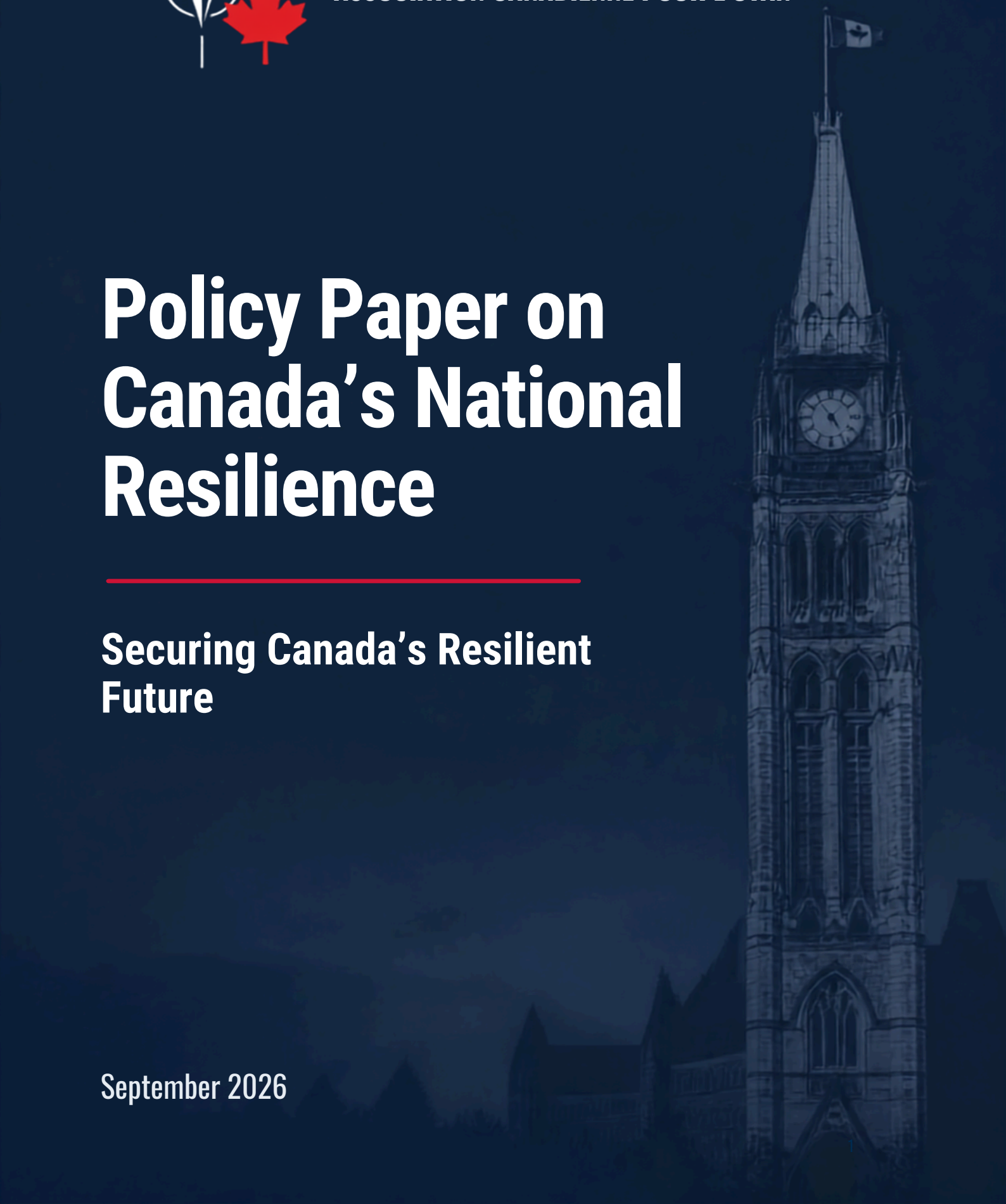
NATO ASSOCIATION OF CANADA |
ASSOCIATION CANADIENNE POUR L'OTAN

Policy Paper on Canada's National Resilience

Securing Canada's Resilient Future



September 2026

Table of Contents

Editorial Team

Managing Editor: Daria Synelnykova
Design Editors: Keya Patel, Manjinder Kaur, Selina Khan

Foreword

Hon. David Collenette, PC, O.Ont
Chair, NATO Association of Canada

As tensions and conflicts grew in an increasingly turbulent world, NATO allies in 2016 agreed on seven Alliance-wide baseline requirements for national resilience. These requirements were intended to ensure that member states build the capacity to continue delivering essential services, including energy, food, healthcare, transport, and communications, in times of crisis. Alongside other NATO members, Canada has committed to strengthening its resilience in line with these requirements.

Ten years later, we are seeing an acceleration in world tensions. Some observers feel that the nature of warfare is evolving at a rapid and disruptive pace, with profound implications for national security, defence innovation, and international stability. Warfare today is being fought across land, sea, air, cyber, and space. These developments are reshaping operational doctrines, force modernization efforts, and strategic decision-making at every level. Along with longstanding and emerging challenges ranging from climate change and digital threats to a changing geopolitical environment, this all contributes to an urgent need for national resilience. Reflecting these developments, NATO's 2026 revision of the Baseline Requirements considers a wider range of cross-cutting risks, including an increased emphasis on cyberattacks, emerging technologies, strategic dependencies, extreme weather events, and reliance on space-based assets.

NATO's renewed spending agreement allocates 1.5% of GDP for defence- and security-related investments, including critical infrastructure and resilience. This is over and above the 3.5% of GDP directed to military spending. All these investments reinforce the essential services and infrastructure on which Canadians rely both in their daily lives and in times of crisis.

Against this backdrop, the NATO Association of Canada has produced a Policy Paper on Canada's National Resilience. Each chapter examines a distinct dimension of resilience, assessing how Canada's current policies and their implementation position the country to meet NATO's baseline requirements and strengthen domestic resilience. Our authors highlight the many areas of achievement and progress Canada has already made. They also identify areas for further improvement and draw inspiration from Canada's allies in proposing ways to address remaining gaps.

Introduction

Justin Michael James Dell, NAOC Editor-in-Chief

History has made a violent return of late.[1] Geopolitical flashpoints, from Russia's illegal war against Ukraine, to internecine bloodshed in the Middle East, to a more unpredictable United States foreign policy, have punctured and deflated the heady hopes of the post-Cold War era. The international system of today seems to be drifting more towards the seventeenth-century British philosopher Thomas Hobbes' infamous description of the state of nature – "solitary, poor, nasty, brutish, and short" – than to Emmanuel Kant's vision of the "perpetual peace" he longed to see enjoyed by a confederation of democratic republics covering the surface of the globe.[2]

One should not become too despondent at this picture. A generous inheritance of institutions that were founded immediately after the Second World War designed to maintain relative peace and prosperity across the globe has been bequeathed to the world's society of states, especially those of the Euro-Atlantic region, which were the principal architects of the rules-based international order. Those primary institutions crystalized in the founding principles of the United Nations – among them sovereign equality, territorial inviolability, open trade, the human rights regime, and international justice – are still available to states willing to elevate them, abide by them, and defend them. They have a proven historical track record of facilitating impressive, albeit imperfectly distributed, results in human flourishing.[3]

While these institutions yet live, they are being stress-tested. Some of the most intense pressure facing them is coming from their erstwhile champions, who have become some of their fiercest critics. As the eminent international relations scholar G. John Ikenberry argues in A World Safe for Democracy (2020), the Euro-Atlantic core of states collectively known as "the West" will have to consolidate and defend these institutions at home if they are to survive, not only from hostile foreign actors, but also from domestic threats.[4]

In their clairvoyance, the founders of the North Atlantic Treaty Organization, men who had been profoundly shaped by the failure of the League of Nations and the ensuing devastation of the Second World War, knew that the global institutions of the post-1945 rules-based international order would not be secure without a nucleus of states prepared to defend them – militarily, if necessary. For this very reason, NATO was born. It committed its members to upholding the multilateral system centred on the United Nations, its charter, and its ancillary organizations, but it also bound them to rely on each other and on themselves as the guarantors of that system. Embedded in the North Atlantic Treaty is the oft-overlooked Article 3: "In order more effectively to achieve the objectives of this Treaty, the Parties, separately and jointly, by means of continuous and effective self-help and mutual aid, will maintain and develop their individual and collective capacity to resist armed attack."[5]

It is this noble third article of the treaty that enjoins NATO members to cultivate, practise, and perfect national resilience, both individually and in concert. How to effectuate this national resilience is the central focus of this publication. The North Atlantic Treaty is a living document, the rights and responsibilities of which have been unpacked, expanded, and proved over the last seventy-five years.[6] NATO's understanding of resilience has thus become more layered and nuanced with the passage of time. The threat of "armed attack" invoked by Article 3 remains NATO's primary concern, especially in a world of growing great-power politics and rivalry. However, many other threats, from climate change to pandemics, have become more manifest in recent decades, and while they may not constitute an "armed attack," they potentially intensify or multiply more conventional security threats. In a world of growing complication, interconnection, and potential for harm, NATO's threat profile has had to evolve beyond the rather one-dimensional concept of "armed attack."[7]

Reflecting this changing threat landscape and the need for members to adapt to it, NATO has established seven baseline requirements for national resilience: (1) assured continuity of government and critical government services, (2) resilient energy supplies, (3) ability to deal effectively with the uncontrolled movement of people, (4) resilient food and water resources, (5) ability to deal with mass casualties and disruptive health crises, (6) resilient civil communications systems, and (7) resilient transport systems.8 The NATO Association of Canada has produced the following compilation of policy proposals as a primer for Canadian policymakers, legislators, business leaders, educators, and even ordinary citizens to make Canada's national resilience a reality in their own respective ways. National resilience requires a whole-of-society approach, and the NATO Association of Canada has sought to produce a document that comprehensively addresses the most pressing challenges facing Canada's resilience from angles that touch upon NATO's seven baseline requirements.

In Chapter 1 of this compilation, Critical Infrastructure Resilience, Bogdana Torbina sets the context of a discussion of national resilience by surveying the state of Canada's "critical infrastructure" (CI). This comprehensive term refers to the composite of physical structures, resources, and utilities that make up the foundation of a functioning society. Canada is a sophisticated modern state that delivers vast quantities of goods and services to its population. However, with this richness comes vulnerabilities. Physical capital, such as roads and factories, is vulnerable to neglect and wear. Government services can be disrupted by hostile actors using digital technology. Water treatment systems can be sabotaged. In times of national crisis, CI is vital to a country's survival and, in particular, its ability to defend itself militarily. Torbina observes that while Ottawa is aware of threats posed to Canada's CI and has drafted policies meant to meet them, follow-through, coordination with other branches of government, and accountability have proved difficult to obtain. She looks to Canada's partners, among them Australia, Estonia, Finland, and the EU, for models Canada can emulate, especially as it relates to the clear delegation of responsibilities to branches of government, as well as a decentralized, whole-of-society approach to national resilience that rallies even the common citizen to that effort.

If critical infrastructure is the foundation of national resilience, economic resilience is its precondition. This is the subject of Chapter 2, Economic Resilience and Supply Chains, by Lou Didelot. Beginning with the General Agreement on Tariffs and Trade (GATT) of 1947, the architects of the rules-based international order envisioned ever-expanding trade between states as laying the groundwork for lasting international peace. Unfortunately, pivots toward populist economic policies, protectionism, and external shocks, such as the COVID-19 pandemic, have underscored the vulnerability of international supply chains. The modern wave of globalization has prioritized economic efficiency above all, even security. Didelot argues that Canada needs to restore balance to these trade-offs, zealously pursue more diverse markets for Canadian exports, and stockpile strategically vital economic inputs. Once again, Canada can look to its NATO allies for models to emulate in this regard.

Moving on to a quintessentially 21st-century dimension of national resilience, Esha Grewal and Daria Synelnykova examine respectively the twin concepts that make up Chapter 3, Cyber Resilience and Digital Sovereignty. The ethereal and transnational nature of the digital world has presented NATO with a front its architects could not have anticipated. Cyberattacks have become a regularity in Canada, Grewal grimly notes, and the difficulty in meeting this threat is compounded by the fact that the public and private sectors both have different priorities in facing it. This makes a unified, national response problematic. Similarly to other contributors, Grewal looks to NATO allies for inspiration, arguing that a big part of cyber resilience involves mobilizing the broader population in a whole-of-society approach, as certain Baltic countries have already done. On the flip side of the coin from cyber resilience, Synelnykova looks at the issue of digital sovereignty, and the vulnerabilities Canada faces from data storage in other countries or jurisdictions. Echoing the trope surrounding the drawbacks of globalization and offshoring, she sounds the alarm regarding Canada's over-reliance on partners for digital services who may no longer be worthy of such trust.

Keya Patel's Public Health constitutes Chapter 4 of this volume. That Canada's vaunted healthcare system is a matter of immense pride for many Canadians there can be no doubt. However, it is being held up by pillars that could potentially give way in a moment of national crisis. Patel notes that Canada faces a significant doctor shortage compared to other OECD states, and while it is on comparatively firmer ground as it relates to nursing, it has problems retaining these vital staff. Many of the challenges associated with critical infrastructure and economic security are applicable to Canada's health resilience, namely as they relate to the downsides of globalization. The health of Canada's population depends on inputs procured abroad, from pharmaceuticals to personal protective equipment (PPE). COVID-19 exposed the folly of this arrangement. What Canada ultimately needs to address these weaknesses is a top-down, unified federal approach to healthcare resilience. This carries with it particular challenges for Canada's federalist governance system, where provinces jealously guard their healthcare responsibilities. Patel looks to Finland and the United Kingdom for answers to the question of how Canada might be able to architect a solution to this conundrum.

Maya Khachab's Chapter 5, Environmental and Natural Disaster Preparedness and Response, will resonate with readers still reeling from a summer of grave ecological challenges that beset both sides of the Atlantic Community this year, from forest fires that blanketed eastern North America with smoke to unprecedented heat waves in Europe. For years, Canada's provinces and territories have had the option of activating Operation LENTUS, entailing the intervention of the Canadian Armed Forces in emergencies that exceed provincial and territorial resources. Reliance on the CAF has grown as the number and intensity of disasters has increased. While having the option of Operation LENTUS is reassuring, Khachab notes that this disincentivizes provinces and territories from resolving emergencies on their own. While the CAF can serve in the secondary role of emergency response, this backstop capacity is not its real purpose. Disaster response is a function best left to civilians, which is why Khachab argues that the time has come for the constitution of a civilian federal corps to provide the logistical wherewithal and expertise needed to complement provincial and territorial efforts at resolving emergencies in their jurisdictions. Such a corps would be a particularly useful adjunct in the Canadian North, where the ravages of climate change, the imperative of Indigenous inclusion in governance, and the challenge of maintaining dual-use infrastructure converge.

In Chapter 6, Education and Information Resilience, Dr. John Walsh and Darren Sargent take the reader back in time to an age when a nation's resilience was thought to begin with, and flow from, its didacticism. A polity can have all the material resources at its disposal to repulse an enemy, but without a clear conception of the ultimate ends to which those means are put, it lacks the spirit with which to animate a defence of itself. Citizens have to know what they are fighting for. This is where education intersects with national resilience. For Walsh and Sargent, this issue is more than theoretical speculation. Both men operate the Serving Scholar Program (SSP) at the University of Guelph, a pilot initiative designed to equip serving members of the CAF to pursue post-secondary education, as well as to foster a culture of complementarity between the military and the academy in Canada. The upshot of SSP and other educational initiatives will not be the encroachment of the military onto the academy or vice versa, but rather their mutual edification and the development of a spirit of comity between them. The ultimate guarantor of Canada's national resilience is a population that not only knows how to defend her, but why.

The academy may instill the proper virtues in Canadian youth necessary for national resilience, but the downstream issue remains regarding how young people might become practically involved in contributing to the country's readiness. Rudy Yuan looks at the available options in Chapter 7, Youth Engagement and Civil Preparedness. Military service is certainly one of these. However, he cautions against the idea of conscription. Canada, he argues, does not have the infrastructure or cultural buy-in to implement such a policy. However, Yuan notes that credible government data indicates that Canadian youth are motivated, conscientious, and seek engagement. But they must be "met where they are" and given choice regarding how they might serve the country. Canada possesses mature organizations, such as the Canada Service Corps, the purviews of which can be expanded to incorporate a greater emphasis on civil defence

in their programs. Yuan observes that four out of seven of NATO's baseline requirements for national resilience depend on civil defence to one degree or another. A generation raised up in a culture of readiness is absolutely vital to the whole-of-society approach needed to buttress government efforts at ensuring national resilience. Government can only do so much. Society must make up the difference.

The NATO Association of Canada is confident that while the following chapters present the unvarnished truth regarding the vulnerabilities Canada faces to its national resiliency all along the various fronts discussed herein, the attendant policy proposals this document offers are sound, practical, and achievable ideas which, if implemented, will measurably reduce those risks. That many of the proposals look to other NATO members and partners for inspiration is a testament to the enduring worth of Canada's commitment to the North Atlantic Treaty. Canada's implementation of these policies, whether in whole or in part, would immeasurably advance its compliance with Article 3. As a consequence, Canada, using its own abilities, and in concert with its allies, can continue to uphold the rules-based international order, which for over eighty years has continued to deliver unprecedented peace and prosperity for humankind. The NATO Association of Canada is deeply grateful to the volunteers who have authored the chapters of the following compilation, its editorial team, and the numerous experts who have generously given of their time to ensure the accuracy of its contents.

Endnotes

1. Francis Fukuyama, "The End of History?," The National Interest, no. 16 (1989): 3–18.
2. Hedley Bull and Stanley Hoffmann, The Anarchical Society: A Study of Order in World Politics, 4. ed (Columbia University Press, 2012).
3. Elizabeth Borgwardt, A New Deal for the World: America's Vision for Human Rights, 1st ed (Harvard University Press, 2007).
4. G. John Ikenberry, A World Safe for Democracy: Liberal Internationalism and the Crises of Global Order, Politics and Culture (Yale university press, 2020).
5. Ian Shapiro and J. Adam Tooze, eds., Charter of the North Atlantic Treaty Organization: Together with Scholarly Commentaries and Essential Historical Documents, Basic Documents in World Politics (Yale University Press, 2018).
6. Stanley R. Sloan, Defense of the West: NATO, the European Union and the Transatlantic Bargain (Manchester University Press, 2016).
7. Joshua Cooper Ramo, The Age of the Unthinkable: Why the New World Disorder Constantly Surprises Us and What We Can Do about It, First Back Bay paperback edition (Back Bay Books, 2010).
8. "Resilience, Civil Preparedness and Article 3," Site Name Seo, accessed September 8, 2026, https://www.nato.int/en/what-we-do/deterrence-and-defence/resilience-civil-preparedness-and-article-3.

Author: Bogdana Torbina, Chief of Staff

Chapter 1. Critical Infrastructure Resilience

Executive Summary

Canada's critical infrastructure underpins civilian continuity, military readiness, and national resilience. However, Canada's current approach to protecting critical infrastructure remains fragmented, outdated, and overly reliant on predominantly voluntary cooperation between public and private-sector actors. As climate change, cyberattacks, aging infrastructure, and global supply chain disruptions become more frequent and interconnected, these vulnerabilities threaten the continuity of essential services and Canada's ability to respond to crises. While the 2009 *National Strategy for Critical Infrastructure* established a foundation for cross-sector collaboration, it lacks clear accountability mechanisms, standardized resilience assessments, and an integrated civil-defence strategy aligned with NATO's Resilience Baseline Requirements.

Main Policy Recommendations

- **Modernize Canada's National Strategy for Critical Infrastructure** to reflect the current threat environment, as well as the evolution and increasing interdependence of Canada's critical infrastructure sectors. The strategy should include clearer governance, accountability mechanisms, and standardized resilience assessments for nationally significant infrastructure. A cross-government task force should be established to map the cross-over in tools and strategies across critical infrastructure, emergency preparedness, and national defence for whole-of-society resilience in time of disruptions.
- **Embed mandatory risk assessments and resilience standards** into regulation and public procurement.
- **Adopt an integrated whole-of-society approach** that aligns critical infrastructure planning with national security, emergency preparedness, and NATO resilience commitments.
- **Improve public preparedness and awareness** through national disruption preparedness education and engagement initiatives.

