.

Stargate reveals a profound geopolitical realignment. AI infrastructure is becoming a vehicle for influence, as those who control it can impose technological standards and control access to data. For countries such as Canada, the challenge is not to replicate such megaprojects, but to negotiate the terms of their dependence in order to preserve their decision-making autonomy. As recommended by Chatham House (2026), a differentiated strategy is required: specializing in promising sectors, forging structured partnerships with reliable actors, and diversifying dependencies to avoid excessive vulnerability.

Stargate illustrates a shift in scale and nature. AI is no longer primarily a software industry, but a heavy industry, characterized by massive investment, high energy intensity, and increased reliance on critical physical infrastructure. This transformation is accompanied by a rapid concentration of capabilities in the hands of a small number of players, capable of mobilizing capital, energy, and computing power on a very large scale. It thus redefines the conditions of competition, innovation, and sovereignty.

In this new environment, computing power has become a strategic bottleneck. Beaumier and Cadieux (IRPP, 2026) highlight the urgency for Canada to develop a national computing capacity. Access to “compute” is no longer merely a technical issue: it is a prerequisite for entry into the AI ecosystem. The international concentration of these capabilities, combined with insufficient private incentives for large-scale domestic investment, creates a structural dependency that market mechanisms alone cannot reduce. The development of national computing capacity, whether public or hybrid in partnership with the private sector, is therefore essential as an industrial policy lever to secure access to critical AI infrastructure.

However, the physical nature of infrastructure is not limited to its availability or location. The analysis by the Center for Data Innovation (2026) on data centres in the United States clearly shows this: the tensions surrounding their expansion, electricity consumption, network access, pricing, reliability, or water usage are not so much a matter of absolute physical constraints as of a mismatch between these and rules. This mismatch pits the rapid deployment of digital infrastructure against the slow evolution of the governance frameworks that should organize its integration.

This observation is crucial. It reveals that the sustainability and performance of AI infrastructure depend less on its raw capacity than on the quality of the regulatory mechanisms governing it. Without pricing structures that reflect the network’s actual constraints, transparent access rules, adequate cost allocation and integrated investment planning, the risks are real: economic distortions, cost shifting to households and a decline in the reliability of energy systems.

Applied to the Canadian context, this analysis takes on a particular dimension. In a federal system where jurisdiction over energy, natural resources and economic development is shared, the governance of AI infrastructure cannot be separated from the broader issue of intergovernmental coordination. The ability to deploy, integrate and regulate data centres therefore depends on two factors: investment in physical infrastructure, but also the alignment of regulatory frameworks, pricing mechanisms, and information systems across levels of government.

This has key implications for Canada’s digital sovereignty. Control over critical AI infrastructure is not merely a question of location or ownership. It rests on the ability to coherently integrate computing power, energy infrastructure, governance frameworks, and data systems. In the absence of such integration, investments in computing risk replicating existing fragmentation, limiting their strategic scope. Conversely, embedding them within a coordinated architecture—linking public data interoperability, infrastructure planning, and economic governance—enables the transformation of physical assets into genuine strategic capability.

Energy and physical constraints

One of the major challenges of AI lies in its growing dependence on energy. Digital infrastructure is among the most energy-intensive in the world. It requires colossal amounts of electricity, as well as high-performance cooling systems to prevent overheating. For Canada, this aspect represents both an opportunity and a risk.

On the one hand, the country has a major asset: its abundant hydroelectric resources, particularly in Quebec, could make it a magnet for green data centres. On the other hand, increased reliance on electricity to power AI exposes Canada to new vulnerabilities. Cyberattacks on energy networks or local shortages could paralyze critical infrastructure, as highlighted by McKinsey & Company (2026).

An energy policy integrated into the digital strategy is therefore essential. It would help secure the supply of critical infrastructure, whilst reducing the risks of excessive dependence. It would also position Canada as a key player in the green AI economy, a rapidly expanding sector. To achieve this, close coordination is essential: between the federal and provincial governments, FPT+, but also with the private sector, in order to align energy and digital objectives.

Critical dependencies and national security

Canada finds itself in a delicate position: it controls none of the global infrastructure underpinning artificial intelligence. This structural dependency limits its ability to set its own rules and restricts its decision-making autonomy. In the current geopolitical context, this issue extends beyond the economic sphere: it is becoming a matter of national security.