Introduction

"Resilience is our first line of defence," noted NATO Secretary General Mark Rutte in a speech earlier this year. "Resilience is everyone's responsibility."[1] Russia's full-scale invasion of Ukraine in 2022 confronted Canada and NATO allies with the consequences that modern kinetic and hybrid warfare can have on a country's critical infrastructure (CI) and essential services when they are not designed to withstand significant disruption. The World Bank estimates that the direct physical damage to Ukraine's CI has reached CAD 195 billion, with housing, transport, and energy sectors being most affected.[2] Russia systemically targets not only militarily critical targets, but also civilian infrastructure, creating socio-economic vulnerabilities which divert attention and resources from Ukraine's defence. Russia continuously strikes power-generating substations, distribution networks, railways, ports, logistics infrastructure, and communications systems, reducing the country's economic capacity, public morale, and societal resilience.[3]

Across the Alliance, countries are beginning to realize that the rapid development of hybrid warfare means that a physical attack is not necessary to compromise their physical CI and essential services. In 2023, a cyber incident temporarily disrupted credit- and debit-card processing at Petro-Canada retail gas stations nationwide. A 2023 Daixin ransomware incident forced temporary shutdowns of internal health systems, led to theft of sensitive files, and delayed health services for five hospitals in Southern Ontario. In 2024, a ransomware incident affected IT systems used to manage the City of Hamilton's municipal functions, including city telephone lines, which were closed for a week.[4] In 2025-26 alone, the Cyber Centre recorded more than 3,200 cyber incidents affecting Government of Canada institutions and CI sectors.[5] Beyond cyber disruptions, Our North, Strong and Free: A Renewed Vision for Canada's Defence identified growing Russian and Chinese physical activity in the Arctic, including Russia's Arctic naval presence and China's expanding naval and submarine capabilities, alongside foreign exploration of Arctic waters and the seafloor, infrastructure probing, and intelligence collection.[6]

> **"The rapid development of hybrid warfare means that a physical attack is not necessary to compromise physical CI and essential services."**

The protection of CI is inherently intertwined with NATO's Article 3 and each of the Seven Baseline Requirements for National Resilience, as the CI sectors act as foundations enabling society's continued functioning. Public Safety Canada defines critical infrastructure as the "processes, systems, facilities, technologies, networks, assets and services essential to the health, safety, security or economic well-being of Canadians and the effective functioning of government."[7] Resilience is described as the ability of a system, community or society to adapt to and recover from disruptions.[8]

Canada's 10 CI sectors listed by Public Safety Canada include:[9]

1. **Energy and Utilities:** electricity grids, power plants, natural-gas networks, fuel depots, utility control rooms
2. **Finance:** banks, credit unions, stock exchanges, online-banking systems
3. **Food:** farms, food-processing plants, cold-storage facilities, distribution centres, grocery supply chains
4. **Government:** defence, emergency operations centres, government data and benefits systems, municipal offices, legislatures
5. **Health:** hospitals, ambulances, medical laboratories, blood-supply systems, long-term-care facilities
6. **Information & Communications Technology:** fibre-optic cables, cell towers, internet service providers, satellites, data centres
7. **Manufacturing:** defence-industrial base, factories, steel and aluminum plants, automotive and aerospace manufacturing facilities, warehousing and industrial supply chains.
8. **Safety:** police stations, fire halls, emergency dispatch/911 systems, search-and-rescue facilities, emergency shelters, disaster-response coordination centres.
9. **Transportation:** highways, bridges, railways, airports, ports, ferries, public transit, trucking and logistics hubs
10. **Water:** drinking-water treatment plants, reservoirs, water mains, sewers, wastewater and stormwater systems

The fundamental policy gap Canada must address to strengthen national resilience is the need to recognize CI resilience as essential towards sustaining the continuation of society and for supporting military readiness in times of disruptions. As NATO states, militaries "depend heavily on the civilian and commercial sectors for transport, communications, energy and even basic supplies such as food and water, to fulfil their missions."[10] For example, approximately 90% of military transport relies on civilian ships, railways, and aircraft during large operations and exercises.[11] Inuvik's Mike Zubko Airport is a Northwest Territories-owned civilian airport which also serves as an RCAF/NORAD Forward Operating Location.[12] CI also serves as the foundation of the Canadian Armed Forces (CAF) domestic disaster assistance Operation LENTUS, such as during the 2025 wildfires in Cross Lake, Sandy Lake, and Garden Hill, which required usable local runways, airfield access, and ground coordination for evacuations.[13] Finally, CI resilience supports both the physical capacity of the CAF in responding to disruptions, as well as ensuring socio-economic stability, allowing a more efficient distribution of resources towards countering pressing threats.

Canada's CI is not keeping up with the changing threat environment and modernization of NATO Allied CI policies. Canada's CI is aging, geographically dispersed, digitally interconnected, and vulnerable to the heightened threat environment posed by a changing climate, increased cyber attacks, global supply-chain disruptions, and

fragmented CI assessment and regulation. The 2025 NATO Summit in The Hague saw a policy commitment to increase Allied resilience through the 1.5% GDP resilience and security-related investments as part of the new 5% GDP defence spending goal.[14] Canada has committed to reaching the 5% spending target by 2035. The North American and Arctic Defence and Security Network (NAADSN) has already made the argument for the 1.5% category to justify major infrastructure investments linked to NATO's civil preparedness and resilience priorities, using NATO's baseline requirements as a framework for infrastructure spending.[15] This chapter aims to assess the current baseline of Canada's CI amidst a new threat environment, evaluate current CI resilience policies, provide a comparative study of existing NATO member and partner state CI resilience policies, and propose policy recommendations to strengthen CI for Canada's national resilience.

> **"Canada's CI is aging and geographically dispersed. It is vulnerable to the heightened threat environment posed by a changing climate, increased cyber attacks, global supply-chain disruptions, and fragmented CI assessment and regulation."**

Critical Infrastructure Threat Environment and Structural Vulnerabilities

Canada's CI threat environment is shaped by interconnected vulnerabilities that compound across sectors, systems, and geography. Today's threat environment is shaped by climate-change-fueled environmental disasters, state-sponsored cyberattacks, aging assets, fragmented governance, and vulnerable supply-chains. These threats have uneven distribution and impact across the country, with northern and Arctic communities being more vulnerable. These pressures create socio-economic vulnerabilities, weaken emergency-response capacity, generate defence and security risks, and undermine Canada's domestic resilience and ability to meet NATO's baseline requirements.

Climate-Change Hazards & Environmental Disasters

Natural disasters constitute 69.9% of all disasters in Canadian history.[16] In the 2024 Disruptions on the Horizon report, climate change-related natural disasters overwhelming Canada's emergency-response systems ranked third among the ten most significant potential disruptions. The risk is expected to emerge as early as 2030.[17] The effects are however already becoming increasingly apparent. In July 2026, Canada

experienced one of its worst wildfire seasons on record, with more than 900 wildfires burning across the country.[18] The federal Government Operations Centre activated Level 3 for wildfire response,[19] while CAF deployed four CC-130 Hercules aircraft to assist with the evacuation of Eabametoong First Nation in Northern Ontario.[20] Quebec received assistance from the United States and France amidst an overwhelming lack of local resources.[21] CAF were also placed on standby to assist with fires in British Columbia.[22] Canada's CI is not prepared to withstand the evolving natural environment threats compounded by climate change-induced changes. Some threats facing infrastructure include more heatwaves, shorter ice-road seasons, thawing permafrost, drought, heavier rainfall, rising seas, and stronger storms. These hazards can damage roads, buildings, ports, utilities, and data centres while disrupting water, energy, and communications services, among others.[23] Northern and First Nations communities are at a heightened risk of being disproportionately affected by emergencies due to a greater CI disparity in those parts of Canada.[24]

Infrastructure Governance

Canada's CI ownership and responsibility is diffused widely across a vast and unevenly populated country. The increasing digitalization and interdependence of CI systems increase both the vulnerability and complexity of coordination between CI actors. Approximately 85% of Canada's 10 CI sectors are owned and operated by non-federal entities, primarily private industry, alongside provincial, municipal, and other public-sector actors, creating a complex web of shared responsibility. Moreover, the interconnectedness between Canadian and U.S. infrastructure systems, such as energy, means that U.S. infrastructure vulnerabilities can have a cross-border effect on Canada's resilience and security. Due to the complexity and interwoven nature of actors involved in owning and operating Canada's CI, there is no one level of government or owner to sustain responsibility. Instead, Public Safety Canada focuses on facilitating dialogue among relevant actors. The difficulty of private-public cooperation is compounded by a divide in threat mitigation focus. Whereas the public focus lies with large-scale disasters and malign interferences, the private sector focuses on day-to-day infrastructure failures, reputation mitigation, and business agenda.[31] The fragmentation of infrastructure governance is therefore a threat multiplier, complicating and potentially slowing emergency response.

Ken Kistler, Electrical Power Lines, photograph, PublicDomainPictures.net, https://www.publicdomainpictures.net/en/view-image.php?image=95061&picture=electrical-power-lines

Aging Infrastructure

The costs of aging and underdeveloped infrastructure are growing, especially in the context of emerging vulnerabilities posed by a changing climate. Calculating the infrastructure gap is a complex undertaking, given that Canada does not have a national infrastructure plan or agency that oversees the central evaluation and prioritization of infrastructure investment.[32] Canada is also missing a national standardized CI risk assessment or vulnerable asset data repository across government levels.[33] Given this deficit in infrastructure gap assessment across the country, it is difficult to gain a holistic understanding of current CI conditions, levels of disparity across the country, or asset criticality to resilience, thus impeding resource prioritization. Some numbers include CAD 250 billion in replacement cost of road transportation infrastructure and CAD 107 billion of water/wastewater/stormwater assets currently in poor/very poor conditions (CAD 109 billion whose condition is unknown).[34] [35] Moreover, the First Nations essential infrastructure (housing, clean water, healthcare, roads) gap was estimated at CAD 376.1 billion over a ten year span in 2023.[36] When it comes to military real portfolio infrastructure, over a quarter of it is over 50 years old, with a growing need for maintenance and replacement.[37] As of a 2024 Audit of Defence Infrastructure, there was also an absence of a formal risk management process and accurate up-to-date data, which has resulted in resource allocation based on historical funding levels rather than data-based need.[38] As of November 2025, the Audit of Defence Infrastructure management action plan is at a 0% implementation status.[39] The 2026-27 Departmental Plan set a target to raise the share of defence infrastructure in fair or better condition from 54.67 in 2024-25 to 70% by March 2027.[40]

Procurement Vulnerabilities and Supply Chain Disruptions

CI resilience depends on resilient procurement processes and supply chains. The COVID-19 pandemic highlighted a major infrastructure resilience vulnerability with global disruptions of supply chains for essential goods.[41] One of the major realizations was Canada's single-source dependency on pharmaceuticals, undermining public health. Single-source dependable, along with increasingly prevalent global disruptions like natural disasters, geopolitical tensions, cyber threats, economic uncertainty, and changing regulations, can undermine the availability of resources to support and develop resilience.[42] Supply-chain resilience also includes considering who owns and controls strategic infrastructure. Through the Belt and Road Initiative (BRI), Chinese state-owned firms have acquired stakes in European ports and related facilities, including Piraeus Port (an important transshipment hub in the Mediterranean and Greece's largest naval base and a hub for NATO and U.S. Sixth Fleet operations).[43] The BRI illustrates the importance of NATO's and Canada's supply-chain resilience as foreign state-owned infrastructure could become a tool of state influence via manipulation of trade, surveillance, and intelligence collection.

"The BRI illustrates the importance of NATO's and Canada's supply-chain resilience as foreign state-owned infrastructure could become a tool of state influence through trade manipulation, surveillance, and intelligence collection."

Procurement Vulnerabilities and Supply Chain Disruptions

CI resilience depends on resilient procurement processes and supply chains. The COVID-19 pandemic highlighted a major infrastructure resilience vulnerability with global disruptions of supply chains for essential goods.[41] One of the major realizations was Canada's single-source dependency on pharmaceuticals, undermining public health. Single-source dependable, along with increasingly prevalent global disruptions like natural disasters, geopolitical tensions, cyber threats, economic uncertainty, and changing regulations, can undermine the availability of resources to support and develop resilience.[42] Supply-chain resilience also includes considering who owns and controls strategic infrastructure. Through the Belt and Road Initiative (BRI), Chinese state-owned firms have acquired stakes in European ports and related facilities, including Piraeus Port (an important transshipment hub in the Mediterranean and Greece's largest naval base and a hub for NATO and U.S. Sixth Fleet operations).[43] The BRI illustrates the importance of NATO's and Canada's supply-chain resilience as foreign state-owned infrastructure could become a tool of state influence via manipulation of trade, surveillance, and intelligence collection.

Existing Critical Infrastructure Policy Evaluation

Canada's 2009 National Strategy for Critical Infrastructure created the basic architecture for CI resilience through partnerships, sector networks, information-sharing, and all-hazards risk management. However, the framework was largely built around predominantly voluntary cooperation rather than clear responsibility, a regulatory framework, or systematic assessment of which infrastructure is vital to Canada's security, emergency response, and defence readiness. Canada's CI strategy has not kept pace with the development of interconnected infrastructure and a changing threat environment, leaving governance, infrastructure assessment, and accountability fragmentation unresolved.

National Strategy for Critical Infrastructure - 2009

Canada's National Strategy for Critical Infrastructure is a federal-provincial-territorial framework for CI resilience. The strategy has three objectives: (1) Build partnerships among federal, provincial, territorial, municipal, and private-sector actors; (2) Apply all-hazards risk management through risk assessments, business continuity, emergency planning, and exercises; (3) Share and protect information so governments and operators can develop a common operating picture before, during, and after disruptions. CI owners and operators have the primary responsibility for protecting their own assets; municipalities and provinces/territories lead initial emergency response, with the federal government providing national leadership and assistance upon request. The strategy proposes sector-specific networks and a National Cross-Sector Forum to address interdependencies. [44]

The national strategy has been criticized for its lack of clear identification of actors responsible for leading on CI resilience and accountability for the results of initiatives. There has also been no systematic mapping of CI fundamental for maintaining Canada's national security and sustaining the operations of national defence and emergency response operations. The strategy also lacks tangible outcomes, such as national standards, enforcement measures, or strategic priorities. [45]

Action Plans

Public Safety Canada issued four critical infrastructure action plans (2010-2013,[46] 2014-2017,[47] 2018-2020,[48] and 2021-2023[49]) alongside a Canada-U.S. plan[50] in 2010. The plans established Sector Networks, a National Cross-Sector Forum (NCSF), and revitalization of the Federal-Provincial-Territorial Critical Infrastructure Working Group with voluntary participation to connect governments with CI owners and operators. Later plans expanded information sharing, risk analysis, cybersecurity guidance, training, and exercises. These initiatives were intended to improve situational awareness, strengthen public-private collaboration, and help operators prepare for emerging risks. The 2021–2023 plan also noted a Canadian Critical Infrastructure Asset List and a risk-based approach to identifying significant assets.[51] Key initiatives included: sectoral and cross-sectoral meetings, Critical Infrastructure Information Gateway (CI Gateway), Canadian Cyber Threat Exchange, Industrial Control System (ICS) Cyber Security training, Virtual Risk Analysis Cell (VRAC), tools such as the Fundamentals of Cyber Security for Canada's Critical Infrastructure Community, Lead Federal Department Critical Infrastructure Network (LFD), participation with international partners such as the Critical Five and OECD, Industrial Control System Security Symposiums, exercises simulating responses to hazard attacks such as the Nexus Vitalis 2019, unclassified panel discussions on emerging threats, guides on enhancing CI resilience to insider risk, and the like.

The Regional Resilience Assessment Program

Launched in 2012 under the Canada–U.S. Beyond the Border Action Plan, RRAP provided free, confidential, voluntary, and non-regulatory all-hazards assessments to help critical-infrastructure owners and operators identify physical, cyber, and interdependency vulnerabilities.[52] Aggregate assessment data also informed sector profiles and annual Critical Infrastructure Resilience Scores.[53] The 2016-2017 RRAP evaluation found that demand and workloads exceeded initial resources and planned budgets.[54] A 2023-24 assessment found that 87% of surveyed participants reported taking resilience action after assessments in 2023–24, while 98% reported improved risk awareness.[55] Public Safety ceased RRAP delivery in fiscal year 2024–25 and no longer maintains the CI Resilience Score.[56] The department has not publicly explained the decision, leaving no visible successor to Canada's principal structured CI assessment program.

RRAP illustrates both the limits of Canada's current policies and the value of systematic CI assessment. The program provided the foundation for creating an understanding of national CI vulnerabilities, CI resilience scores, and standardized sector profiles through site assessment aggregate data. It was in demand by CI owners and operators, many of whom invested in CI resilience following the assessments. However, the program remained voluntary and was constrained by limited funding and the uneven geographic availability of assessment professionals, resulting in inconsistent site coverage across Canada before its eventual closure.

National Critical Infrastructure Strategy Renewal

The national strategy was reviewed under the 2018–20 Action Plan,[57] while the 2021–23 Action Plan provided an update on the review process and recommended a broader renewal of the strategy, including the renewal of fundamental definitions and concepts, roles and responsibilities, legislative authorities and regulations, and overall program delivery.[58] As of 2026, neither a renewed national strategy nor a 2024-2027 action plan has been released.

Renewal Consultation and Unresolved Gaps

A review initiated under the 2018–20 Action Plan led Public Safety Canada to recommend a broader renewal process (as reported in the 2021–23 Action Plan).[59] Public Safety Canada subsequently consulted critical-infrastructure stakeholders through meetings, written submissions, and an online consultation process, publishing Renewing Canada's Approach to Critical Infrastructure Resilience: What We Heard Report in 2022.[60] Stakeholders identified a multitude of gaps in each of the Strategy's three objectives, which can be summarized under five gaps:[61]

1. **Definitions:** update CI definition to reflect growing interdependency of CIs and vulnerability of global supply chains; enlargement of the CI list to include the Space and Defence sectors to address the evolving threat environment.
2. **Objective 1 - Partnership Building:** expand partnerships to include municipalities and Indigenous communities; strengthen cross-sector partnerships; expand public-private dialogue avenues.
3. **Objective 2 - All-Hazard Risk-Management Pillar:** increase governance coherence and coordination across jurisdictions; develop a methodology for identifying vital CI; establish data registries to identify threats.
4. **Objective 3 - Information Sharing:** expand risk information sharing to the public and broader infrastructure community; two-way threat information sharing between stakeholders and government; create a centralized coordination National CI Centre.
5. **Implement a new objective - Critical Infrastructure Protection:** identify concrete oversight and support entities required to meet specific obligations; establish regulations for benchmarked standard of service in the CI system; formal designation and regulation of interdependent systems; creation of a national regulatory framework for CI with effective incentives and penalties; government support and guidance on the process.

Gogerr. Wildfire Smoke in St. Catharines, Ontario (4). Photograph, July 15, 2026. Wikimedia Commons. https://commons.wikimedia.org/wiki/File:Wildfire_smoke_in_St._Catharines,_Ontario_(4).jpg.

CI Adjacent Policy

The national strategy was reviewed under the 2018–20 Action Plan,[57] while the 2021–23 Action Plan provided an update on the review process and recommended a broader renewal of the strategy, including the renewal of fundamental definitions and concepts, roles and responsibilities, legislative authorities and regulations, and overall program delivery.[58] As of 2026, neither a renewed national strategy nor a 2024-2027 action plan has been released.

While Canada's National Strategy for Critical Infrastructure remains the central federal framework for critical-infrastructure resilience, more recent emergency preparedness, defence, cyber, and industrial policies increasingly recognize that infrastructure resilience is also a matter of national security, military readiness, procurement capacity, and economic sovereignty. Our North, Strong and Free (2024),[62] Canada's National Cyber Security Strategy (2025),[63] and Canada's Defence Industrial Strategy (2026)[64] each address a different component of the infrastructure challenge: the physical infrastructure and logistical systems required for CAF operations; the cyber security of increasingly interconnected critical systems; and the industrial, procurement, and supply-chain capacity required for defence capacity. Public Safety Canada's National Risk Profile adds a national assessment of disaster risks and emergency-management capabilities, but does not replace assessments of individual critical infrastructure assets.[65] Public Safety Canada is also working to renew the Emergency Management Strategy[66] and the Federal Emergency Response Plan,[67] which guide emergency management cooperation and federal response. Recent investments expand civilian response capacity through the renewed Humanitarian Workforce Program and national aerial wildfire firefighting capacity.[68] Described in greater detail in Chapter 3 on Cyber Resilience and Digital Sovereignty, the 2026 Bill C-8, which amended the Telecommunications Act and enacted the Critical Cyber Systems Protection Act, once in force will place mandatory cyber-security obligations on designated operators in federally regulated sectors.[69] Other sectors have mixed regulations of their own, such as the strict regulation of the nuclear sector.[70]

> **"Canada acknowledges the relationship between critical infrastructure, emergency preparedness, national defence and security. However, policies remain divided across separate policy silos.**

The Emerging Role of Research Institutions in CI Resilience

The National Centre for Critical Infrastructure Protection, Security, and Resilience (NC-CIPSeR) as a not-for-profit based in Carleton University aiming to close the gap between government, industry, and academia on issues relating to CI resilience.[71] Currently, NC-

CIPSeR is developing a series of connected research initiatives intended to improve coherence without attempting to replace existing authorities. Its emerging CAnexus framework examines fragmentation across governance, tools and standards, research, data, and education and training. Through Project CANVAS, Integrated Profiles and Analysis, comparative work on threat and risk assessment methodologies, and applied projects involving CI prioritization, civil readiness and interdependencies, the Centre is exploring how distributed organizations can produce more consistent, comparable and decision-relevant analysis.[72] The Critical Infrastructure Mapping and Analysis System (CIMAS) supports this work as an open-source geospatial and economic-modelling platform for examining infrastructure, industry, supply-chain and regional dependencies under different threat and hazard scenarios.[73]

Summary

Overall, Canada's CI National Strategy and subsequent action plans established a broad collaborative framework for partnership building, information sharing, and all-hazards risk management between private-public and cross-sector stakeholders with a variety of tools and initiatives. The policy framework did build a foundation for governments and infrastructure owners-operators to exchange information, discuss cross-sector risks, and improve preparedness. However, the established networks and programs were built on a predominantly voluntary, engagement-based mechanism of meetings, forums, assessments, situational awareness briefs, exercises, training, and guides encouraging CI sectors to facilitate action. The policy did not establish clear national priorities, responsibility and accountability mechanisms, consistent methods for identifying vital CI, or tracking resilience progress. More recent CI-adjacent policies indicate growing recognition that infrastructure resilience is essential to national defence and security, but do not establish an integrated national methodology for identifying vital civilian and military infrastructure. The majority of outlined gaps were already evaluated during the stakeholder consultations conducted in 2022, as well as a recognition that the strategy needs renewal. As of 2026, the absence of a renewed Strategy or successor Action Plan leaves those gaps unresolved.

NATO Ally & Partner Country Case Studies

NATO member and partner countries have been actively re-evaluating their domestic CI resilience to support national resilience against emerging threats. The EU, Estonia, Australia, and Finland offer valuable lessons for Canada's current gaps, including a civil-military approach to CI disruption preparedness, strong regulatory frameworks, procurement resilience, climate adaptation, and civil preparedness.

European Union: How the EU Holds Critical Entities Accountable

The European Union established the Critical Entities Resilience Directive (CER Directive) in 2022 to ensure that organizations providing services essential to daily societal

functioning and the economy can prevent, withstand, respond to, and recover from disruption. Under the directive, each EU member state must develop a national resilience strategy, conduct all-hazards risk assessments, and identify the companies or public bodies whose failure would significantly disrupt essential services. Once identified (by July 2026), the critical entities must assess their own vulnerabilities and adopt proportionate resilience measures (within 9 months). Member states are to establish penalties for directive infringements which must be "effective, proportionate and dissuasive."[74]

Estonia: Decentralized Governance & Unified Legal Framework

Estonia's approach to security, national defence and resilience has been based on Finland's and Sweden's models of total defence, with the 2010 version of the National Security Concept of Estonia introducing the concepts of "societal continuation and cohesion.[75]" The National Security Concept includes five national-defence lines of action with the State Defence Action Plan, based on principles of a comprehensive approach to national defence, translating the five pillars into 67 national-defence tasks for ministries, agencies, municipalities, and essential service providers.[76]

Aaron Einstein, Iqaluit Skyline, photograph, March 24, 2010, Wikimedia Commons, https://commons.wikimedia.org/wiki/File:Iqaluit_skyline.jpg Aaron Einstein, Iqaluit Skyline, photograph,

These tasks link domestic security efforts with NATO's collective defence, explicitly incorporating NATO's seven baseline resilience requirements. Crisis preparedness is decentralized, with each ministry, government agency, and local government responsible for preventing and managing crises within their own domain while coordinated by the central Government Office. Each institution must identify potential risks, conduct risk analyses, and develop response plans accordingly. The National Risk Assessments are conducted across military, hybrid, and civil threats for relevant stakeholders to have a unified picture of the threat environment to support resilience planning. Entering into force in October of 2026, the Crisis Situation and National Defence Act will consolidate Estonia's Emergency Act, State of Emergency Act, and National Defence Act into a single legal framework for preparing for, managing, and coordinating civilian and national-defence crises.[77]

Like Canada, Estonia distributes responsibility for critical-infrastructure resilience across government bodies and essential-service providers. However, it possesses centralized risk assessment, planning standards, and a legal framework, connecting the importance of civilian infrastructure continuity to domestic and NATO's baseline resilience requirements.

Australia: Procurement Resilience

Australia, one of NATO's Indo-Pacific partner countries, regulates procurement risk at the level of CI operators. Under the Security of Critical Infrastructure Act 2018[78] and its Critical Infrastructure Risk Management Program (CIRMP)[79], responsible entities for covered asset classes must maintain and comply with a written risk-management program. The program must address material cyber, personnel, supply-chain, physical-security and natural hazards. For supply chains, entities must, as far as reasonably practicable, minimize risks such as unauthorized access, misuse of supplier access, disruption, and reduced capacity elsewhere in the supply chain, and mitigate their effects. Additional requirements introduced in 2026 require operators of specified assets to map major suppliers and critical components, assess supplier access and foreign-influence risks, and identify acceptable outage periods. Entities submit annual reports approved by their boards or governing bodies.[80]

A Canadian framework could similarly require designated operators to map essential suppliers and components, assess foreign-influence and single-source risks, identify alternatives, and build continuity and access controls into supplier contracts.

Finland: Total Defence and Civil Engagement

Finland's famous total defence comprehensive-security model considers citizens as active contributors to national resilience alongside government, businesses, and civil-society organizations. The 2025 Security Strategy for Society identifies individuals as key actors in safeguarding essential societal functions during disruptions, crises, and emergency conditions. Canada's National Strategy for Critical Infrastructure assigns responsibility to individual Canadians "to be prepared for a disruption and to ensure that they and their families are ready to cope for at least the first 72 hours of an emergency". [81] However, it does not outline practical paths or programs for the Canadian public to engage with. Finland's Preparing for Incidents and Crises guide[82] and 72 Hours program[83] recommends that every household be able to cope independently for at least three days during disruptions. While the program is voluntary, it is supported through a national network with trained instructors delivering presentations and webinars to housing associations, workplaces, and community groups.[84] Finland's model illustrates how Canada can engage with the public through civil-preparedness education and engagement to support national resilience in a time of disruption.

Policy Recommendations

Develop an updated National Strategy for Critical Infrastructure aligned with whole-of-society national resilience

Canada should renew the 2009 National Strategy for Critical Infrastructure to reflect the current threat environment, as well as the evolution and increasing interdependence of Canada's ten critical-infrastructure sectors. The strategy should include a clearer governance and regulatory structure that better defines roles, responsibilities, and accountability across federal, provincial, territorial, municipal, and private-sector actors. The renewed Strategy should explicitly position and reflect CI resilience as a foundation for domestic emergency preparedness, national security and defence, including Canada's capacity to fulfil its commitments under NATO's seven baseline requirements for national resilience . A cross-government task force should be established to map the strategies, initiatives, risk-assessment tools, governance bodies, and information-sharing tools operating across critical infrastructure, emergency preparedness, and national defence. The task force should identify gaps, crossovers, and best practices to develop a mechanism for increased cross-jurisdictional awareness and strategy alignment for a whole-of-society approach to resilience in time of disruptions.

Create a mandatory National Critical Infrastructure Resilience Assessment Program

Canada should establish a mandatory resilience assessment program for specific CI owners and operators whose disruption would significantly affect essential services, national security, emergency preparedness, or CAF readiness. The program should include assessment of physical, cyber, climate, supply-chain, and interdependency risks. Designated operators should be required to complete periodic assessments, submit resilience-improvement plans, and report progress on high-risk vulnerabilities. The aggregate data and sector profiles could serve as national CI resilience awareness tools.

Establish mandatory resilience standards for nationally significant critical infrastructure

Canada should introduce tiered resilience obligations for designated critical infrastructure entities whose disruption would significantly affect essential services, national security, emergency preparedness, or CAF readiness. These standards should require operators to maintain business-continuity plans, cyber security protections, physical security measures, climate-risk adaptation plans, incident reporting, and regular exercises. Requirements should be proportionate to criticality.

Embed resilience into infrastructure procurement

Canada should embed resilience levers into public procurement and federally regulated

or funded CI projects. Procurement criteria should require climate and cyber risk modelling, lifecycle maintenance planning, supplier mapping, as well as assessment of foreign ownership, vendor access, and single-source dependency.

Build a whole-of-society preparedness and critical infrastructure disruption exercise program

Canada should develop a national civil-preparedness program to support the Canadian public in reaching a level of preparedness to sustain themselves for 72-hours in time of a disruption. The program can include practical guides, community and neighbourhood-level training, and regular cross-sector exercises for CI operators.

Conclusion

Canada's approach to critical-infrastructure resilience has not kept pace with the scale, complexity, and interconnectedness of the current threat environment. The 2009 National Strategy and its subsequent action plans created a valuable foundation for partnership building, information sharing, and all-hazards risk management. However, the threat environment is rapidly evolving with climate-change-fueled environmental disasters, cyber disruptions, aging infrastructure, and global supply-chain disruptions. Canada therefore needs to move beyond a voluntary and engagement-based model toward a more systematic framework with clearer governance, mandatory assessments for designated CI operators, enforceable resilience standards, resilience-minded procurement criteria, and public preparedness programs. As modern threats blur the boundary between domestic emergencies and national-security threats, Canada should treat CI protection and resilience as a foundation for sustaining societal continuity, military capacity, and meeting Canada's national and NATO resilience commitments.

Canadian Armed Forces, [photograph of civilians boarding a military aircraft], Facebook photograph, July 27, 2021, https://www.facebook.com/CanadianForces/photos/3260340504193129/

Donnie McDonald, LX02-2019-0025-088, photograph, April 29, 2019, Canadian Forces Imagery Gallery, https://www.combatcamera.forces.gc.ca/gallery/cc_photos/detail/?assetId=126564&filename=LX02-2019-0025-088

Endnotes:

1. "NATO Secretary General at the Rotterdam City Hall Event—Resilience Is Everyone's Responsibility," NATO, May 26, 2026,
2. "Updated Ukraine Recovery and Reconstruction Needs Assessment Released," World Bank, February 23, 2026, https://www.worldbank.org/en/news/press-release/2026/02/23/updated-ukraine-recovery-and-reconstruction-needs-assessment-released.
3. Hanna Duggal and Marium Ali, "In Maps and Charts: Russian and Ukrainian Attacks on Civilian Targets," Al Jazeera, September 9, 2026, https://www.aljazeera.com/news/2026/9/9/in-maps-and-charts-russian-and-ukrainian-attacks-on-civilian-targets.
4. Canadian Centre for Cyber Security, National Cyber Threat Assessment.
5. Communications Security Establishment Canada, Communications Security Establishment Canada Annual Report 2025–2026 (Government of Canada, 2026), https://www.cse-cst.gc.ca/en/accountability/transparency/reports/communications-security-establishment-canada-annual-report-2025-2026
6. Department of National Defence, Our North, Strong and Free: A Renewed Vision for Canada's Defence (Government of Canada, 2024), https://www.canada.ca/en/department-national-defence/corporate/reports-publications/north-strong-free-2024.html.
7. "Canada's Critical Infrastructure (CI)," Public Safety Canada, last modified August 12, 2026, https://www.publicsafety.gc.ca/cnt/ntnl-scrt/crtcl-nfrstrctr/cci-iec-en.aspx
8. Federal, Provincial, and Territorial Ministers Responsible for Emergency Management, An Emergency Management Framework for Canada, 3rd ed. (Public Safety Canada, 2017), https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2017-mrgnc-mngmnt-frmwrk/index-en.aspx
9. "Canada's Critical Infrastructure (CI)," Public Safety Canada, last modified August 12, 2026, https://www.publicsafety.gc.ca/cnt/ntnl-scrt/crtcl-nfrstrctr/cci-iec-en.aspx
10. "NATO Resilience, Civil Preparedness and Article 3," NATO, updated November 13, 2024, https://www.nato.int/en/what-we-do/deterrence-and-defence/resilience-civil-preparedness-and-article-3
11. Carol V. Evans et al., Enabling NATO's Collective Defense: Critical Infrastructure Security and Resiliency, NATO COE-DAT Handbook 1 (Centre of Excellence–Defence Against Terrorism and Strategic Studies Institute, U.S. Army War College Press, 2022), https://press.armywarcollege.edu/monographs/955/
12. "Infrastructure in the North," National Defence, last modified August 22, 2023, https://www.canada.ca/en/department-national-defence/corporate/reports-publications/proactive-disclosure/secd-april-24-2023/infrastructure-north.html
13. "Operation LENTUS," National Defence, last modified July 30, 2026, https://www.canada.ca/en/department-national-defence/services/operations/military-operations/current-operations/operation-lentus.html
14. "The Hague Summit Declaration," NATO, June 25, 2025, https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2025/06/25/the-hague-summit-declaration.

Endnotes:

15. Ryan Dean and P. Whitney Lackenbauer, Military Spending, NATO's Seven Baseline Requirements, and Infrastructure (North American and Arctic Defence and Security Network, November 3, 2025), https://www.naadsn.ca/wp-content/uploads/2025/11/25nov3-NAADSN-7BLR-Policy-Primer-RD-PWL.pdf
16. Office of Critical Infrastructure Protection and Emergency Preparedness, Threats to Canada's Critical Infrastructure (Government of Canada, March 12, 2003), https://publications.gc.ca/site/fra/9.842491/publication.html
17. Policy Horizons Canada, Disruptions on the Horizon.
18. James Michelin, "Weather Tracker: More than 900 Wildfires Rage across Canada," The Guardian, July 24, 2026, https://www.theguardian.com/environment/2026/jul/24/weather-tracker-wildfires-canada-argentina-heat
19. "Wildfires: Federal Response," Public Safety Canada, last modified July 27, 2026, https://www.canada.ca/en/public-safety-canada/campaigns/wildfires.html
20. "Statement from the Canadian Armed Forces on the Evacuation of Eabametoong First Nation (Fort Hope), Ontario, due to Wildfire," National Defence, July 18, 2026, https://www.canada.ca/en/department-national-defence/news/2026/07/statement-from-the-canadian-armed-forces-on-the-evacuation-of-eabametoong-first-nation-fort-hope-ontario-due-to-wildfire.html
21. Daniel J. Rowe and Robin Della Corte, "Nearly 200 Wildfires Burn across Northwestern Quebec as Province Awaits Help from U.S. and France," CTV News, July 20, 2026, https://www.ctvnews.ca/montreal/article/nearly-200-wildfires-burn-across-northwestern-quebec-as-province-awaits-help-from-us-and-france/.
22. Rob Gillies and Jamie Stengle, "Canada Puts the Military on Standby as British Columbia Wildfires Kill 1 and Displace Thousands," Associated Press, August 10, 2026, https://apnews.com/article/canada-wildfires-british-columbia-de5556e3d5323dd85ee7ed87a378cf8f
23. Darren Swanson et al., Advancing the Climate Resilience of Canadian Infrastructure: A Review of Literature to Inform the Way Forward (International Institute for Sustainable Development, July 2021), https://www.iisd.org/publications/climate-resilience-canadian-infrastructure.
24. "National Risk Profile: Strengthening Canada's All-Hazards Approach to Emergency Management," Public Safety Canada, last modified August 7, 2025, https://www.publicsafety.gc.ca/cnt/mrgnc-mngmnt/ntnl-rsk-prfl/index-en.aspx
25. Policy Horizons Canada, Disruptions on the Horizon.
26. Public Safety Canada, Canada's National Cyber Security Strategy: Securing Canada's Digital Future (Government of Canada, 2025), https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg-2025/index-en.aspx.
27. "Backgrounder: Malicious Cyber Activity Targeting Canadian Critical Infrastructure," Communications Security Establishment Canada, November 26, 2025, https://www.canada.ca/en/communications-security/news/2025/11/backgrounder-malicious-cyber-activity-targeting-canadian-critical-infrastructure.html

Endnotes:

28. "Security Considerations for Critical Infrastructure (ITSAP.10.100)," Canadian Centre for Cyber Security, last modified July 28, 2025, https://www.cyber.gc.ca/en/guidance/security-considerations-critical-infrastructure-itsap10100
29. Canadian Centre for Cyber Security, "Security Considerations for Critical Infrastructure."
30. Christopher Nardi, "Russian Group Hacked Quebec Water Treatment Plant, Gained Access to Control Pumps and Chlorine Dosing: CSE," National Post, June 30, 2026, https://nationalpost.com/news/politics/russian-group-hacked-quebec-water-treatment-plant-gained-access-to-control-pumps-and-chlorine-dosing-cse
31. Andrew Graham, Canada's Critical Infrastructure: When Is Safe Enough Safe Enough? (Macdonald-Laurier Institute, December 2011), https://www.macdonaldlaurier.ca/files/pdf/Canadas-Critical-Infrastructure-When-is-safe-enough-safe-enough-December-2011.pdf.
32. Kathryn Exon Smith et al., Making Up for Lost Time: Strategic Infrastructure Development for Growth and Resilience (School of Cities, University of Toronto, 2025), https://utoronto.scholaris.ca/items/35157569-667f-48f3-b917-88ef16b37d99
33. Perry Steckly, "Unraveling the Complexity: How Canada Can Build a Clearer, Stronger Approach to Critical Infrastructure Risk Assessment," National Centre for Critical Infrastructure Protection, Security and Resilience, March 4, 2025, https://carleton.ca/cipser/2025/standardized-risk-assessment-for-critical-infrastructure-in-canada/
34. Statistics Canada, "Canada's Core Public Infrastructure Survey: Replacement Values, 2022," The Daily, October 21, 2024, https://www150.statcan.gc.ca/n1/daily-quotidien/241021/dq241021b-eng.htm
35. Canadian Infrastructure Council, State of Clean Water and Sanitation Systems in Canada (technical paper, 2025), https://canadianinfrastructurecouncil.ca/state-of-clean-water-and-wastewater-systems
36. "Closing the Infrastructure Gap," Assembly of First Nations, https://afn.ca/economy-infrastructure/infrastructure/closing-the-infrastructure-gap/
37. Department of National Defence, Defence Real Property Portfolio Strategy (Government of Canada, 2022), https://www.canada.ca/en/department-national-defence/corporate/reports-publications/real-property-portfolio-strategy.html.
38. Department of National Defence, Audit of Defence Infrastructure (Government of Canada, June 2024), https://www.canada.ca/en/department-national-defence/corporate/reports-publications/audit-evaluation/audit-defence-infrastructure.html
39. "Key Compliance Attributes of Internal Audit: August 2025," National Defence, last modified October 3, 2025, https://www.canada.ca/en/department-national-defence/corporate/reports-publications/audit-evaluation/key-compliance-attributes-internal-audit-2024.html

Endnotes:

40. Department of National Defence, Department of National Defence and the Canadian Armed Forces 2026–27 Departmental Plan (Government of Canada, 2026), https://www.canada.ca/en/department-national-defence/corporate/reports-publications/departmental-plans/departmental-plan-2026-27.html
41. Public Safety Canada, National Cross Sector Forum 2021–2023 Action Plan for Critical Infrastructure (Government of Canada, 2021), https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2021-ctn-pln-crtcl-nfrstrctr/index-en.aspx
42. Organisation for Economic Co-operation and Development, OECD Supply Chain Resilience Review: Navigating Risks (OECD Publishing, 2025), https://doi.org/10.1787/94e3a8ea-en
43. Evans et al., Enabling NATO's Collective Defense
44. Organisation for Economic Co-operation and Development, OECD Supply Chain Resilience Review: Navigating Risks (OECD Publishing, 2025), https://doi.org/10.1787/94e3a8ea-en
45. Jason Clemens and Brian Lee Crowley, eds., Solutions to Critical Infrastructure Problems: Essays on Protecting Canada's Infrastructure (Macdonald-Laurier Institute, February 2012), https://macdonaldlaurier.ca/mli-files/pdf/Solutions-to-Critical-infrastructure-Problems-February-2012.pdf.
46. Public Safety Canada, Action Plan for Critical Infrastructure (Government of Canada, 2009), https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/archive-pln-crtcl-nfrstrctr/index-en.aspx.
47. Public Safety Canada, Action Plan for Critical Infrastructure, 2014–2017 (Government of Canada, 2014), https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/archive-pln-crtcl-nfrstrctr-2014-17/index-en.aspx.
48. Public Safety Canada, National Cross Sector Forum 2018–2020 Action Plan for Critical Infrastructure (Government of Canada, 2018), https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/archive-pln-crtcl-nfrstrctr-2018-20/index-en.aspx.
49. Public Safety Canada, National Cross Sector Forum 2021–2023 Action Plan for Critical Infrastructure (Government of Canada, 2021), https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2021-ctn-pln-crtcl-nfrstrctr/index-en.aspx.
50. Public Safety Canada and U.S. Department of Homeland Security, Canada–United States Action Plan for Critical Infrastructure (2010), https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cnd-ntdstts-ctnpln/index-en.aspx.
51. Public Safety Canada, 2021–2023 Action Plan for Critical Infrastructure.
52. Public Safety Canada, "Regional Resilience Assessment Program (RRAP): Technical Guide," https://www.publicsafety.gc.ca/cnt/ntnl-scrt/crtcl-nfrstrctr/crtcl-nfrstrtr-rrap-faq-en.aspx.