As highlighted by the Munk School (2026), data, digital architectures and AI systems have become vectors of influence and vulnerability. They expose Canada to major risks: restrictions on access to critical technologies, flaws in the governance of its infrastructure, and insufficient resilience against cyber threats. These vulnerabilities are exploited by foreign actors, compromising the country's sovereignty.

To address this, Canada must adopt a systemic approach, combining three key elements. First, it must strengthen the sovereignty of its critical infrastructure by securing access to essential resources. Next, it must establish active governance of its dependencies by diversifying its partnerships to avoid excessive vulnerability. Finally, it must develop continuity plans for its critical infrastructure to ensure it remains operational even in the event of a crisis. Such a strategy would enable Canada to turn a constraint into an asset. By structuring its dependencies strategically, Canada could preserve its decision-making autonomy. Rather than being subject to the choices of major powers, it could negotiate balanced partnerships and develop complementary national capabilities.

Part Three: Canadian Architecture and Moving to Action

Interoperability as strategic infrastructure

The interoperability of public data in Canada is not merely a technical issue. It constitutes a strategic infrastructure, as essential as energy networks or transport. Yet, despite its abundance, Canadian data remains siloed. It is produced according to heterogeneous standards and rarely shared in a structured manner between different levels of government.

This fragmentation has direct consequences. It limits the ability to gain a comprehensive overview of economic, social, and logistical issues. It slows down decision-making by preventing a rapid and coherent analysis of situations. It also hinders the adoption of AI in public processes, as algorithms require integrated, high-quality data to function effectively.

Data quality and metadata infrastructures

Interoperability cannot deliver its benefits without sustained attention to data quality and the robustness, availability and clarity of metadata. Data that is accessible but not comparable, poorly documented or of uneven quality severely limits analytical capacity and may even introduce decision-making biases. In an FPT+ environment, where data comes from multiple sources, the standardisation of definitions, classifications and indicators becomes an essential prerequisite for their strategic use.

Metadata infrastructures (descriptions of concepts, methods, limitations and uses) must be regarded as critical assets. They enable not only technical integration, but also the correct interpretation of data by decision-makers and artificial intelligence systems. Investing in data quality and documentation thus directly strengthens analytical capacity and the reliability of public decisions.

Distributed governance and systemic integration

The interoperability of public data should not be confused with centralization. In the Canadian context, where the division of powers between the different levels of government is a fundamental principle, it aims instead to facilitate the flow of data between separate systems. This approach preserves the autonomy of each stakeholder whilst allowing for the coordinated use of information. This distributed governance offers a balanced solution. It avoids the false dilemma between centralization and total autonomy by proposing a third way: the pooling of resources between different jurisdictions and FPT+ collaboration. It allows the specific competences of each level of government to be preserved whilst strengthening the overall coherence of public action.

As highlighted by **Chatham House (2026)** and the **CIRANO Burgundy report (2025)**, such a governance model must be structured around three pillars. It must establish clear standards to ensure interoperability. It must ensure effective coordination between the various stakeholders. It must also enforce compliance with rules whilst establishing mechanisms of trust. These mechanisms must be based on transparency, security, and the protection of fundamental rights to gain the support of all partners. These mechanisms include system audits and compliance audits with standards such as Assurance 5000 and other international ethical standards.

Particular attention must be paid to data from First Nations, Inuit and Métis communities, whose governance is based on distinct principles, particularly regarding control, access and use. FPT+ integration must respect these specific frameworks to ensure sustainable and legitimate collaboration.

Institutional architecture

For interoperability to become an operational reality, Canada must clarify the roles of its key institutions and strengthen their synergies. The Treasury Board Secretariat (TBS) occupies a central position within this architecture. Its responsibilities cover data governance, the modernization of public services and coordination between the different levels of government. To fully fulfil this role, TBS must expand its mandate. It must make FPT+ interoperability an explicit strategic priority, create incentives to encourage provinces and territories to participate, and streamline administrative processes to accelerate implementation.

Shared Services Canada (SSC) plays a complementary but equally crucial role. As the operational arm of digital transformation, it is responsible for modernizing infrastructure, ensuring secure data hosting and strengthening the cybersecurity of systems. To fully support interoperability, SPC must develop common platforms accessible to all levels of government, harmonize technical protocols to facilitate data exchange, and collaborate closely with the provinces to avoid duplication and optimize the use of resources.