Endnotes:

53. Public Safety Canada, Departmental Results Report 2019–20 (Government of Canada, 2020), https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/dprtmntl-rslts-rprt-2019-20/index-en.aspx.
54. Public Safety Canada, 2016–2017 Evaluation of the Regional Resilience Assessment Program and the Virtual Risk Analysis Cell (Government of Canada, February 22, 2018), https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2016-vltn-rrap/index-en.aspx.
55. Public Safety Canada, "Horizontal Initiatives," in Departmental Results Report 2023–24 (Government of Canada, 2024), https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/dprtmntl-rslts-rprt-2023-24/hrz-hzl-en.aspx.
56. Public Safety Canada, Public Safety Canada's 2026 to 2027 Departmental Plan (Government of Canada, 2026), https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/dprtmntl-pln-2026-27/index-en.aspx.
57. Public Safety Canada, 2018–2020 Action Plan for Critical Infrastructure.
58. Public Safety Canada, 2021–2023 Action Plan for Critical Infrastructure.
59. Public Safety Canada, 2018–2020 Action Plan for Critical Infrastructure.
60. Public Safety Canada, Renewing Canada's Approach to Critical Infrastructure Resilience: What We Heard Report (Government of Canada, 2022), https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/rnwng-cnd-pprch-crtcl-nfrstrctr-rslnc-2022/index-en.aspx.
61. Public Safety Canada, Renewing Canada's Approach.
62. Our North, Strong and Free: Department of National Defence, Our North, Strong and Free.
63. Public Safety Canada, "Canada's National Cyber Security Strategy."
64. Department of National Defence, Canada's Defence Industrial Strategy (Government of Canada, February 26, 2026), https://www.canada.ca/en/department-national-defence/corporate/reports-publications/industrial-strategy/security-sovereignty-prosperity.html.
65. Public Safety Canada, "National Risk Profile: Strengthening Canada's All-Hazards Approach to Emergency Management," last modified August 7, 2025, https://www.publicsafety.gc.ca/cnt/mrgnc-mngmnt/ntnl-rsk-prfl/index-en.aspx.
66. Public Safety Canada, Public Safety Canada's 2024 to 2025 Departmental Plan (Government of Canada, 2024), https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/dprtmntl-pln-2024-25/index-en.aspx.
67. Public Safety Canada, Public Safety Canada's 2026 to 2027 Departmental Plan
68. Public Safety Canada, "The Government of Canada Updates on the 2026 Wildfire Season Preparedness and Outlook," Government of Canada, May 28, 2026, https://www.canada.ca/en/public-safety-canada/news/2026/05/the-government-of-canada-updates-on-the-2026-wildfire-season-preparedness-and-outlook.html.

Endnotes:

69. An Act Respecting Cyber Security, Amending the Telecommunications Act and Making Consequential Amendments to Other Acts, S.C. 2026, c. 9, assented to June 15, 2026, https://www.parl.ca/documentviewer/en/45-1/bill/C-8/royal-assent.
70. Nuclear Safety and Control Act, S.C. 1997, c. 9, current to July 21, 2026, https://laws-lois.justice.gc.ca/eng/acts/n-28.3/.
71. National Centre for Critical Infrastructure Protection, Security and Resilience, "National Centre for Critical Infrastructure Protection, Security and Resilience," Carleton University, https://carleton.ca/cipser/.
72. National Centre for Critical Infrastructure Protection, Security and Resilience, Our Projects, Carleton University, https://carleton.ca/cipser/research-work/#canexus.
73. National Centre for Critical Infrastructure Protection, Security and Resilience, "Critical Infrastructure Mapping and Analysis Substrate (CIMAS)," Carleton University, https://carleton.ca/cipser/critical-infrastructure-mapping-and-analysis-substrate-cimas/.
74. European Union, "Official Journal of the European Union," EUR-Lex, https://eur-lex.europa.eu/TodayOJ/index.html
75. Minna Ålander et al., Strengthening Critical Infrastructure Protection: Strategic Insights and International Best Practices (e-Governance Academy, 2025), https://ega.ee/publication/strengthening-critical-infrastructure-protection/
76. Ålander et al., Strengthening Critical Infrastructure Protection.
77. Government Office of Estonia, "Riigikaitseülesanded ja planeerimine" [National Defence Tasks and Planning], last updated February 19, 2026, https://riigikantselei.ee/el-poliitika-julgeolek-ja-riigikaitse/lai-riigikaitse/riigikaitseulesanded.
78. Security of Critical Infrastructure Act 2018 (Cth), no. 29, 2018, compilation no. 9, June 4, 2026, https://www.legislation.gov.au/C2018A00029/latest/text.
79. Cyber and Infrastructure Security Centre, Guidance for the Critical Infrastructure Risk Management Program (Australian Department of Home Affairs, March 2025), https://www.cisc.gov.au/resources-subsite/Documents/guidance-for-the-critical-infrastructure-risk-management-program.pdf.
80. Cyber and Infrastructure Security Centre, Guidance for the Critical Infrastructure Risk Management Program.
81. Public Safety Canada, National Strategy for Critical Infrastructure.
82. Security Committee, Security Strategy for Society (Government of Finland, January 16, 2025), https://turvallisuuskomitea.fi/en/security-strategy-for-society/.
83. Ministry of the Interior of Finland, "Preparing for Incidents and Crises," Suomi.fi, https://www.suomi.fi/guides/preparedness.
84. 72 Hours, "72 Hours Training Is Available to Everyone," Finnish National Rescue Association, https://72tuntia.fi/en/training/.

Author: Lou Didelot, Junior Research Fellow

Chapter 2. Economic Resilience and Supply Chains

Executive Summary

Recent crises have exposed significant weaknesses in Canada's economic resilience. The COVID-19 pandemic, Russia's full-scale invasion of Ukraine, climate-related disruptions, and growing geopolitical competition have shown how quickly disruptions to supply chains, transportation networks, energy systems, and critical imports can affect the Canadian economy. For NATO members, military readiness also depends on resilient civilian infrastructure and reliable access to essential goods and services.

Canada is particularly vulnerable because of its reliance on international supply chains and its close economic relationship with the United States. This integration has brought significant economic benefits, but it has also left Canada exposed to changes in U.S. trade policy, protectionist measures, transportation disruptions, and other external shocks. Canada also remains dependent on foreign markets in strategically important sectors such as pharmaceuticals, advanced technologies, and critical mineral processing.

Finland, Germany, and the Baltic states provide useful lessons for Canada on strategic stockpiles, economic dependencies, and the integration of resilience into national defence planning.

Main Policy Recommendations

- **Develop a Canadian Economic Security Strategy** that unifies trade, national defence, infrastructure planning, and industrial policy within a single governance framework.
- **Diversify supply chains and trade partnerships** to reduce Canada's dependence on individual suppliers and markets, particularly in strategically important sectors.
- **Expand domestic strategic capacity** through government incentives, public investment, and industrial partnerships in industries critical to national resilience.
- **Build strategic reserves and strengthen emergency procurement capacity** for essential goods, including medical supplies, pharmaceuticals, emergency equipment, and fuel.
- **Integrate economic resilience into national security and defence planning** by incorporating supply chain vulnerabilities, critical infrastructure risks, and strategic economic dependencies into national security assessments.

Introduction

Recent crises, including the COVID-19 pandemic, Russia's full-scale invasion of Ukraine, increasingly frequent climate-related disasters, and growing geopolitical competition, have exposed significant weaknesses in Canada's economic resilience. Supply chain disruptions, shortages of essential goods, transportation bottlenecks, and energy market volatility have demonstrated that economic security can no longer be viewed solely as an issue of trade or commerce. Rather, the ability of states to maintain essential economic functions during crisis has become an increasingly important component of national security and collective defence.[1]

This shift is reflected in NATO's renewed emphasis on resilience under Article 3 of the North Atlantic Treaty, which recognizes that effective deterrence and defence depend not only on military capabilities but also on the ability of member states to maintain the continuity of government, protect critical infrastructure, and sustain essential civilian services during times of disruption. NATO's Seven Baseline Requirements for Resilience further emphasize the importance of resilient transportation systems, secure energy supplies, reliable communications networks, and the continuity of essential services. Together, these civilian capabilities strengthen Allied readiness by ensuring that military operations can be sustained even during periods of significant economic or geopolitical disruption.[2]

In the Canadian context, economic resilience can be understood as the ability to withstand, adapt to, and recover from external shocks while maintaining the continuity of essential services, critical infrastructure, and supply chains. As one of the world's most trade-dependent economies, Canada has benefited significantly from access to global markets and highly integrated international supply chains, particularly through its close economic relationship with the United States.[3] At the same time, this level of integration has increased Canada's exposure to external risks. Dependence on foreign suppliers for strategically important goods, aging transportation infrastructure, climate-related disruptions, and rising geopolitical tensions have all heightened the country's vulnerability to economic shocks and supply chain disruptions.[4]

Rabich, Dietmar. Vancouver (BC, Canada), Vancouver Centerm Terminal -- 2022 -- 1902. Photograph. June 12, 2022. Wikimedia Commons. CC BY-SA 4.0. [Wikimedia Commons image page] (https://commons.wikimedia.org/wiki/File:Vancouver_(BC,_Canada),_Vancouver_Centerm_Terminal_--_2022_--_1902.jpg)

Recent events have demonstrated how disruptions affecting transportation networks, energy systems, and critical imports can quickly cascade across multiple sectors of the economy. The COVID-19 pandemic exposed significant shortages of personal protective equipment (PPE), pharmaceuticals,[5] and semiconductor components, while the 2021 British Columbia floods temporarily severed key rail and highway connections that are essential to domestic and international trade.[6] Likewise, Russia's full-scale invasion of Ukraine disrupted global energy and food markets, illustrating how international conflicts can generate far-reaching economic consequences for Canada and its NATO allies.[7]

As economic resilience becomes increasingly central to NATO's approach to collective security, Canada must adopt a more coordinated and strategic approach to strengthening supply chains and reducing strategic dependencies. This chapter argues that improving Canada's economic resilience will require long-term investments in transportation infrastructure, diversified trade and supply chains, domestic strategic capacity, and stronger coordination between governments and the private sector. By strengthening these foundations, Canada will be better positioned to withstand future disruptions while making a more resilient and reliable contribution to NATO's collective security.

Why Economic Resilience Has Become a Security Issue

NATO's Resilience Framework

For much of the post-Cold War period, national security was primarily understood through the lens of military capability. Defence policy focused on armed forces, deterrence, and military readiness, while economic issues such as trade, infrastructure, and industrial production were often treated as separate policy areas. However, recent crises have shown that military strength alone is insufficient when the civilian systems supporting it are vulnerable to disruption. Supply chains, transportation networks, energy infrastructure, telecommunications, and other critical civilian systems have become essential components of national resilience, allowing governments to maintain essential services while supporting military operations during times of crisis.[8]

NATO's renewed emphasis on resilience reflects this broader understanding of security. Building on the framework outlined earlier, NATO's Seven Baseline Requirements demonstrate how civilian preparedness, including resilient transportation systems, energy supplies, communications networks, and continuity of government, supports both national security and alliance operations. Rather than treating these civilian systems as separate from defence, NATO recognizes them as essential components of military readiness and collective resilience.[9]

Several of NATO's Seven Baseline Requirements are directly linked to economic resilience. Resilient transportation systems ensure that personnel, military equipment, medical supplies, and essential goods can continue moving during emergencies despite disruptions to ports, railways, roads, or airports. Reliable energy supplies are equally

critical, as electricity and fuel are necessary to sustain transportation networks, communications systems, healthcare facilities, industrial production, and military operations. NATO also identifies secure food and water supplies as essential components of resilience, recognizing that shortages of necessities can quickly generate humanitarian challenges and social instability during prolonged crises. Finally, continuity of government and essential public services ensures that governments remain capable of making decisions, coordinating emergency responses, and maintaining public confidence during periods of significant disruption.[10]

These baseline requirements reflect the growing recognition that modern economies operate through highly interconnected systems. Critical infrastructure—including transportation, energy, telecommunications, financial services, healthcare, and digital networks—functions through complex interdependencies in which disruptions affecting one sector can quickly cascade across many others. For example, disruptions to ports or rail networks can delay the movement of food, medical supplies, industrial components, and military equipment, producing consequences that extend well beyond the transportation sector itself.[11]

Canada's economy relies heavily on international markets for both exports and imports, while domestic industries increasingly depend on supply chains that span multiple countries. As a result, economic disruptions occurring abroad can rapidly affect production, employment, consumer prices, and the availability of essential goods at home.[12] Economic resilience has therefore become an increasingly important component of national security, ensuring that states can continue to function effectively during external shocks while fulfilling their commitments to NATO's collective defence.

The Limits of Efficiency-Based Globalization

The growing importance of economic resilience reflects broader changes in the global economy over the past several decades. Since the late twentieth century, globalization has encouraged governments and businesses to prioritize efficiency, lower production costs, and deeper international economic integration. Advances in transportation, communications technology, and trade liberalization allowed firms to distribute production across multiple countries, sourcing components wherever costs were lowest while minimizing inventories through just-in-time production systems. These practices significantly reduced operating expenses and increased productivity, contributing to decades of economic growth and expanding global trade.[13]

While these highly integrated supply chains proved efficient under stable conditions, they also reduced redundancy and increased dependence on uninterrupted international trade. As companies sought to eliminate excess inventory and concentrate production in specialized locations, many supply chains became increasingly vulnerable to disruption. Essential industries frequently relied on a limited number of suppliers or manufacturing hubs, leaving governments and businesses with few alternatives when production was interrupted. The emphasis on efficiency often came at the expense of resilience, as maintaining strategic reserves, diversifying suppliers, or preserving

domestic production capacity was viewed as economically inefficient.[14]

> **"The emphasis on efficiency often came at the expense of resilience. Maintaining strategic reserves, diversifying suppliers, or preserving domestic production capacity was viewed as economically inefficient."**

The COVID-19 pandemic exposed these vulnerabilities on an unprecedented scale. Factory closures, labour shortages, border restrictions, and transportation disruptions interrupted the global movement of goods, creating shortages of products ranging from personal protective equipment and pharmaceuticals to semiconductors and industrial components. Governments that had assumed global markets would reliably supply essential goods instead found themselves competing for limited resources while facing significant delays in procurement. The pandemic demonstrated that supply chains optimized solely for efficiency were poorly equipped to withstand prolonged global disruptions.[15]

> **"The pandemic demonstrated that supply chains optimized solely for efficiency were poorly equipped to withstand prolonged global disruptions."**

Russia's full-scale invasion of Ukraine further reinforced these vulnerabilities by illustrating how geopolitical conflict can generate widespread economic consequences. The disruption of global energy markets, food exports, and transportation routes highlighted the extent to which strategic dependencies can be exploited during periods of international tension.[16] Increasing geopolitical competition, including the growing use of trade restrictions, export controls, sanctions, and investment screening, has further underscored that economic relationships are no longer governed exclusively by market considerations but are increasingly influenced by national security concerns.[17]

In response, many NATO members have begun reassessing the balance between economic efficiency and resilience. Rather than pursuing globalization solely based on cost reduction, governments have increasingly adopted policies aimed at strengthening economic security and reducing strategic vulnerabilities. Reshoring seeks to relocate critical manufacturing and production capacity back within national borders, particularly in sectors such as pharmaceuticals, semiconductors, and defence-related industries. Friend-shoring, meanwhile, encourages the relocation of supply chains to trusted allies

and like-minded partners that share common security interests and political values, thereby reducing dependence on potentially adversarial states. Alongside these initiatives, many governments have embraced broader strategies of strategic autonomy and economic security that emphasize supply chain diversification, investment screening, domestic industrial capacity, and the protection of critical infrastructure.[18]

For NATO members, these developments extend well beyond economic policy. Disruptions affecting transportation systems, energy infrastructure, communications networks, or critical imports can directly undermine civilian resilience while limiting the ability to mobilize military forces, sustain operations, and support Allies during periods of crisis. Consequently, strengthening economic resilience is no longer simply a matter of improving economic performance; it has become an essential requirement for national preparedness, collective defence, and the long-term security of the Alliance.[19] For Canada, these evolving approaches highlight the importance of balancing the economic benefits of global integration with the need to reduce strategic dependencies in sectors critical to national security.

"Strengthening economic resilience is no longer a matter of improving economic performance; it has become an essential requirement for national preparedness, collective defence, and the long-term security of the Alliance."

Canada's Supply Chain Vulnerabilities and Strategic Dependencies

Continental Integration and U.S. Trade Volatility

While trade openness drives Canadian prosperity, it creates acute exposure to external shocks beyond domestic control. Canada's integration into global markets means that logistical bottlenecks, foreign protectionism, and geopolitical conflicts rapidly convert into domestic supply shortages and economic volatility.[20]

Canada's economic relationship with the United States illustrates both the strengths and vulnerabilities of deep economic integration. Since the implementation of the Canada–United States Free Trade Agreement in 1989 and its subsequent evolution through the North American Free Trade Agreement (NAFTA) and the Canada–United States–Mexico Agreement (CUSMA), North American supply chains have become increasingly interconnected. Manufacturers routinely source components from multiple jurisdictions before final assembly, while agricultural products, energy resources, and manufactured goods cross the Canada–United States border each day. This integration

has enhanced productivity, lowered production costs, and strengthened Canada's international competitiveness by providing businesses with access to larger markets and highly specialized supply networks.[21]

However, the concentration of Canada's trade within a relatively small number of partners, particularly the United States, also creates strategic vulnerabilities. Because approximately three-quarters of Canadian merchandise exports are destined for the American market, disruptions affecting bilateral trade can have immediate economic consequences across multiple sectors.[22] Border restrictions, customs delays, transportation interruptions, or changes in United States trade policy can disrupt manufacturing schedules, increase production costs, and delay the movement of essential goods throughout Canadian supply chains.

Physical infrastructure bottlenecks, such as the 2022 Ambassador Bridge blockade, have highlighted the operational fragility of cross-border logistics.[23] Beyond physical disruptions, Canada faces acute strategic exposure from protectionist policies and unilateral trade actions originating within its primary trade partner. The expansion of "Buy American" procurement requirements illustrates how U.S. domestic procurement policy can affect Canadian firms' access to government procurement opportunities.[24] When nearly three-quarters of Canadian merchandise exports are bound for a single market, unilateral shifts in Washington translate into immediate macro-level domestic shocks. Relying on integrated North American production networks without insulating key sectors from sudden regulatory shifts, arbitrary duties, or political volatility in the United States leaves Canada's domestic supply chains inherently insecure.[25]

“When nearly three-quarters of Canadian merchandise exports are bound for a single market, unilateral shifts in Washington translate into immediate macro-level domestic shocks.”

For NATO members, resilient trade networks are not solely an economic concern but also a strategic necessity. Military readiness depends upon the reliable movement of equipment, fuel, industrial inputs, and essential civilian goods through secure transportation corridors and functioning international supply chains.[26] Consequently, strengthening Canada's trade resilience requires balancing the continued benefits of North American economic integration with policies that reduce strategic dependencies, diversify international partnerships, and enhance the country's capacity to withstand future disruptions.

Global Supply Chains and Non-North American Dependencies

Canada's exposure extends beyond its immediate border to highly concentrated global

supply chains. Key sectors required for national security and the green transition remain dependent on foreign production and processing capacity, including pharmaceuticals, semiconductors, and critical minerals. Although Canada possesses significant domestic reserves of critical minerals, global processing capacity for several critical minerals remains highly concentrated, creating vulnerabilities to supply disruptions and geopolitical pressure.[27] China's export controls on key inputs such as gallium and germanium demonstrate how disruptions outside North America can affect strategically important supply chains.[28] Building true economic resilience requires insulating Canada from continental policy shifts while actively diversifying away from concentrated global dependencies.

NATO Ally Case Studies

Finland and Economic Security of Supply

Among NATO members, Finland offers a leading framework for trade and supply chain resilience through its market-integrated Security of Supply model. Overseen by the National Emergency Supply Agency (NESA) under the Ministry of Economic Affairs, Finland treats economic continuity not merely as civic preparedness, but as an essential pillar of state sovereignty.[29] Rather than relying on state-run monopolies or nationalized industries, the Finnish model establishes formal public-private partnerships across critical economic sectors, including logistics, energy, digital infrastructure, and manufacturing. Private firms participate in continuity management through institutional coordination within Finland's security-of-supply system, which is supported by the National Emergency Supply Fund.[30]

Central to Finland's strategy is proactive material preparedness and supply chain hedging. Finland maintains extensive strategic and compulsory stockpiles across essential sectors, with reserve requirements varying by commodity. Fuel stockpiles cover about five months of normal consumption, while Finland also maintains substantial reserves of grain and pharmaceuticals.[31] For Canada, Finland demonstrates how middle powers can buffer critical industries against external trade leverage and global supply chain bottlenecks by combining strategic reserves with institutional public-private coordination.

Germany and Energy Dependence

Germany's experience before and after Russia's full-scale invasion of Ukraine illustrates the risks associated with excessive dependence on a single external supplier for strategically important resources. For many years, Germany pursued an energy strategy that relied heavily on relatively inexpensive Russian natural gas. While this approach supported industrial competitiveness, it also created significant strategic vulnerabilities that became apparent following Russia's invasion of Ukraine in 2022.[32]

As geopolitical tensions intensified, Germany's dependence on Russian energy exposed the country to significant supply risks. Russian gas deliveries declined sharply during 2022, with deliveries through Nord Stream 1 ultimately falling to zero by the beginning

of September. Germany compensated in part through increased imports from Norway, the Netherlands, Belgium, and other suppliers.[33] The speed of this adjustment illustrates the difficulties governments face when correcting strategic dependencies after they have already become deeply entrenched.

Germany's experience demonstrates that economic efficiency should not be pursued at the expense of long-term resilience. Dependence on authoritarian states for strategically important resources may provide short-term economic benefits but can generate significant security risks when political relationships deteriorate. Germany's experience has reinforced a broader recognition among NATO members that energy security is an essential component of national security rather than solely an economic policy issue.

Canada faces different circumstances given its abundant domestic energy resources and status as a major energy producer. Nevertheless, Germany's experience remains highly relevant. Strategic dependencies can emerge in sectors extending well beyond energy, including critical minerals processing, advanced technologies, pharmaceuticals, and telecommunications, all of which have become increasingly important to Canada's economic and national security. Diversifying supply chains before crises occur is, therefore, considerably less costly than attempting to rebuild resilience under emergency conditions.

Baltic States and Resilience Planning

The Baltic states, Estonia, Latvia, and Lithuania, have emerged as leaders within NATO in resilience planning due to their long-standing exposure to Russian military pressure, cyberattacks, disinformation campaigns, and economic coercion. Their experience illustrates that contemporary security threats often combine military, economic, technological, and informational elements, requiring resilience strategies that extend well beyond conventional defence planning.

Cyber security has become a particularly important component of Baltic resilience. Following major cyberattacks targeting Estonia in 2007, Estonia significantly strengthened the protection of government networks, financial institutions, critical infrastructure, and digital public services. Investments in cybersecurity, secure communications systems, and digital redundancy have reduced vulnerabilities while improving the government's ability to maintain essential services during periods of disruption.[34]

More broadly, NATO's resilience framework emphasizes the importance of civilian preparedness, critical infrastructure, transportation, energy, communications, and continuity of essential services as foundations of collective defence. For Baltic allies facing a demanding regional security environment, these civilian dimensions of resilience form an important complement to conventional military preparedness.[35]

Another important lesson is the emphasis placed on reducing vulnerability to economic coercion. By diversifying energy supplies, strengthening regional cooperation, and improving infrastructure connectivity with European partners, the Baltic states have

sought to reduce opportunities for external actors to exploit strategic economic dependencies for political leverage.[36]

Although Canada's geographic environment differs from the Baltic region, these strategic principles remain directly applicable. Rapidly evolving cyber threats, foreign interference, and critical infrastructure vulnerabilities require Ottawa to integrate supply chain continuity into national defence planning, providing a framework for the actionable recommendations that follow.

Policy Recommendations

The preceding analysis demonstrates that Canada's economic resilience is constrained by structural vulnerabilities across supply chains, critical infrastructure, transportation networks, and strategic dependencies. Addressing these challenges requires more than reactive responses to individual crises; it demands a coordinated, long-term approach that integrates economic security into broader national resilience planning. Drawing on NATO's resilience framework and lessons from Allied countries, the following recommendations outline practical steps that can strengthen Canada's preparedness for future disruptions.

Develop a Canadian Economic Security Strategy

Canada's approach to economic resilience spans multiple departments, levels of government, and policy areas, including trade, critical infrastructure, industrial strategy, emergency management, and national security.[37] To improve coordination across these policy areas, Canada should establish a comprehensive Economic Security Strategy that unifies trade, national defence, infrastructure planning, and industrial policy into a single governance framework. This strategy should establish a centralized coordinating body to map critical sector interdependencies, conduct cross-departmental vulnerability assessments, and align resilience mandates across federal, provincial, and private-sector stakeholders.

Diversify Supply Chains and Trade Partnerships

Canada's reliance on a limited number of suppliers, markets, and transportation corridors has increased its exposure to geopolitical disputes and supply chain disruptions.[38] Reducing these vulnerabilities requires greater diversification across critical supply chains. Although the United States will remain Canada's principal trading partner, expanding trade relationships with trusted democratic partners and NATO allies can strengthen the security of essential imports and reduce strategic dependence on individual suppliers. Diversification efforts should prioritize sectors involving pharmaceuticals, advanced technologies, critical minerals, and other products essential to both economic stability and national security.

Expand Domestic Strategic Capacity

The COVID-19 pandemic demonstrated that excessive dependence on foreign

can leave Canada vulnerable during periods of global disruption.[39] Building greater domestic capacity in strategically important industries would strengthen Canada's ability to respond to future emergencies while reducing reliance on external suppliers. Government incentives, public investment, and industrial partnerships should support increased domestic production of pharmaceuticals, clean energy technologies, batteries, semiconductors, emergency medical supplies, and other goods critical to national resilience. Expanding domestic production would provide greater flexibility during future crises.

Build Strategic Reserves and Emergency Procurement Capacity

The shortages experienced during the COVID-19 pandemic demonstrated that governments cannot rely exclusively on global markets during periods of crisis.[40] Canada should therefore expand strategic stockpiles of essential goods while modernizing emergency procurement systems. Strategic reserves should include medical supplies, pharmaceuticals, emergency equipment, fuel, and other goods necessary to maintain essential services. Procurement procedures should also be reviewed to improve coordination, accelerate purchasing, and reduce dependence on foreign suppliers during crises.

Integrate Resilience into National Security and Defence Planning

Economic resilience should become a permanent component of Canada's national security and defence planning rather than being treated solely as an economic policy issue. Supply chain vulnerabilities, critical infrastructure risks, and strategic economic dependencies should be incorporated into national security assessments alongside more traditional military threats.[41] Greater cooperation among civilian agencies, defence institutions, emergency management organizations, and private-sector partners would improve Canada's ability to sustain essential services and support military operations during periods of crisis. Continued alignment with NATO's resilience objectives would further strengthen Canada's contribution to collective defence while reinforcing the Alliance's broader resilience framework.

Acoteleg. Supercheminee Sudbury. Photograph. March 29, 2021. Wikimedia Commons. CC BY-SA 4.0. [Wikimedia Commons image page] (https://commons.wikimedia.org/wiki/File:Supercheminee_Sudbury.jpg)

Conclusion

Economic resilience has become inseparable from national security. Recent crises, including the COVID-19 pandemic, Russia's full-scale invasion of Ukraine, climate-related disasters, and growing geopolitical competition, have demonstrated that disruptions to supply chains, transportation systems, energy infrastructure, and critical imports can have significant consequences for both economic stability and national defence.

Canada's highly integrated economy has benefited considerably from globalization and international trade, yet these same characteristics have also created strategic vulnerabilities. Dependence on complex global supply chains, aging infrastructure, climate-related risks, and growing geopolitical uncertainty have exposed weaknesses that cannot be addressed through reactive crisis management alone. Resilience is most effective when it is built into long-term national planning rather than developed in response to individual crises.

As NATO places increasing emphasis on resilience as a cornerstone of collective security, Canada has an opportunity to strengthen both its domestic preparedness and its contribution to the Alliance.[42] Investing in resilient infrastructure, diversifying supply chains, expanding domestic strategic capacity, strengthening public-private cooperation, and integrating economic resilience into national security planning will improve Canada's ability to anticipate, withstand, and recover from future disruptions.

Economic resilience means ensuring that governments, critical infrastructure, and essential services continue to function during crises, whether from geopolitical conflict, natural disasters, cyberattacks, or other external shocks. By adopting a coordinated and forward-looking approach to economic security, Canada will be better positioned to reduce strategic vulnerabilities, reinforce NATO's collective resilience, and navigate an increasingly complex and uncertain security environment.

Endnotes:

1. North Atlantic Treaty Organization, "Resilience, Civil Preparedness and Article 3," https://www.nato.int/cps/en/natohq/topics_132722.htm.
2. North Atlantic Treaty Organization, "Resilience, Civil Preparedness and Article
3. Statistics Canada, "Canadian International Merchandise Trade, December 2025," February 19, 2026, https://www150.statcan.gc.ca/n1/daily-quotidien/260219/dq260219a-eng.htm.
4. Bank of Canada, "Linking the Chains: Supply Chain Interdependencies and the Canadian Economy," June 14, 2023, https://www.bankofcanada.ca/2023/06/linking-the-chains/.
5. Health Canada, "Health Canada's Plan to Address Health Product Shortages, 2024 to 2028," https://www.canada.ca/en/health-canada/services/drugs-health-products/drug-products/drug-shortages/plan-2024-2028.html.
6. British Columbia Ministry of Transportation and Infrastructure, "2021/22 Annual Service Plan Report" (2022), https://bcbudget.gov.bc.ca/annual_reports/2021_2022/pdf/ministry/tran.pdf.
7. International Energy Agency, "World Energy Outlook 2022: Executive Summary," 2022, https://www.iea.org/reports/world-energy-outlook-2022/executive-summary; Peter Levi and Gergely Molnar, "How the Energy Crisis Is Exacerbating the Food Crisis," International Energy Agency, June 14, 2022, https://www.iea.org/commentaries/how-the-energy-crisis-is-exacerbating-the-food-crisis.
8. North Atlantic Treaty Organization, "Resilience, Civil Preparedness and Article 3."
9. North Atlantic Treaty Organization, "Resilience, Civil Preparedness and Article 3."
10. North Atlantic Treaty Organization, "Resilience, Civil Preparedness and Article 3."
11. Bank of Canada, "Linking the Chains: Supply Chain Interdependencies and the Canadian Economy."
12. Bank of Canada, "Linking the Chains."
13. Alan McKinnon, "Building Supply Chain Resilience: A Review of Challenges and Strategies," International Transport Forum Discussion Papers, no. 2014/06 (Paris: OECD Publishing, 2014).
14. Organisation for Economic Co-operation and Development, "Global Value Chains: Efficiency and Risks in the Context of COVID-19," OECD Policy Responses to Coronavirus (COVID-19) (Paris: OECD Publishing, February 11, 2021).
15. Organisation for Economic Co-operation and Development, "Global Value Chains."
16. International Energy Agency, "World Energy Outlook 2022: Executive Summary"; Levi and Molnar, "How the Energy Crisis Is Exacerbating the Food Crisis."
17. Henry Farrell and Abraham L. Newman, "Weaponized Interdependence: How Global Economic Networks Shape State Coercion," International Security 44, no. 1 (2019): 42–79.
18. Bublu Thakur-Weigold and Sébastien Miroudot, "Promoting Resilience and Preparedness in Supply Chains," OECD Trade Policy Papers, no. 286 (Paris: OECD Publishing, 2024).
19. North Atlantic Treaty Organization, "Resilience, Civil Preparedness and Article 3."
20. Bank of Canada, "Linking the Chains."
21. Global Affairs Canada, "Canada–United States–Mexico Agreement (CUSMA)," https://www.international.gc.ca/trade-commerce/trade-agreements-accords-commerciaux/agr-acc/cusma-aceum/index.aspx.
22. Statistics Canada, "Canadian International Merchandise Trade, December 2025."

Endnotes:

23. Department of Justice Canada, "Explanation for the Declaration of a Public Order Emergency," https://www.justice.gc.ca/eng/trans/bm-mb/other-autre/emergencies-urgence/58.html.
24. Trade Commissioner Service, Global Affairs Canada, "The Buy American Act and Buy America Requirements," https://www.tradecommissioner.gc.ca/en/market-industry-info/search-country-region/country/canada-united-states-export/u-s-government-procurement/buy-america-requirements.html.
25. Henry Farrell and Abraham L. Newman, "Weaponized Interdependence: How Global Economic Networks Shape State Coercion," International Security 44, no. 1 (2019): 42–79.
26. North Atlantic Treaty Organization, "Resilience, Civil Preparedness and Article 3."
27. Global Affairs Canada, "Canada's State of Trade 2024: Supply Chains"; Natural Resources Canada, "Canadian Critical Minerals Strategy Annual Report 2024."
28. Global Affairs Canada, "Deputy Minister of Foreign Affairs Appearance before the House of Commons Special Committee on Canada-People's Republic of China Relations (CACN)," June 17, 2024, https://international.canada.ca/en/global-affairs/corporate/transparency/briefing-documents/parliamentary-committee/2024-06-17-cacn.
29. National Emergency Supply Agency, "Security of Supply," https://www.huoltovarmuuskeskus.fi/en/security-of-supply.
30. National Emergency Supply Agency, "Security of Supply."
31. National Emergency Supply Agency, "NESA's Janne Känkänen: Potential Impacts of Ukraine War on Finland's Security of Supply Are Manageable," March 4, 2022, https://www.huoltovarmuuskeskus.fi/en/a/nesas-janne-kankanen-potential-impacts-of-ukraine-war-on-finlands-security-of-supply-are-manageable-2.
32. Bundesnetzagentur, "Gas Supply Figures for 2022."
33. Bundesnetzagentur, "Gas Supply Figures for 2022." 3."
34. Christian Czosseck, Rain Ottis, and Anna-Maria Talihärm, "Estonia After the 2007 Cyber Attacks: Legal, Strategic and Organisational Changes in Cyber Security" (NATO Cooperative Cyber Defence Centre of Excellence, 2011), https://ccdcoe.org/library/publications/estonia-after-the-2007-cyber-attacks-legal-strategic-and-organisational-changes-in-cyber-security/.
35. North Atlantic Treaty Organization, "Resilience, Civil Preparedness and Article 3"
36.
37. International Energy Agency, "Accelerating Energy Diversification in Central and Eastern Europe," September 6, 2022, https://www.iea.org/commentaries/accelerating-energy-diversification-in-central-and-eastern-europe.
38. Public Safety Canada, "National Strategy for Critical Infrastructure," https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/srtg-crtcl-nfrstrctr/index-en.aspx.
39. Statistics Canada, "Canadian International Merchandise Trade, December 2025."
40. Organisation for Economic Co-operation and Development, "Global Value Chains."
41. Organisation for Economic Co-operation and Development, "Global Value Chains."
42. North Atlantic Treaty Organization, "Resilience, Civil Preparedness and Article 3."
43. North Atlantic Treaty Organization, "Resilience, Civil Preparedness and Article 3."

Authors: Esha Grewal, Program Editor
Daria Synelnykova, Publications Team Lead

Chapter 3. Cyber Resilience and Digital Sovereignty

Executive Summary

Canada's digital resilience depends on two interconnected pillars: cyber resilience and digital sovereignty. As cyberattacks become more frequent and sophisticated, Canada's critical infrastructure faces risks from fragmented governance, uneven cyber security standards, and the increasing use of hybrid tactics by hostile actors. Simultaneously, Canada's digital sovereignty is undermined by its heavy reliance on foreign cloud infrastructure and digital service providers, and a low IP retention rate. This is exacerbated by comparatively weak regulatory frameworks which leave sensitive public and private data subject to foreign jurisdictions and limits Canada's control over critical digital infrastructure. While recent legislative initiatives represent important progress, some major gaps persist, and Canada continues to lack a comprehensive whole-of-society approach to strengthening cyber resilience and digital sovereignty.

Main Policy Recommendations

- **Establish a national cyber reserve** to connect the private sector, the Canadian population, and government bodies in civil resilience-building.
- **Conduct regular national cyber exercises** to test and demonstrate domestic resilience with publicly available data, findings, and actions.
- **Introduce measurable cyber security targets for critical infrastructure** within the CCSPA that includes specific oversight requirements for government agencies.
- **Strengthen Canada's data privacy and cross-border data-transfer legislation** by requiring foreign companies operating in Canada to comply with Canadian standards.
- **Prioritize domestic cloud services** for sensitive data storage and identify strategic digital services that should remain under full Canadian control.
- **Diversify GPU procurement** by introducing interoperability standards and, where technically feasible, multi-vendor requirements for publicly funded computing infrastructure.
- **Revise existing AI policies** to address job displacement, entry-level employment, and the environmental impacts of data-centre expansion, while balancing these concerns against national security & digital sovereignty objectives.

Introduction, Cyber Resilience

With the mass digitization of government services, the concept of cyber security has become increasingly important in discussions of national resilience. The Canadian Centre for Cyber Security (Cyber Centre) defines the concept as "the protection of digital information, as well as the integrity of the infrastructure housing and transmitting digital information."[1] When it comes to resilience building, however, Canada's cyber strategy currently stands as fragmented and suggestive, rather than an all-encompassing resilience framework. This is due to a lack of standardization across different sectors and jurisdictions, exacerbated by private ownership of critical cyber infrastructure. As a result of this policy gap, Canada is more susceptible to cyber attacks from hostile actors that pose significant risk to the country's security. In particular, attacks involving ransomware, malware, Distributed Denial-of-Service (DDoS) attacks, and Cybercrime-as-a-Service threaten Canadian security.