The Office of Digital Transformation (ODT), although still under development, has a pivotal role to play. It must function as the link between the strategy defined by TBS and its implementation by SPC. It must facilitate coordination among all stakeholders and identify high-impact use cases to demonstrate the concrete benefits of interoperability.

The positioning of the BTN within the TBS is not a mere organizational detail. It constitutes a structural choice. This configuration allows governance and coordination functions to be concentrated within a single institutional framework, whilst maintaining a clear separation from the operational functions conducted by SPC. This alignment is essential. It prevents the fragmentation of responsibilities and strengthens the overall coherence of the system. Without this coordination, efforts risk remaining fragmented and interoperability will never become an operational reality.

Official statistical agencies constitute an often-underestimated pillar of the FPT+ architecture. Their value is not limited to producing dashboards or time series: they ensure comparability, methodological consistency, the protection of confidentiality and the sharing of data from multiple jurisdictions. Statistics Canada’s specific mandate is to promote and develop integrated social, economic and environmental statistics, in collaboration with departments and agencies, whilst avoiding duplication; its mission is also based on reliable data, methodological rigour, independence, trusted statistical services, a robust infrastructure and the maintenance of public confidence.

To fully fulfil this role, statistical agencies will require an explicit mandate for inter-institutional coordination, rapid and secure access to administrative data, sustained investment in data infrastructure and metadata, as well as clear support for the standardisation of common classifications, definitions and identifiers. Without these conditions, interoperability will remain limited; with them, these agencies can become the foundation of trust, comparability and continuity upon which any FPT+ strategy for AI and digital sovereignty depends.

Roadmap for the next 12–24 months

To turn this vision into concrete results by 2028, Canada must focus on four priority and complementary actions. The first is to develop flagship use cases that tangibly demonstrate the value of interoperability. The St. Lawrence—Great Lakes corridor offers an ideal opportunity. By integrating logistics, energy and customs data from this strategic region, the government could demonstrate how interoperability improves coordination, strengthens resilience, and optimizes operations.

The second action aims to create a core of interoperable strategic data. This core should cover the critical areas underpinning the country’s competitiveness and security. These include supply chains, the domestic market, critical infrastructure, and public finances. By making this data accessible and compatible across different levels of government, Canada could support the development of advanced analytical capabilities. These capabilities would enable better crisis anticipation and more informed decision-making.

The third action involves establishing a clear and operational FPT+ governance framework. This framework must precisely define the responsibilities of each stakeholder. It must establish common rules for the flow of data between different levels of government. It must also provide for effective coordination mechanisms. Finally, it must incorporate robust safeguards for the protection of personal information, in order to maintain the trust of citizens and businesses.

The fourth initiative aims to strengthen institutional learning capacity. This involves setting up innovation labs where new approaches can be evaluated and refined. CIRANO and other independent bodies could be tasked with conducting regular evaluations to measure progress and identify obstacles. This learning capacity must also incorporate the transformations in the labour market brought about by AI, as highlighted in the report *AI and the Future of Work* (2025). This report highlights the need to train human resources across all sectors and disciplines in the new skills required by the data economy, particularly in predictive analytics, the management of technological dependencies, and the governance of interoperable systems. Without this adaptation of skills, the benefits of interoperability risk being limited by a mismatch between technical infrastructure and the human capacity to utilize it. Targeted training programmes should also be developed for civil servants, to equip them with the skills needed to work in an FPT+ interoperable data environment.

These four actions should not be viewed as isolated initiatives. They form the building blocks of a coherent and integrated strategy. Their coordinated implementation could create a positive knock-on effect. By demonstrating the concrete benefits of interoperability, it would strengthen the public sector's capacity for integration. This capacity has become essential in a world marked by accelerating geopolitical transformations, the consolidation of technological architectures dominated by a few players, and the rise of hybrid risks.

Time is running out. The window of opportunity is limited. Without swift and coordinated action, Canada's strategic room for manoeuvre will be significantly reduced. The decisions taken over the next 12 to 24 months will determine whether the country can transform its strengths into an integrated strategic capability or whether it will remain trapped in the current fragmentation.

Beyond architectures and governance frameworks, the success of interoperability depends on genuine adoption by organisations and individuals. However, such adoption cannot be imposed: it depends on clear incentives, perceived short-term benefits and the reduction of organisational costs associated with change. Without aligned incentives, the force of the status quo and silo-based thinking tend to persist, even in the presence of shared infrastructure.