Current Issues

The main pitfall of Canada's current cyber resilience strategy is the lack of implementation of a whole-of-society approach. Canada focuses on government-led initiatives that aim to engage the private sector, but lack real collaboration between different sectors in developing policies, standards, and targeted resilience goals. Across sectors such as government, technology, finance, academia, retail, energy, and healthcare, Canada has inadvertently adopted different oversight standards. While the Government of Canada (GC) outlined "secure and resilient Canadian systems" as its first goal for the 2019-2024 National Cyber Security Action Plan, their mid-term evaluation suggested issues with implementing strategies in different sectors, including health.[2] In the 2023 cyber attack on five of Ontario's hospitals, attackers gained access to private health information of hundreds of thousands of individuals, likely due to the lack of multi-factor authentication on three administrator accounts.[3] Despite Public Safety's (PS) strategy to assist different sectors in better securing their digital systems by holding various events, PS reported "very few attendees" from particular sectors, including health.[4] These events included conferences, webinars, and workshops that were aimed at educating on managing cyber risk, particular with critical infrastructure. Although securing critical Canadian systems was a key priority for PS, its lack of policy implementation and follow-through in external sectors has created fragmentation in cyber resilience-building. This is one instance of how Canada's strategies have thus far fallen short of intended outcomes. The GC's recent strategies and policies aimed at addressing this gap will be evaluated later in this chapter.

The issue of fragmented governance is not easily addressed, as Canada faces a significant challenge with private ownership of its critical cyber infrastructure.[5] The divergent priorities between the public and private sector become apparent when discussing oversight; while the GC has an obligation to protect its population with defined standards for cyber security, the private sector faces concerns with liability exposure, competitive disadvantage, disclosure risk, and security clearance limitations. With competing interests, developing a policy framework to respond to cyber threats proves difficult. Even more so, the implementation of said framework is challenging to

enforce. For example, despite federal recommendations to not pay ransoms to malicious cyber actors, private firms have often disregarded this advice.[6] During the 2019 cyber attack on LifeLabs, the organization paid a ransom to retrieve sensitive customer data.[7] While paying a ransom is not illegal in Canada, the GC's lack of standardization in its recommendations (stating most recently that paying ransoms "is up to [the] organization"[8]), further illustrate this fragmentation. As mentioned earlier in chapter one, 85% of Canada's critical infrastructure is estimated to be owned outside of the federal government. As a result, the diversity of shareholders involved with Canada's cyber infrastructure poses a challenge in both policy development and implementation.[9]

Threats

Due to these challenges, Canada is exposed to significant cyber security risks. Sophisticated attacks from adversary actors such as Russia, the People's Republic of China (PRC), Iran, and North Korea undermine Canada's efforts to achieve cyber resilience. Some of these attacks include ransomware, DDoS attacks, and Cybercrime-as-a-Service.[10] The Cyber Centre has identified ransomware (a type of malware that denies access to system or data unless a ransom is paid) as a major threat to Canada's critical infrastructure.[11] Since 2021, there has been an average 26% annual increase in ransomware incidents in Canada, with recovery costs in 2023 totalling CAD 1.2 billion.[12] A DDoS attack involves "[flooding] an online server with internet traffic to prevent users from accessing connected services and sites."[13] Unlike ransomware, a DDoS is used to simply take a system or network offline, rather than temporarily restrict. However, actors may use a DDoS attack as a distraction while employing ransomware 'under the surface.' Both types of attacks could be retained through Cybercrime-as-a-Service, which has become an increasingly common way for adversaries to conduct cybercrime by enlisting non-state actors, such as cybercriminals, to engage in hybrid warfare. While not always state-sponsored, Cybercrime-as-a-Service is growing in prevalence due to the lack of oversight within adversarial countries, who choose to not persecute cybercriminals so long as 'unfriendly' nations are the target.[14]

> **"Since 2021, there has been an average 26% annual increase in ransomware incidents in Canada, with recovery costs in 2023 totalling CAD 1.2 billion"**

Russia's cyberattacks against Ukraine illustrate the growing risks posed by increasingly sophisticated digital threats. In January 2022, Russia successfully infiltrated[15] Ukrainian government websites and attacked multiple points of digital infrastructure using "Whispergate" malware.[16] The year after, a Russian cyber actor left millions of Ukrainians without internet or service by attacking the private telecommunications company, Kyivstar.[17] The use of DDoS has also become a global concern after its use against Ukraine. Russia has launched a series of such attacks in Ukraine, primarily

targeting banking and defence websites.[18] Accordingly, Cybercrime-as-a-Service has grown as Russia turns more toward cybercriminals to engage in such attacks for low-cost and efficiency.[19]

As mass digitization across all sectors grows globally - from financial institutions, to energy grids, to railways, and hospitals - the serious consequences of a cyber attack increase. Accordingly, the risks associated with a lack of an adequate cyber resilience strategy are significant. Many may recall the global IT outage on July 19, 2024 that impacted the Microsoft Windows platform, causing flight delays, affecting hospitals, and pushing businesses offline for hours.[20] While not attributed to a cyber attack, the high-impact of the outage raises concerns for how a legitimate hostile threat may impact Canadian society. A faulty software update within the CrowdStrike Falcon Endpoint Detection and Response Tool (EDR) affected Windows systems globally, without the involvement of any hostile actors.[21] In only a few hours, government agencies and private companies alike were severely impacted, creating a large inconvenience for the everyday consumer. The widespread reliance on privately operated services indicates that a sophisticated cyber attack against a single system could produce consequences that extend well beyond the system itself.

Recent Policy Initiatives

Canada has made efforts to improve its cyber posture, namely with its recent National Cyber Security Strategy.[22] Released in February 2025, this strategy aims to address the gaps in Canada's previous cyber security approach primarily through the dedicated implementation of a 'whole-of-society' framework.[23] The three pillars of the 2025 strategy focus on: (1) working with partners to protect Canadians and Canadian businesses; (2) making Canada a global leader in cyber security; and (3) detecting and disrupting cyber threat actors. To accomplish this, the strategy sets out key action items including the establishment of the Canadian Cyber Defence Collective (CCDC), a new senior policy official for cyber, targeted grants for cyber security awareness, and new partnerships with academia. Canada is already an active player in defensive and active cyber operations through the Communications Security Establishment Canada (CSE), which has a uniquely legislated mandate to protect Canadians through defensive cyber operations.[24] Even so, these pillars make great improvements in engaging with the private sector by creating direct partnerships, providing financial assistance, and creating more educational pathways.

Additionally, the Cyber Centre's recent initiative - Critical Infrastructure Resilience and Escalated Threat Navigation (CIREN) - aims to provide organizations with a roadmap for strengthening their cyber resilience.[25] Launched in April 2026, the initiative outlines specific actions for organizations to undertake to improve their cyber security posture, moving past prevention and more toward resilience-building. Similarly, the Canadian Armed Forces Cyber Command (CAFCYBERCOM) aims to build resilience by unifying multiple different operation centres into one, unified command.[26] Launched in September 2024,[27] CAFCYBERCOM combines the existing Canadian Forces Station (CFS) Leitrim, Canadian Forces Electronic Warfare Centre (CFEWC), and the Canadian Forces Network Operations Centre (CFNOC) into a single operations command. This

command supports Canada's NATO commitments and allows for greater interoperability between Canada's key security agencies.

Most notable is the GC's recently legislated Bill C-8, which amends the Telecommunications Act and establishes the Critical Cyber Systems Protection Act (CCSPA).[28] This Bill will introduce direct oversight of telecommunications operators, mandatory cyber attack reporting, and compliance orders for designated operators. Although very recent (receiving royal assent in June 2026), these initiatives signal a more positive outlook for Canada's cyber future due to its improvements with private sector engagement and centralizing cyber security standards.

Microsoft Azure data centres in Pangborn, Wenatchee, Washington. Photo: Tedder/Wikimedia Commons, CC BY 4.0. https://commons.wikimedia.org/wiki/File:Wenatchee_washington_azure_datacenter_aerial_2.jpg

Of NATO's seven baseline requirements for ensuring national resilience, the most relevant to cyber security include: (1) assured continuity of government and critical government services and (6) resilient civil communications systems.[29] NATO's first baseline requirement compels members to ensure the continuity of critical government services in a crisis, including the ability to communicate with citizens. Bill C-8 addresses Canada's previous shortfalls in meeting this metric through multiple amendments to the Telecommunications Act. In particular, relevant amendments give the Minister of Industry power to require that a telecommunications service provider develop a security plan, conduct vulnerability assessments, take mitigation efforts, implement specific standards, and use a backup system.[30] While these amendments make strides to ensure the continuity of critical services, it shifts responsibility onto individual telecommunications entities and lacks a collaborative strategy between private agencies and different levels of government in resilience building.

NATO Ally Case Studies

Several NATO members have conducted national cyber exercises to build resilience collaboratively. These exercises bring together government agencies, private companies, and the general population to train national responses to a cyber crisis. For

example, the United States conducts its annual Cyber Storm exercise, which brings together government agencies from multiple jurisdictions and critical infrastructure operators to test cyber resilience through simulated attacks.[31] Through this, the United States can test and demonstrate its response to a potential cyber crisis and ensure it is maintaining the continuity of critical services. Similarly, the EU runs Cyber Europe to test cyber crisis management between all member states.[32]

Canada has made efforts to improve its cyber posture, namely with its recent National Cyber Security Strategy.[22] Released in February 2025, this strategy aims to address the gaps in Canada's previous cyber security approach primarily through the dedicated implementation of a 'whole-of-society' framework.[23] The three pillars of the 2025 strategy focus on: (1) working with partners to protect Canadians and Canadian businesses; (2) making Canada a global leader in cyber security; and (3) detecting and disrupting cyber threat actors. To accomplish this, the strategy sets out key action items including the establishment of the Canadian Cyber Defence Collective (CCDC), a new senior policy official for cyber, targeted grants for cyber security awareness, and new partnerships with academia. Canada is already an active player in defensive and active cyber operations through the Communications Security Establishment Canada (CSE), which has a uniquely legislated mandate to protect Canadians through defensive cyber operations.[24] Even so, these pillars make great improvements in engaging with the private sector by creating direct partnerships, providing financial assistance, and creating more educational pathways.

While NATO runs its Alliance-wide exercises (notably Locked Shields,[33] Cyber Coalition,[34] and Vigorous Warrior[35]), Canada lacks its own recurring, public-facing, cross-sector national preparedness exercise. Given the country's heavy involvement in Vigorous Warrior 2026 (NATO's largest multinational medical exercise), a domestic-focused exercise would be beneficial for government agencies and private sector alike. While a collaborative pilot exercise was started by PS in 2023, no follow-up has since been announced.[36] Putting a whole-of-society approach into practice, Estonia involves its citizens in resilience-building through its Cyber Reserve, composed of experts from the public and private sectors who would be mobilized in the event of a crisis.[37] While not yet fully implemented, the reserve force offers a unique solution to cross-sector crisis management.[38]

"While NATO runs its Alliance-wide exercises, Canada lacks its own recurring, public-facing, cross-sector national preparedness exercise."

NATO's sixth baseline requirement compels NATO members to ensure the resilience of civil communications systems in a crisis, including the ability to restore, use, and access telecommunication and cyber networks. In the newly legislated CCSPA, Canada aims to address this condition by imposing resilience standards for "designated operators." [39] These operators, as defined within the Act, are any actor that owns, controls, or operates a critical system. A broad definition that is narrowed when looking at the vital services and systems that are currently included in the legislation: telecommunications, interprovincial or international pipeline and power line systems, nuclear energy, transportation, banking, and clearing and settlement systems. The legislation puts responsibility on the operators to mitigate identified cyber risks, report cyber attacks, and comply with their appropriate regulator. In particular, six regulators are identified: the Minister of Industry, the Minister of Transport, the Superintendent of Financial Institutions, the Bank of Canada, the Canada Energy Regulator, and the Canadian Nuclear Safety Commission.

While much needed, the CCSPA falls short of achieving its purpose of "[supporting] the continuity of vital services and vital systems" as its narrow definition fails to reach sectors under provincial jurisdiction: health, education, and provincially-regulated utilities . As discussed earlier, sectors such as health are arguably the areas with the highest risk of harm in the face of a cyber attack. What is lacking in the CCSPA is any mention or role for the CCDC, which was a part of Canada's National Cyber Strategy. The CCDC was created to serve as a "national multi-stakeholder engagement body" that utilizes public-private partnerships to identify and advance key cyber priorities. [40] However, the government has provided little information on the initiative's progress since releasing the strategy. The CCSPA, while beneficial, does not currently include requirements for collaborative resilience building, nor does it impose responsibility on the government to forward these priorities. The CCSPA does include six different regulatory bodies, each with their own supervisory and enforcement cultures, that further indicates a fragmentation in strategy. The GC's suggested approach to cyber reporting, however, is an illustration of a cross-sector collaborative strategy. In the case of a cyber attack, incidents are reported to the centralized Cyber Centre, with notice given to the appropriate regulator.

Unlike the Telecommunications Act, the CCSPA did not become operative once it received Royal Assent. Part 2 of the Bill comes into force on a day to be fixed by order of the Governor in Council. No date, at the time of this publication, has been fixed to modify or add to the vital services and systems under Schedule 1, or classify the designated operators under Schedule 2. This, according to the GC, will be implemented in phases. [41] As time remains before the CCSPA becomes operative, there is opportunity for the GC to address these gaps by looking to our allies.

In the EU, critical sectors must demonstrate and test their resilience to a standard defined by the collective. The 2022 NIS2 Directive contains detailed provisions for business continuity, including digital backup and recovery.[42] Rather than a more vague cyber security program, as detailed in the CCSPA, the NIS2 directive outlines specific criteria for entities to meet to ensure cyber resilience. These specific provisions must

be overseen by management bodies, who are liable for infringements of the directive. In incorporating roles and responsibilities for management bodies, as well as laying out specific criteria for cyber resilience, the NIS2 Directive provides a more comprehensive framework to adequately meet the sixth baseline requirement in contrast to Canada's CCSPA.

Individual member states within NATO are also putting larger responsibility on the government, rather than individual private entities, to ensure cyber resilience of telecommunication and cyber networks. In Estonia, the government ensures the protection of its networks by keeping secure back-ups of critical systems in the physical territory of NATO ally, Luxembourg. This so-called "data embassy" allows Estonia to maintain ownership of its servers located outside of its borders and effectively ensure its critical systems are able to be restored, used, and accessed during a crisis.[43]

> **"In contrast to Canada's CCSPA, the NIS2 Directive provides a more comprehensive framework to adequately meet the sixth baseline requirement."**

Individual member states within NATO are also putting larger responsibility on the government, rather than individual private entities, to ensure cyber resilience of telecommunication and cyber networks. In Estonia, the government ensures the protection of its networks by keeping secure back-ups of critical systems in the physical territory of NATO ally, Luxembourg. This so-called "data embassy" allows Estonia to maintain ownership of its servers located outside of its borders and effectively ensure its critical systems are able to be restored, used, and accessed during a crisis.[43]

Overall, Canada's current policy framework and federal strategies aim to meet NATO's baseline requirements relevant to cyber resilience, but have notable gaps. However, opportunities remain (notably with the pending implementation of the CCSPA) to introduce continuity criteria and compliance expectations with named accountability measures for management bodies. Establishing a recurring, public-facing, and cross-sector national cyber exercise with a dedicated cyber reserve, in addition to CCSPA amendments, will strengthen and demonstrate domestic cyber resilience. With more room to engage private actors and the general population, as well as to pursue national solutions to better protect network security, Canada can improve its current posture and achieve its goal of becoming a leader in the cyber space.

Introduction, Digital Sovereignty

Recent advances in artificial intelligence (AI) and the growing reliance of governmental and business operations, as well as critical services, on foreign-controlled digital infrastructure have made digital sovereignty an increasingly prominent concern for Canadian policymakers. The Government of Canada (GC) defines digital sovereignty as "the capacity to exercise effective autonomy and control over digital infrastructure, data, and critical technologies".[44] In practice, this requires the government to securely store sensitive personal, public-sector, and commercially significant data and protect it from unauthorized foreign access. It also means that Canada can respond to crises that disrupt major civilian systems, such as the electricity grid, banking services, emergency alerts, healthcare, telecommunications, and other critical infrastructure. Such crises may occur due to domestic infrastructure failures, natural disasters, or adversary attacks.

Main Barriers to Canadian Digital Sovereignty

Canada is far from achieving digital sovereignty. Over 85% of Canada's market for commercial cloud services is controlled by three American hyperscalers: Amazon Web Services (AWS), Microsoft Azure, and Google Cloud.[45] Thus, much of Canadian data is subject to U.S. data governance laws. Two main laws enable American extraterritorial access to data and jeopardize Canada's digital sovereignty. The Clarifying Lawful Overseas Use of Data Act, commonly known as the CLOUD Act, allows U.S. law enforcement authorities to compel service providers subject to U.S. jurisdiction to release any data owned by them for criminal investigations, even when such data is physically stored outside the U.S.[46] In practice, this permits American companies operating in Canada, including those that control most commercial cloud services, to share Canadian data with the U.S. government without Canada's authorization.

In addition to the CLOUD Act, the American Foreign Intelligence Surveillance Act (FISA) allows the U.S. government to conduct surveillance of foreign nationals located outside the United States, as well as foreign powers and their agents, including by compelling electronic communication service providers to disclose user data.[47] Importantly, foreign power is defined as any foreign government with all its components.[48] Outside of the telecommunications sector, most electronics communications companies providing services in Canada are American. Therefore, under FISA, if a Canadian person, company, or government agency is designated as a foreign intelligence target under U.S. law, American service providers may facilitate intelligence collection without Canada's knowledge and authorization. This creates an additional risk of disclosing potentially sensitive data to foreign authorities. The GC itself has labeled FISA as the primary risk to Canada's data sovereignty.[49]

Canada's defence sector is no exception to the aforementioned laws. The Department of National Defence (DND) and the Canadian Armed Forces (CAF) use Defence 365 - a version of Microsoft 365 adapted to DND and CAF security requirements, for

communication and information management.[50] While classified information is handled through separate networks, DND has authorized the storage and processing of Protected A and certain types of Protected B information through SharePoint Online and Microsoft Azure, both Microsoft-owned cloud platforms.[51] Protected B level data includes sensitive personnel, security, medical, financial, and operational information and, if compromised, can result in a substantial injury to individuals and organizations.[52] Stored by Microsoft, this potentially sensitive defence information becomes subject to U.S. jurisdiction and may fall within reach of the CLOUD Act and FISA.

Another challenge Canada faces on its path toward digital sovereignty is low R&D investment, which halts the development of new technologies. Canada spends a smaller share of GDP on R&D than most of its G7 and OECD partners - a pattern driven largely by a sluggish private-sector investment in innovation.[53] This issue is compounded by intellectual property (IP) outflow and weak commercialization pathways - two mutually reinforcing challenges. Canada has a low IP conversion rate, which creates a gap between raw discoveries and their legal protection and commercialization.[54] Canadian IP is often sold or transferred to foreign corporations before its commercial potential is realized domestically. Even when an IP is filed at home, Canada does not provide strong commercialization pathways for new technologies, which causes many businesses to eventually incorporate abroad.[55] Therefore, it produces commercially valuable research but fails to turn it into innovation and productivity gains, effectively subsidizing the economic development of other countries, primarily the U.S. As a reflection of this trend, the past decades saw a threefold increase in Canadian-invented patent transfer abroad.[56]

> **"The past decades saw a threefold increase in Canadian-invented patent transfer abroad"**

Canadian and French cyber personnel participate in NATO Exercise CYBER COALITION 25. Photo credit: SIRPA Terre (France), via National Defence, Government of Canada. https://www.canada.ca/en/department-national-defence/maple-leaf/defence/2025/12/cafcybercom-strengthens-allied-cyber-resilience.html

This dynamic is especially visible in the digital technology sector, which is central to Canada's digital sovereignty. Approximately three-quarters of the patents attributed to discoveries of researchers at two of Canada's leading AI institutes - the Vector Institute and Mila - are owned by entities outside Canada, primarily large American technology companies.[57] Perhaps the best-known illustration of Canada's limited ability to capture the commercial value of its domestically generated digital technology research is the development of large language models (LLMs). Canada-based researchers, Geoffrey Hinton of the University of Toronto and Yoshua Bengio of the Université de Montréal, achieved breakthroughs in the foundations of modern deep learning, the core technology underpinning AI systems such as LLMs.[58] Less than a decade ago, Canada had a real window to capitalize on this foundational research and capture its commercialization. However, limited growth-stage capital and compute power, as well as a lack of major customers, prevented Canada from seizing this opportunity. Profit capture occurred in the U.S., with prominent AI companies, such as OpenAI and Anthropic, developing and scaling south of the border.

> **"Approximately three-quarters of the patents attributed to discoveries of researchers at two of Canada's leading AI institutes are owned by entities outside Canada"**

IP outflow and weak commercialization pathways hinder the development of sovereign digital infrastructure, as Canada's best talent and research flow abroad in search of profits. The Canadian government may develop strategies to invest in domestic companies. Still, they will not yield globally competitive firms if commercialization incentives continue pushing companies to incorporate in the U.S.

Current Threats

For many years, Canada has felt comfortable relying on foreign-controlled digital technology services, even if it meant sacrificing a large degree of control over critical infrastructure and sensitive government data. However, changing economic and geopolitical conditions no longer allow such a setup. Washington's increasingly volatile stance toward collective security, as well as its foreign policy that foregrounds national interest over bilateral and multilateral collaboration, presents a new challenge for Canada. Admittedly, Washington is unlikely to deliberately disrupt Canada's digital and physical infrastructure in the foreseeable future. It is far more probable that Canada's dependency on American digital technologies will become a tool of diplomatic coercion - for example, to pressure Canada into certain domestic and foreign policy choices. Canada thus risks losing a tangible degree of freedom to pursue independent policy choices, even if remaining relatively insulated from direct threats from the U.S. Other states and non-state actors continue to pose a risk of direct attacks against Canada. This challenge is compounded by the rapid digitalization of most economic processes and public services, which is exposing an increasing share of Canada's infrastructure and economic activity to digital disruptions.

Recent Policy Initiatives

Against this backdrop, the GC has begun paying increased attention to digital sovereignty and cyber security and has candidly recognized Canada's excessive strategic dependencies in the area. The White Paper on Data Sovereignty and Public Cloud (the White Paper), released in 2018 and updated in 2020, asserts the need for increased autonomy in critical sectors. Recognizing that global innovation often yields net benefit for all, it sets a path to reduce excessive reliance and manage dependencies without fully replacing them. The strategy also differentiates between data residency and data sovereignty. It acknowledges that jurisdiction over data matters more than its physical location, discussing the strategic implications of Canada's overreliance on foreign cloud providers in the context of the CLOUD Act.[59] While candid, the strategy did not propose concrete measures to build domestic compute capacity or establish targets for reducing dependencies. It also failed to identify which critical services should be fully Canadian-owned and publicly anchored and which data can be safely stored by foreign providers.

The White Paper has also yielded limited progress. Cloud consumption through Shared Services Canada rose from $1.4 million in 2019-20 to $156.9 million in 2022-23, owing in large part to a public shift to the cloud. 96% of the cloud-related spending went to three U.S. providers: Microsoft Azure, AWS, and Salesforce. Communications Security Establishment Canada and Statistics Canada were the largest consumers of cloud services.[60] Therefore, Canada's reliance on foreign cloud providers to store data, including potentially sensitive data, expanded shortly after the release of the White Paper. In this context, the GC's 2025 Digital Sovereignty Framework reiterated fundamental issues raised in the White Paper. It discussed Canada's limited digital sovereignty and reliance on foreign cloud providers, and elaborated on emerging cyber security and AI-related threats.[61]

In June 2026, to address the aforementioned challenges with clear metrics and solutions, the GC introduced AI for All Strategy, an update to the 2024 Canadian Sovereign AI Compute Strategy. AI for All commits to developing Canadian-controlled compute and data centres, requiring sovereign infrastructure that operates under Canadian law. It promises substantial investment in Canadian AI companies, namely a $500-million Canadian Tech Growth Fund and $1.75 billion in previously announced federal and venture-capital investment.[62] These concrete metrics aim to alleviate reliance on foreign digital infrastructure and lack of adequate startup financing. AI for All also addresses the challenge of IP retention and domestic commercialization. It draws on $159 million previously committed through Elevate IP and IP Assist to help Canadian SMEs protect and scale their innovations and invests $130 million in commercialization programs through Canada's national AI institutes. As with previous strategies, instead of withdrawing Canada into isolation, AI for All seeks to develop and diversify trusted partnerships, particularly with the EU, while also strengthening ties with partners in the Indo-Pacific and the Middle East.[63]

Several recent developments align with the strategy's digital sovereignty objectives. This includes significant investments from Canadian telecommunications firms into

building sovereign data centers and developing domestic compute capacity.[64] Such data centers will allow Canada to control who has access to its data and monitor the cyber and physical security of data facilities. Nevertheless, these facilities are still expected to run on tens of thousands of NVIDIA's graphics processing units (GPUs) - a computer chip used to train and operate AI models, designed in the U.S. and manufactured primarily by companies in Asia, most notably Taiwan-based TSMC.[65] NVIDIA also controls the supporting software required to operate AI systems efficiently on its GPUs.[66] This dependency leaves Canada vulnerable to export restrictions, supply chain disruptions, and potential caps on computing capacity imposed by actors controlling GPU development and production. Therefore, even with sovereign data centers, Canada may struggle to procure sufficient quantities to replace and upgrade the hardware used in its computing infrastructure.

High costs and technically complex manufacturing processes with an advanced supply chain spanning many countries make GPU sovereignty more unattainable than domestic ownership of data centres. Although AI for All, in passing, mentions the need to strengthen Canada's chip-design and fabrication capabilities, reaching sovereign production in the near future is unrealistic.[67] In the short and medium term, Canada should prioritize diversifying its GPU procurement and reducing vendor lock-in to help minimize the risk of a single entity gaining control over supply-chain chokepoints. Interoperability standards and, where technically feasible, multi-vendor requirements for publicly funded computing infrastructure could be practical starting points for Canada to improve its policies on procurement and operation of GPUs.

In addition to the limitations outlined above, AI for All has faced backlash caused by the expected environmental effects of building data centres and the implications of AI adoption for employment.[68] Admittedly, AI for All provides limited reassurance to young Canadians who fear that AI expansion could further intensify the existing employment crisis. While promising to secure employment through the creation of new AI-related jobs and entry-level AI training, the strategy does not offer a mechanism to monitor job displacement, support workers whose positions disappear, or address the loss of entry-level jobs outside the AI sector.[69] Environmental and social considerations should therefore be addressed more thoroughly in forthcoming policies and carefully balanced against national security objectives.

NATO Ally Case Studies: Sovereign Compute and Data Protection Legislation

Despite aforementioned challenges, it is feasible for Canada to develop digital sovereignty capabilities. Here, Canada's NATO allies offer inspiration. For instance, in February 2026, France announced that all of its government departments will cease using Microsoft 365 and Zoom by 2027.70 Instead, the country is transitioning to Visio - a government-developed platform, hosted on French cloud infrastructure. Government officials are already banned from using Teams or Zoom at work. France does not represent an isolated case. Growing attention to the extraterritorial reach of U.S. data laws, together with heightened uncertainty around U.S. foreign and domestic policy

under the second Trump administration, has prompted many countries to reassess their reliance on American hyperscalers. Many EU states have begun moving away from Microsoft software, primarily adopting a free and open-source alternative called LibreOffice.[71]

Canada should follow the example of its allies and avoid overstating the challenges involved in reducing reliance on American hyperscalers. As shown by examples above, viable alternatives already exist, and Canada should begin pursuing them today. Nevertheless, decoupling may not always be a preferred option. As proposed in the 2025 Federal Digital Sovereignty Framework, Canada should adopt a risk-based approach to digital sovereignty and assess how individual systems may be operated.[72] Lower-risk workloads may continue using foreign-owned cloud platforms, while systems essential to national security, critical infrastructure, and the continuity of essential services should be owned and controlled in Canada. Some private sector entities might find it desirable to continue using foreign providers due to their cost-effectiveness and wide range of services. In such a case, Canada must enact more stringent regulations to compel foreign providers to operate within the Canadian data governance framework.

In this area as well, Canada can reflect on the experience of its allies.. The European Union General Data Protection Regulation (GDPR) is one example that offers valuable lessons. GDPR lays out the EU's data privacy laws. Many view it as a counterpart to Canada's Personal Information Protection and Electronic Documents Act (PIPEDA), although GDPR is often considered more comprehensive.[73] One important distinction between GDPR and PIPEDA lies in the former's inclusion of the right to be forgotten. This right allows EU citizens to request that a cloud provider erase their personal data from its servers under specific circumstances, meaning users can compel foreign companies to delete their data upon request.[74] The right to be forgotten does not override extraterritorial reach laws such as the CLOUD Act, but it reduces the amount of data foreign companies can share with their governments.

Another crucial difference lies in the gravity of fines that a governing body can impose on a company that fails to comply with the data protection laws. Under GDPR, such fines can reach up to 20 million EUR or 4% of the company's annual global revenue.[75] In contrast, PIPEDA's fines rarely exceed 10,000 CAD.

This underwhelming sum does not provide a sufficiently strong incentive to comply with the data protection laws. Several articles in Chapter 5 of the GDPR also guarantee that international data transfers must comply with protection guaranteed by European law.[76] This clause was most famously enforced in the 2020 Schrems II case, which arose from Austrian privacy activist Max Schrems's complaint concerning Facebook Ireland's transfer of personal data to the U.S. Schrems argued that American surveillance programs did not comply with the protection of EU citizens' data guaranteed under EU law. The European Court of Justice concluded that data transfers were indeed broader than necessary, invalidating the previous EU-U.S. Privacy Shield data-sharing agreement between the EU and the U.S.[77] This case serves as a clear example of enforcing domestic data-protection law and constraining data transfers to major foreign service providers.

This underwhelming sum does not provide a sufficiently strong incentive to comply with the data protection laws. Several articles in Chapter 5 of the GDPR also guarantee that international data transfers must comply with protection guaranteed by European law.[76] This clause was most famously enforced in the 2020 Schrems II case, which arose from Austrian privacy activist Max Schrems's complaint concerning Facebook Ireland's transfer of personal data to the U.S. Schrems argued that American surveillance programs did not comply with the protection of EU citizens' data guaranteed under EU law. The European Court of Justice concluded that data transfers were indeed broader than necessary, invalidating the previous EU-U.S. Privacy Shield data-sharing agreement between the EU and the U.S.[77] This case serves as a clear example of enforcing domestic data-protection law and constraining data transfers to major foreign service providers.

Until recently, Canada's PIPEDA did not provide an equivalent of the aforementioned GDPR protections. Bill C-36, a legislation proposed in June 2026, offered a first comprehensive overhaul to Canada's private-sector privacy laws in 25 years. Bill C-36 introduced a right to request deletion of user personal information in certain instances - a right akin to Article 17 of the GDPR. The bill also proposed increasing the non-compliance fines up to $25 million or 5% of the organization's global revenue for the most serious offences. One remaining gap is that of extraterritorial data transfers.[78] Unlike GDPR, neither PIPEDA nor a newly proposed BILL C-36 requires international data transfers to preserve the domestic level of data and privacy protection. If passed, Bill C-36 would require organizations to assess and mitigate transfer risks, but it would not prohibit transfers when foreign surveillance laws make a domestic level of protection impossible.

> **"Neither PIPEDA nor a newly proposed BILL C-36 requires international data transfers to preserve the domestic level of data and privacy protection"**

Bill C-36 is an important step toward implementing more stringent rules on data protection and sharing in Canada. However, it does not adequately restrict extraterritorial data transfers, leaving a major gap in Canada's privacy framework. Additionally, the law will likely not be passed in the immediate future. Although careful legislative review is necessary, rapid AI developments and foreign surveillance campaigns represent real and immediate threats, requiring prompt and adaptive legislation and policymaking that respond to emerging challenges. Achieving digital sovereignty for Canada still requires closing policy gaps and modernizing regulation to ensure greater control over its citizens' data. This step does not require extensive financial investment or the creation of complex new governing structures.. Its implementation relies on Canada's long-standing institutional strengths, including respect for the rule of law and fair and democratic institutions, making regulatory reform one of the most immediately achievable steps Canada can take toward greater digital sovereignty.

Endnotes:

1. "Glossary," Government of Canada, Canadian Centre for Cyber Security, Accessed August 23, 2026, https://www.cyber.gc.ca/en/glossary.
2. Public Safety Canada, "National Cyber Security Action Plan 2019-2024" (2019).
3. "Privacy Investigator in Ontario Hospital Cyberattack Outlines Missteps, Chances to Improve," CBC News, June 18, 2025, https://www.cbc.ca/news/canada/windsor/ransomware-privacy-commissioner-hospitals-1.7564336.
4. Public Safety Canada, "Mid-Term Evaluation of the National Cyber Security Strategy - Public Safety Canada's Initiatives - Evaluation Report" (2022).
5. "Critical Infrastructure," Public Safety Canada, Government of Canada, Last modified March 26, 2025, https://www.publicsafety.gc.ca/cnt/trnsprnc/brfng-mtrls/prlmntry-bndrs/20200724/020/index-en.aspx.
6. "Parliamentary Committee Notes: Ransomware," Public Safety Canada, Government of Canada, Published July 31, 2023; last modified June 4, 2024, https://www.securitepublique.gc.ca/cnt/trnsprnc/brfng-mtrls/prlmntry-bndrs/20240614/18-en.aspx.
7. Ron Babin, "LifeLabs: The Ethics of Responding to a Ransomware Cyber Attack," Open Access Teaching Case Journal 1, no.2 (2023), doi: https://doi.org/10.58067/7wmc-gv65.
8. "Ransomware Playbook," (ITSM.00.099, Canadian Centre for Cyber Security, 2021).
9. Public Safety Canada, "Canada's National Cyber Security Strategy," (ISBN: 978-0-660-72268-9, 2025).
10. Canadian Centre for Cyber Security, "National Cyber Threat Assessment 2025-2026" (ISSN 2816-9174, 2024).
11. "Ransomware Threat Outlook 2025-2027," Canadian Centre for Cyber Security, Government of Canada, Last modified January 28, 2025, https://www.cyber.gc.ca/en/guidance/ransomware-threat-outlook-2025-2027.
12. See note 10.
13. Canadian Anti-Fraud Centre, "Distributed Denial of Service Attacks," Government of Canada, Last modified March 9, 2026. https://antifraudcentre-centreantifraude.ca/scams-fraudes/ddos-eng.htm.
14. Hannah Gately, "Russian Organized Crime and Ransomware as a Service: State Cultivated Cybercrime," Macquarie University, (2023). https://doi.org/10.25949/23692932.v1.
15. Oleksandr Bakalynskyi and Maggie McDonough, "Learning the Lessons from Ukraine's Fight Against Russian Cyber Warfare," Atlantic Council, November 6, 2025, https://www.atlanticcouncil.org/blogs/ukrainealert/learning-the-lessons-from-ukraines-fight-against-russian-cyber-warfare/.
16. Maxime Nijs, "Cyber Operations Against Government Systems in Ukraine (January 2022)," Cyber Law CCDCOE, Last modified March 1, 2022, https://cyberlaw.ccdcoe.org/wiki/Cyber_operations_against_government_systems_in_Ukraine_(January_2022).
17. Canadian Centre for Cyber Security, "National Cyber Threat Assessment 2025-2026" (ISSN 2816-9174, 2024).
18. Kyle Fendorf and Jessie Miller, "Tracking Cyber Operations and Actors in the Russia-Ukraine War," Council on Foreign Relations, March 24, 2022, https://www.cfr.org/articles/tracking-cyber-operations-and-actors-russia-ukraine-war.

Endnotes:

19. Antoaneta Roussi, "Russia Taps Cybercriminals to Keep Military Pressure on Ukraine," Politico, February 12, 2025, https://www.politico.eu/article/russia-cybercriminal-military-pressure-ukraine/.
20. CBC News, "Day of Disruptions, Dashed Plans for Many Canadians After Global Tech Outage," July 19, 2024, https://www.cbc.ca/news/world/cyberstrike-worldwide-outage-1.7268863.
21. Canadian Centre for Cyber Security, "Alert - Issue Impacting CrowdStrike Falcon EDR," Government of Canada, July 19, 2024, https://www.cyber.gc.ca/en/alerts-advisories/issue-impacting-crowdstrike-falcon-edr.
22. Public Safety Canada, "Canada's National Cyber Security Strategy."
23. Public Safety Canada, "Government of Canada Introduces New National Cyber Security Strategy," Government of Canada, February 6, 2025, https://www.canada.ca/en/public-safety-canada/news/2025/02/government-of-canada-introduces-new-national-cyber-security-strategy.html.
24. National Security and Intelligence Committee of Parliamentarians (NSICOP), "Part III: Key Cyber Defence Players, Authorities and Activities," Accessed September 13, 2026, https://nsicop-cpsnr.ca/reports/rp-2022-02-14/05-en-part-3-3.html.
25. Communications Security Establishment Canada, "Cyber Centre Launches New Initiative to Help Canada's Critical Infrastructure Prepare for Severe Cyber Threats," April 17, 2026, https://www.canada.ca/en/communications-security/news/2026/04/cyber-centre-launches-new-initiative-to-help-canadas-critical-infrastructure-prepare-for-severe-cyber-threats.html.
26. National Defence, "Canadian Armed Forces Cyber Command (CAFCYBERCOM)," Government of Canada, Modified April 7, 2026, https://www.canada.ca/en/department-national-defence/corporate/organizational-structure/cafcybercom.html.
27. National Defence, "Canadian Armed Forces establishes a new Cyber Command," Government of Canada, September 26, 2024, https://www.canada.ca/en/department-national-defence/news/2024/09/canadian-armed-forces-establishes-a-new-cyber-command.html.
28. An Act Respecting Cyber Security, Amending the Telecommunications Act and Making Consequential Amendments to Other Acts, 45th Parl., Session 1 (2026).
29. NATO, "Resilience, Civil Preparedness and Article 3," Last modified November 13, 2024, https://www.nato.int/en/what-we-do/deterrence-and-defence/resilience-civil-preparedness-and-article-3.
30. An Act Respecting Cyber Security, 45th Parl., Session 1 (2026).
31. Cybersecurity & Infrastructure Security Agency, "Cyber Storm X: National Cyber Exercise," Accessed August 24, 2026, https://www.cisa.gov/resources-tools/resources/cyber-storm-x.
32. European Union Agency for Cybersecurity, "Cyber Europe," Accessed August 24, 2026, https://www.enisa.europa.eu/topics/skills-and-competences-for-companies/cyber-europe.
33. The NATO Cooperative Cyber Defence Centre of Excellence, "Locked Shields," Accessed August 24, 2026, https://ccdcoe.org/exercises/locked-shields/.
34. Allied Command Transformation, "Cyber Coalition: NATO's Flagship Cyber Exercise," Accessed August 24, 2026, https://www.act.nato.int/activities/cyber-coalition/.

Endnotes:

35. NATO, "NATO's Largest Medical Exercise Strengthens Allied Medical Readiness," June 25, 2026, https://www.nato.int/en/news-and-events/articles/news/2026/06/25/natos-largest-medical-exercise-strengthens-allied-medical-readiness.
36. Public Safety Canada, "Cyber-Physical Capstone Exercise After-Action Report," Government of Canada, October 26, 2023, https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cpstn-xrcs-ftr-ctn-rprt-2024/index-en.aspx.
37. Republic of Estonia Information System Authority, "Cyber Security in Estonia 2026," Last modified February 11, 2026, https://www.ria.ee/en/worst-case-we-could-be-without-electricity-days.
38. Republic of Estonia Ministry of Economic Affairs and Communications, "Cybersecurity Strategy 2024-2030 'Cyber-Conscious Estonia'," (2024).
39. An Act Respecting Cyber Security, 45th Parl., Session 1 (2026).
40. Public Safety Canada, "Canada's National Cyber Security Strategy."
41. Public Safety Canada, "Government of Canada Strengthens Cyber Security and Critical Infrastructure with Royal Assent of Bill C-8," Government of Canada, June 16, 2026, https://www.canada.ca/en/public-safety-canada/news/2026/06/government-of-canada-strengthens-cyber-security-and-critical-infrastructure-with-royal-assent-of-bill-c8.html.
42. Directive (EU) 2022/2555 of the European Parliament and of the Council, L 333/80, (2022).
43. E-Estonia, "Data Embassy," Accessed August 24, 2026, https://e-estonia.com/service/e-governance/data-embassy/.
44. Shared Services Canada, "Digital Sovereignty - Canada.Ca," Canada.Ca, 2026, https://www.canada.ca/en/shared-services/services/digital-sovereignty.html.
45. Curtis McCord and David Eaves, "Parting Clouds: Creating a Competitive Marketplace for Compute," Canadian Anti-Monopoly Project, June 2026, https://antimonopoly.ca/wp-content/uploads/2026/05/CAMP_Report_Parting_Clouds.pdf.
46. U.S. Department of Justice, Promoting Public Safety, Privacy, and the Rule of Law Around the World: The Purpose and Impact of the CLOUD Act (U.S. Department of Justice, 2019), https://www.justice.gov/d9/press-releases/attachments/2019/04/10/department_of_justice_cloud_act_white_paper_2019_04_10_final_0.pdf.
47. Office of the Director of Intelligence, "INTEL - Foreign Intelligence Surveillance Act," Www.Intel.Gov, 2026, https://www.intel.gov/foreign-intelligence-surveillance-act.
48. Cornell Law School, "50 U.S. Code § 1801 - Definitions," LII / Legal Information Institute, 2010, https://www.law.cornell.edu/uscode/text/50/1801.
49. Government of Canada, "Government of Canada White Paper: Data Sovereignty and Public Cloud," Canada.Ca, June 25, 2018, https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/cloud-services/digital-sovereignty/gc-white-paper-data-sovereignty-public-cloud.html.
50. Government of Canada, "Defence 365 - Frequently Asked Questions (FAQs)," Government of Canada, August 5, 2025, https://www.canada.ca/en/department-national-defence/corporate/job-opportunities/civilian-jobs/new-job/d365.html.