Concrete mechanisms must therefore be considered: funding conditional on data integration, performance indicators linked to inter-institutional collaboration, recognition of contributions to data sharing, and simplification of access processes. Interoperability then becomes not only possible, but rational from the perspective of the stakeholders who must implement it.

Conclusion

The geopolitical landscape has changed radically. The resurgence of tensions between major powers, Sino-American rivalry, the politicization of economic dependencies and targeted sanctions have redefined the rules of the game. Defence considerations, traceability requirements, and pressure on critical minerals have transformed supply chains. They are no longer merely vehicles for trade. They have become instruments of power, resilience and, at times, vulnerability.

In this new strategic environment, one truth stands out: a state that does not control its data cannot control its decisions. The integration of public data at the FPT+ level is no longer an option. It is now an essential condition of Canadian sovereignty. This development has three major consequences.

Firstly, access to foreign markets remains crucial for Canada. But it is becoming increasingly uncertain and costly. Non-tariff barriers are multiplying. Economic alliances are being reconfigured. Supply chains are becoming regionalized. Secondly, geographical proximity, the quality of institutions and the reliability of logistics corridors are taking on greater importance. In a world where distances are also measured in response times, these assets become decisive competitive advantages. Thirdly, a state's ability to rapidly coordinate its stakeholders and maintain a real-time view of its economy is becoming a key factor in competitiveness. The smooth flow of trade is no longer sufficient. The internal integration of data and decision-making systems is becoming just as important.

These transformations explain why the various issues can no longer be addressed separately. Trade, logistics, critical minerals, infrastructure, data governance, and AI are now part of the same strategic agenda. The central question is this: will Canada succeed in establishing a coherent economic architecture? An architecture that would enable it to respond more quickly to crises, plan its actions with greater precision, reduce internal friction, and enhance its credibility on the international stage?

This paradigm shift also requires an evolution in the language of public policy. It is no longer enough to treat the flow of trade, digital innovation, or productivity as separate areas of focus. We must now speak of an integrated national system. A system in which goods, data, and decisions flow in a coordinated manner. The St. Lawrence—Great Lakes Corridor offers a concrete illustration of this. This project demonstrates how the integration of logistics, energy, environmental, urban, and custom data can transform a region into a genuine driver of national competitiveness.

For Canada, this transformation represents both a major challenge and a historic opportunity. The country already possesses the necessary elements: strong institutions, abundant energy resources, and a world-class scientific ecosystem. The challenge is not to create these assets, but to connect them strategically. The interoperability of public data is the central lever of this integration. It enables structural fragmentation to be transformed into a shared strategic capability. It offers a concrete pathway to strengthening Canada's decision-making autonomy in a globalized and competitive environment.

Data integration is not an end in itself. Its value lies in its ability to transform information into informed, rapid and consistent decisions. This requires close alignment between data systems, analytical capabilities and decision-making processes. Without this integration, even the most advanced architectures risk delivering limited benefits.

The challenge for Canada is therefore to complete the data value chain: from collection to integration, from analysis to action. This ability to 'close the loop' between information and decision-making represents the true strategic advantage in an environment characterised by uncertainty, rapid change and complex challenges.

Canadian sovereignty cannot be conceived as a retreat into isolation. On the contrary, it must be active participation in the global system. Participation that allows dependencies to be structured whilst preserving room for manoeuvre. It rests on three fundamental capabilities: understanding complex dynamics, integrating different systems, and making informed decisions. In the economy of artificial intelligence, sovereignty cannot be improved. It is built methodically. It emerges from the coherence of systems and the quality of decisions. It is orchestrated through an integrated strategic vision. It is this capacity for integration that will make Canada a sovereign and influential player in the digital economy of the 21st century.

Annotated bibliography

Barbet, P. (April 2026). *The Stargate Project: The risks of the race for gigantism in data centres dedicated to artificial intelligence*. IRIS, Geopolitical Observatory of Digital and Emerging Technologies.

This study analyzes the physical and geopolitical dimensions of AI infrastructure, focusing on the Stargate project. It documents the scale of this project, the risks of industrial concentration it entails, and the energy and competitive implications of the industrialization of data centres. The author highlights the sovereignty issues linked to dependence on massive computing infrastructure and proposes strategies for middle powers such as Canada.

Beaumier, G. & Cadieux, H. (2026, 8 April). *Canada must develop its own AI computing power*. Institute for Research on Public Policy (IRPP). <https://policyoptions.irpp.org/fr/2026/04/ia-infrastructure-publique/>

This essay highlights the strategic importance of computing power as a bottleneck for AI development. The authors highlight the international concentration of computing capacity and the resulting structural dependencies for countries such as Canada. They propose public intervention (direct or hybrid) to support the development of national infrastructure, justified by market failure. This analysis complements the work of McKinsey and the Munk School, particularly in relation to its operational perspective focused on critical infrastructure.

Dudoit, A. (2025). *Federal-Provincial Data Interoperability and AI Adoption: Leveraging Current Federal-Provincial Dynamics and the Canada-EU Strategic Partnership* (2025RB-02, Bourgogne Reports, CIRANO). <https://doi.org/10.54932/AXET1370>

This report recommends two urgent measures: the conclusion of an FPT agreement on data interoperability and the creation of a permanent council on AI and interoperability. These proposals are not merely technical adjustments, but strategic foundations for any national development project. The author highlights the importance of coordination between levels of government and the potential of the Canada-EU partnership as a lever to accelerate the modernization of public systems. This work lays the groundwork for CIRANO's subsequent analyses on data integration as critical infrastructure.

Dudoit, A., Labillois, T. & Oliveira, C. (2026). *Public Sector Data Interoperability in Canada and the Responsible Adoption of AI: Strategic Synthesis and Call to Action* (2026PR-01, For Consideration, CIRANO). <https://doi.org/10.54932/VOKC1489>

This report forms the conceptual foundation of the present update. It establishes the link between interoperability, economic performance, public governance, and the responsible adoption of AI. The authors develop the idea that data interoperability is not merely a technical project, but a prerequisite for institutional transformation and economic resilience. This document inspired subsequent recommendations on the integration of FPT+ systems and the creation of a unified strategic capacity in Canada.

Goldfarb, D. (March 2026). [*Intelligent governance: Using AI for Canadian strategic intelligence gaps*](#). CSA Public Policy Centre.

This study is central to understanding AI as a tool for public capacity. It identifies four low-risk, high-return areas of application: supply chain visibility, Arctic surveillance, critical mineral management and economic early warning systems. The author demonstrates that Canada's main challenge lies in the fragmentation of strategic information and proposes solutions to address these gaps through intelligent governance. This work sheds light on the role of AI in enhancing resilience and sovereignty.

Government of Canada. (2023). [*Data Strategy 2023–2026 for the Federal Public Service*](#).

This document provides the government framework for data governance, responsible use, and data-driven decision-making. It directly supports the argument that interoperability is not merely a technical add-on, but a prerequisite for institutional transformation. The strategy emphasizes data quality, accessibility, and security, whilst highlighting the importance of alignment across different levels of government. It serves as the official reference for federal initiatives on the modernization of data systems.

Government of Canada (2025) [*Annual Report on the 2023–2026 Data Strategy for the Federal Public Service—Year Two*](#)

This second annual report assesses progress made in implementing the 2023–2026 Data Strategy for the Federal Public Service. It highlights concrete advances in data governance, improvements in data quality and the adoption of data-driven practices within departments. The report highlights three key priorities: harmonizing standards to facilitate interoperability between federal systems. Strengthening data security and protection, particularly in the context of growing cyber threats; Integrating data into decision-making, with concrete examples of pilot projects (e.g., the use of AI for predictive analytics).

The document complements the departmental plans of TBS and PCH by providing performance indicators and lessons learnt after two years of implementation. It offers an operational perspective on the challenges encountered, notably the persistent fragmentation of systems and the need for greater coordination among federal stakeholders, which reinforces the arguments developed in this publication regarding the urgency of coherent FPT+ governance.

Government of Canada. (2026). [*Treasury Board of Canada Secretariat Departmental Plan 2026–2027*](#).

This departmental plan is a key source for understanding the TBS's role in data governance, digital transformation, and the adoption of AI. It confirms that the TBS is positioning itself as a focal point for these issues, incorporating cybersecurity, the review of digital policies and support for the creation of the Office of Digital Transformation. This document illustrates the shift in federal priorities towards a more integrated and strategic approach to data and AI.

Government of Canada. (2026). [*Shared Services Canada's 2026–2027 Departmental Plan*](#).

This plan is essential for documenting the federal government's capacity to deliver in the area of digital transformation. It highlights the role of Shared Services Canada (SSC) in infrastructure modernization, secure hosting, cybersecurity, and platform integration. The document also highlights the importance of SPC for operational digital sovereignty, demonstrating how investments in technical infrastructure support the strategic objectives defined by TBS. It complements the TBS plan by illustrating the complementarity between governance and delivery.

Government of Quebec. (2026). [*Policy Statement on Digital Sovereignty and Information Technology Procurement*](#).

This statement offers a Canadian concrete example of digital sovereignty in action. It focuses on infrastructure (government cloud, data localization), secure hosting, the governance of technology procurement and strategic choices regarding partnerships. Whilst illustrating Quebec's progress, it also reveals the limitations of a purely infrastructure-based strategy lacking interoperability on a larger scale. This document demonstrates how a province can structure its digital sovereignty, whilst highlighting the need for pan-Canadian coordination to maximize the impact of these initiatives.

Human Technology Foundation (2025) [*Report on AI and the Future of Work*](#).

This report examines the impact of artificial intelligence on work organization and productivity, highlighting a significant gap between technological investment and the gains observed. It emphasizes that the main constraints do not lie in the technical capabilities of AI, but in difficulties with organizational integration, governance shortcomings, and skills gaps. By emphasizing the centrality of human, institutional and operational factors, this report complements existing infrastructural analyses of AI by demonstrating that performance depends above all on organizations' ability to integrate these technologies into coherent systems. In the Canadian context, these findings reinforce the importance of public data interoperability and integrated governance as prerequisites for effectively transforming technological capabilities into institutional performance.

McKinsey & Company. (Collaborative article) (2026, 3 March). [*Sovereign AI: Building ecosystems for strategic resilience and impact*](#).

This report is fundamental to understanding sovereign AI as an ecosystem issue. McKinsey demonstrates that sovereignty is not built in isolation, but through the interplay between energy, computing power, data, models, platforms, and applications. The authors propose a framework for evaluating AI ecosystems and identifying levers to strengthen strategic resilience. This work directly influences the Canadian conception of interoperability as critical infrastructure and the importance of linking technical capabilities to strategic objectives.

Mullin, S., & Khan, J. (2026, 6 March). [*Sovereign by design: Strategic options for Canadian AI sovereignty*](#). Munk School of Global Affairs & Public Policy.

This text is significant for Canada's positioning within the AI landscape. The authors redefine sovereignty not as self-sufficiency, but as the absence of external constraints that limit strategic choices. They assess Canadian vulnerabilities across five dimensions: legal, operational, technological, societal, and economic. This analysis complements the work of Chatham House by offering a multidimensional assessment framework to guide decisions on digital sovereignty and interoperability.

Omaar, H., & Pasricha, M., Center for Data Innovation. (2026). *AI data centres and the future of infrastructure policy: Rethinking electricity, pricing, and environmental impact*.

<https://www2.datainnovation.org/2026-ai-data-centers.pdf>

This report examines the challenges associated with the expansion of AI data centres, including electricity consumption, network access, pricing, reliability and water usage. It shifts the debate from a focus on infrastructure constraints to an analysis of the governance frameworks needed to integrate these infrastructures into energy systems. The study highlights the role of pricing mechanisms and cost-allocation rules in managing economic and social impacts, whilst demonstrating that modernized frameworks can reconcile the expansion of digital capacity, consumer protection, and environmental sustainability. Although focused on the United States, this analysis offers lessons directly applicable to Canada, particularly regarding federal-provincial coordination.

Sandoval, F., J. & Wilkinson, I., Chatham House. (2026). [*How middle powers can weather US and Chinese AI dominance: The case for "sovereign AI" strategies*](#).

This report proposes a framework for analysis relevant to middle powers such as Canada. It demonstrates that sovereignty in AI does not mean self-sufficiency, but rather the ability to manage dependencies through strategies of specialization, alignment, shared sovereignty, or diversification. The authors identify strategic options for countries unable to compete with the tech giants, emphasizing the importance of structuring partnerships and ecosystems. This theoretical framework sheds light on Canada's choices regarding data interoperability and AI governance.