Endnotes:

51. Government of Canada, "Defence 365 - Frequently Asked Questions (FAQs)," Canada.Ca, 2025, https://www.canada.ca/en/department-national-defence/corporate/job-opportunities/civilian-jobs/new-job/d365.html.
52. Government of Canada, "Levels of Security ," Canada.Ca, 2026, https://www.canada.ca/en/public-services-procurement/services/industrial-security/security-requirements-contracting/safeguarding-equipment-sites-assets-information/levels-security.html.
53. The Centre for Innovation Studies, "R&D in Canada – Increasing but More Is Needed. - Blog #78," THECIS - The Centre for Innovation Studies, December 18, 2024, https://thecis.ca/rd-in-canada-increasing-but-more-is-needed-blog-78/.
54. Canadian Shield Institute, "Foundations of Digital Sovereignty Chapter 3," Canadianshieldinstitute.Ca, May 31, 2026, https://canadianshieldinstitute.ca/reports/foundations-of-digital-sovereignty-chapter-3.
55. Nancy Gallini Gallini and Aidan Hollis, "To Sell or Scale Up: Canada's Patent Strategy in a Knowledge Economy," IRPP, Institute for Research on Public Policy, August 27, 2019, https://irpp.org/research-studies/to-sell-or-scale-up-canadas-patent-strategy-in-a-knowledge-economy/.
56. Canadian Shield Institute, Foundations of Digital Sovereignty.
57. Anja Karadeglija, "Canada Is a Force in AI Research. So Why Can't the Country Commercialize It?," The Globe and Mail, June 26, 2024, https://www.theglobeandmail.com/business/technology/article-canada-is-a-force-in-ai-research-so-why-cant-the-country-commercialize/.
58. Association for Computing Machinery, "2018 ACM A.M. Turing Award Laureates," Awards.Acm.Org, 2018, https://awards.acm.org/about/2018-turing.
59. Government of Canada, "Government of Canada White Paper".
60. Shared Services Canada, "Evaluation of Shared Services Canada's Cloud Services," Government of Canada, 2024, https://www.canada.ca/en/shared-services/corporate/about-us/transparency/audits-evaluations/2024-25/evaluation-ssc-cloud-services.html.
61. Government of Canada, "Digital Sovereignty: A Framework to Improve Digital Readiness of the Government of Canada - Canada.Ca," Canada.Ca, 2025, https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/cloud-services/digital-sovereignty/digital-sovereignty-framework-improve-digital-readiness.html.
62. Government of Canada, "Canada's National Artificial Intelligence Strategy: AI for All," Canada.Ca, June 5, 2026, https://ised-isde.canada.ca/site/ised/en/canadas-national-artificial-intelligence-strategy-ai-all.
63. Government of Canada, AI for All.
64. Pippa Norman et al., "Telus Plans AI Data Centre Expansion in B.C., Including Two New Centres in Vancouver," The Globe and Mail, May 11, 2026, https://www.theglobeandmail.com/business/article-telus-plans-ai-data-centre-expansion-in-bc-including-two-new-centres/.
65. William Alan Reinsch and Jack Whitney, "Silicon Island: Assessing Taiwan's Importance to U.S. Economic Growth and Security," Csis.Org, January 10, 2025, https://www.csis.org/analysis/silicon-island-assessing-taiwans-importance-us-economic-growth-and-security.

Endnotes:

66. NVIDIA, "CUDA Toolkit 13.4 - Release Notes — Release Notes 13.4 Documentation," Nvidia.Com, 2026, https://docs.nvidia.com/cuda/cuda-toolkit-release-notes/index.html?_gl=1.
67. Government of Canada, AI for All.
68. Joe Castaldo, "Majority of Canadians Oppose Government Support for AI Data Centres, Poll Shows," The Globe and Mail, August 11, 2026, https://www.theglobeandmail.com/canada/article-ai-data-centre-opposition-government-support-nanos-poll/.
69. Prime Minister of Canada, Prime Minister Carney Launches AI for All: Canada's New National Artificial Intelligence Strategy," Prime Minister of Canada, June 4, 2026, https://www.pm.gc.ca/en/news/speeches/2026/06/04/prime-minister-carney-launches-ai-all-canadas-new-national-artificial.
70. Pascale Davies, "French Government to Ditch US's Teams and Zoom for 'Sovereign Control'," Euronews, euronews.com, January 27, 2026, https://www.euronews.com/next/2026/01/27/france-to-ditch-us-platforms-microsoft-teams-zoom-for-sovereign-platform-amid-security-con.
71. Vass Bednar, "France Is Ditching American Tech. When Will Canada?," Theglobeandmail.Com, February 10, 2026, https://www.theglobeandmail.com/business/commentary/article-france-is-ditching-american-tech-when-will-canada/.
72. Government of Canada, Digital Sovereignty: A Framework to Improve Digital Readiness.
73. Alexis Dessaints, "PIPEDA vs GDPR: Understanding the Key Differences In 2025," Dpo-Consulting.Com, DPO Consulting, September 19, 2025, https://www.dpo-consulting.com/blog/pipeda-vs-gdpr.
74. GDPR, "General Data Protection Regulation (GDPR)," GDPR, 2018, https://gdpr-info.eu/.
75. Alexis Dessaints, PIPEDA vs GDPR.
76. GDPR.
77. RISMA, "What Is Schrems II | See the Rules for Data Transfers | RISMA," Rismasystems.Com, RISMA Systems A/S, February 14, 2025, https://www.rismasystems.com/en/resources/articles/schrems-ii.
78. Innovation, Science and Economic Development Canada, "Backgrounder: Government of Canada Introduces Legislation to Protect Canadians' Privacy in the Digital Age," Canada.Ca, Government of Canada, June 15, 2026, https://www.canada.ca/en/innovation-science-economic-development/news/2026/06/government-of-canada-introduces-legislation-to-protect-canadians-privacy-in-the-digital-age.html.

Author: Keya Patel, Program Editor

Chapter 4. Public Health

Executive Summary

Canada's national public health resilience faces several impediments that undermine its ability to meet NATO's fifth baseline requirement of developing resilient health systems capable of coping during crises. These challenges include healthcare workforce shortages, limitations with physician training, a nursing retention problem, Federal-Provincial-Territorial jurisdictional fragmentation, issues with upkeep of National Emergency Strategic Stockpile (NESS), and a dependency on foreign-manufactured medical countermeasures. These issues share a common root cause: Canada has the capacity to address them, but lacks the legal, financial, and institutional mechanisms to convert capacity into functioning resilience.

Main Policy Recommendations

- **Health Workforce:** Canada should continue utilizing foreign-trained professionals to close the gap in the short-run, while expanding domestic medical and nursing training for the long term, and improve nurse retention through better working conditions.
- **Pan-Canada Coordination**: Canada should expand shared health data collection, create a dedicated coordinating body modeled on the UK's approach, and continue working to bring Quebec into national planning while respecting its autonomy.
- **Stockpile (NESS):** Canada should stock more routine medical supplies, guarantee stable long-term funding, and encourage increased participation through the private-sector, while promoting household stockpiling.
- **Medical Supply Chain:** Canada should keep investing in domestic production of critical medical countermeasures to reduce reliance on foreign manufacturers.

Introduction

If there's one thing the recent COVID-19 pandemic has highlighted, it is the need for public health resilience, an often overlooked but critical component of national resilience, given that issues ranging from war to environmental concerns to supply chain disruptions to pandemics are all bound to affect public health. This section explores Canada's gravest challenges to national public health resilience, primarily affecting NATO's fifth baseline requirement for resilience. The first challenge is rooted in Canada's health workforce shortage among a variety of primary care professions. While actions such as the Pan-Canadian Health Workforce Data Strategy and the Foreign Credential Recognition Action Fund mark a start toward addressing Canada's largest barrier to public health resilience, additional work will be needed. The second challenge stems from the fact that Canada's healthcare systems are governed provincially and territorially, which not only compounds the first challenge but also serves as a roadblock to national health resilience planning more broadly. The third challenge comes from the mismanagement of the National Emergency Strategic Stockpile (NESS). Since COVID-19, the NESS has received significant attention and investment toward revitalization. However, true success will lie in whether this attention continues once the memory of the pandemic fades. Finally, the fourth challenge this paper identifies is Canada's dependency on foreign-manufactured drugs and medical devices, a vulnerability also shared by other NATO members.

Valerushka_kay. "Coronavirus, Paramedic, Protective Suit." Pixabay. February 4, 2021. https://pixabay.com/photos/coronavirus-paramedic-5981935/ .

> **"While no nation can be fully self-sufficient, Canada must take further steps to ensure that, in times of crisis, crucial drugs and medical supplies can be produced domestically."**

This chapter begins by exploring these four barriers to national public health resilience in detail, then examines case studies from Finland and the United Kingdom that offer useful structures for reducing these barriers, and finally prescribes a range of policy recommendations to address each key challenge.

Policy Overview and Evaluation

Healthcare Workforce Shortage

One of the preliminary roadblocks to attaining national public health resilience in Canada comes from a significant shortage in its healthcare workforce. The recent Caring for Canadians: Canada's Future Health Workforce - The Canadian Health Workforce Education, Training and Distribution Study (the Study), published in January 2025 by the Government of Canada, was the first pan-Canada study of this kind, and was specially requested, almost unanimously, by the nation's Federal-Provincial-Territorial Health Ministers in October of 2023 to help better understand Canada's health workforce capacity.[1] One of the key findings from the study was that a health workforce shortage does exist, and more importantly, is projected to worsen over the next ten years if no action is taken to address the issue. The study sought to evaluate, in particular, the primary care workforce, narrowed down to the following five professions: nursing (of varying kinds), occupational therapy, physiotherapy, pharmacy, and physicians. Shortages exist in all five categories, much of which can be attributed to a lack of commitment in educating people within these professions. For instance, in 2024, Canada had a nearly 14,000 physician deficit. At the same time, Canada only has a new medical graduate rate of 7.5 per 100,000, which is only slightly more than half the rate of the OECD average at 14.2 per 100,000.[2] In contrast, the rates for nursing, which appear quite promising at 10.0, higher than the OECD average of 9.0 per 1,000 population in 2025, are misleading,[3] with the Canadian Federation of Nurses Unions estimating that over 30,000 nursing positions went vacant within the same year. This alludes to a greater problem of the nursing profession's retention rates, with many nurses experiencing burnout from their workplaces operating at overcapacity.[4] In fact, a 2022 statistic from the MEI reports that among young nurses, 40 out of 100 leave the profession before the age of 35.[5] NATO's fifth baseline requirement for national resilience states that NATO members should be able to ensure civilian health systems can cope in the event of disruptions,[6] and primary care can be regarded as a crucial basis for health systems. If health systems are already facing primary care shortages in the day-to-day, it raises serious doubts about their preparedness in the event of shocks. In fact, the most recent health shock, COVID-19, actually left Canada with a smaller

healthcare workforce than prior to it; in 2019, Health Canada had 10,794 employees and has since dropped to 9,628 in 2025. C.D. Howe describes Health Canada as the "only major federal department with fewer employees now than before the pandemic."[7]

The evidence for healthcare worker shortage is extensive. However, the government has taken various actions to help close the gap in two ways, firstly, by making it easier for foreign-trained professionals to join the Canadian healthcare sector to address the short-run gap, and secondly, by expanding medical training within Canada to increase the capacity of domestically trained health professionals in the long-run. In the short-run, the Canadian government introduced the Foreign Credential Recognition Action Fund, which will allow $97 million allocated over five years from the 2025 budget to work towards speeding up the process for internationally trained healthcare professionals to become approved to work in Canada.[8] Maximizing on the foreign-trained labour strategy, British Columbia has incentivized U.S.-trained professionals, and nurses in particular, to join their healthcare system amidst the declining retention rates of Canadian nurses. While attracting U.S. nurses is a short-term fix to the nursing shortage, B.C., alongside recruiting these nurses, aims to fix the systematic problem of nursing burnout by introducing retention bonuses, nurse-patient ratios and flexible shift options.[9] For the long-term fix, many provinces are focused on training more professionals domestically. For instance, Ontario announced the addition of 270 new residency seats alongside opening two new medical schools, with existing schools working to expand their programs.[10] Alberta has taken a similar approach, committing roughly $20 million to add 120 new medical school seats and 100 new residency spots over three years, alongside a further $30 million toward 1,800 new training seats for nurses, paramedics, and other healthcare workers.[11] New Brunswick has pursued a narrower but still notable expansion, funding eight new francophone medical school seats at Université de Moncton, aimed specifically at addressing linguistic and rural access gaps in the province.[12] British Columbia has similarly expanded its training pipeline, launching a new competitive residency stream open to both Canadian and international medical graduates, prioritizing specialties facing the most acute shortages, such as emergency medicine, internal medicine, and diagnostic radiology.[13]

Federal-Provincial-Territorial Jurisdictional Fragmentation

The second barrier to attaining national public health resilience in Canada would be the Federal-Provincial-Territorial Jurisdictional Fragmentation, which exacerbates the first challenge by impeding national coordination. This fragmentation runs directly against the coherence NATO's framework assumes at the national level. Baseline Requirement 1 calls for continuity of government functions during a crisis, a standard that presumes some baseline coordination across levels of government, not thirteen provincial and territorial health systems each operating according to their own priorities and timelines. As discussed in the previous section, provinces are taking varying steps to ensure an increase in domestically trained medical professionals, but this is not a coordinated effort. If anything, the federal government should serve as a coordinator amongst provinces and territories to ensure an equitable distribution of funding towards the

areas that are projected to need medical professionals the most. Practically, this could mean shifting away from provinces and territories independently planning medical school and residency placements towards a coordinated national approach where placements are planned collectively across the nation.

For example, while a medical school could train future healthcare professionals where facilities may best be built in one province, residency placements for students of such a medical school would be dispersed all across the country and especially where primary care providers are needed most. If provinces and territories continue to simply work individually to fix their systems according to their own means, addressing the needs of health systems across Canada will not be possible. Given that provinces and territories have thus far had full control of their health systems, it would no doubt be challenging to bring each region on the same page towards collaborating on a nationally coordinated health system plan. Certain regions, such as Quebec, would likely be hard to convince as Quebec was the only region within Canada to not take part in the Study and has been described to "not subscribe to pan-Canadian approaches regarding the health workforce and intends to retain its full autonomy in its jurisdiction in the administration of its health system."[14] Quebec's individualism isn't just a problem for workforce coordination, but also as we'll later see in other issues, impacts collective national resilience for public health at a greater scale. Moreover, when Canada's national resilience for public health crises was tested in 2020, a 2025 Frontiers in Public Health Publication claimed that the "complexity" of the nation's pandemic response was as difficult and was due to the "multilevel governance structure of public health, with roles and responsibilities delineated across federal, provincial/territorial, and local health authorities."[15]

Learning from this, the federal government has since taken some action towards pan-Canada coordination with the launch of the Pan-Canadian Health Workforce Data Strategy, which was released in March 2026 and aims to accurately collect, manage and use health workforce data in order to better plan workforce allocation in the future.[16] Moreover, the aforementioned Foreign Credential Recognition Action Fund was also aimed to induce Provincial and Territorial coordination, with the federal government playing "a coordinating role—bringing together key partners, providing information and support, and facilitating access to programs and services that help newcomers obtain credential recognition."[17] The federal government has also attempted to use its fiscal leverage to encourage coordination: through the "Working Together to Improve Health Care for Canadians" plan, Ottawa has committed $25 billion over ten years specifically to support the health workforce and modernize health systems.[18] Taking actions such as the Pan-Canadian Health Workforce Strategy, Working Together Plan and the Foreign Credential Recognition Action Fund are important first steps towards Canada becoming more nationally resilient for public health; however, only time will tell the success these initiatives have. These tools, however, remain fundamentally soft-power instruments; the federal government can offer data, funding incentives, and coordination support, but cannot compel provincial action. Quebec's explicit refusal to participate in the pan-Canadian Study is direct evidence of this limitation: a province can simply decline the federal government's coordinating role entirely, and there is currently no mechanism to

prevent this. Regardless, Canada seems to be taking a promising step forward in collective preparation for health crises. After all, a nation cannot be considered truly nationally resilient when it has varying levels of health crisis preparedness across its regions.

> **"After all, a nation cannot be considered truly nationally resilient when it has varying levels of health crisis preparedness across its regions"**

National Emergency Strategic Stockpiles (NESS)

The third impediment to Canadian national public health resilience is the state of the National Emergency Strategic Stockpile (NESS), which exists to address the "sufficient medical supplies are stocked and secure" component of NATO's fifth baseline requirement for national resilience.[19] The NESS was introduced following the Cold War to ensure materials needed for nuclear disaster response were set aside, and has since evolved to stockpile medical supplies for other public health emergencies, including natural disasters and pandemics.[20] The NESS upkeep is expensive and often overlooked. In fact, when the demand for personal protective equipment (PPE) rose sharply in 2020, a 2021 Office of the Auditor General (OAG) audit found that Health Canada and the Public Health Agency of Canada (PHAC) were "not as prepared as [they] could have been" to meet provincial and territorial demand for routine medical countermeasures in a globally competitive market. The audit traced this directly to long-standing funding gaps: with limited ongoing budgets, the NESS had prioritized investment in niche, high-consequence but low-probability assets, such as countermeasures for chemical or nuclear threats, on the assumption that routine supplies like PPE would remain readily available on the open market. That assumption collapsed the moment a pandemic created global competition for the same limited stock, and the result was a stockpile ill-equipped for the exact kind of shock NATO's fifth baseline requirement anticipates.[21]

The available evidence does not show whether the NESS was subject to meaningful audit oversight before the pandemic began; the audits available are all from 2021 onward, conducted in the pandemic's aftermath rather than in advance of it.[22] What those retrospective audits do reveal, however, is that the underfunding driving NESS's routine-supply gaps was not a sudden or unforeseeable failure: the 2021 OAG audit traced the problem to long-standing funding decisions that predated the pandemic itself. In other words, the crisis did not create the vulnerability; it exposed a vulnerability that had already been built into how the stockpile was funded and prioritized, and it took the crisis itself to trigger the audit that identified it.

In response, the federal government introduced a Comprehensive Management Plan (CMP) to modernize NESS operations, including a new Warehouse Management System and expanded legal authorities for distribution.[23] This represents notable progress, and the PHAC has since held bilateral meetings with provinces and territories to discuss lessons learned from the pandemic response. Yet these consultations themselves surfaced an unresolved gap: provinces and territories explicitly told the federal government they wanted clearer delineation of federal-provincial-territorial roles and responsibilities, along with stronger federal leadership in building a shared understanding of Canada's threat and supply chain landscape, meaning that as of these 2023 discussions, that clarity still did not exist.[24] This is the same jurisdictional fragmentation identified as Canada's second resilience impediment, resurfacing here in a different form. The CMP's administrative modernization is a necessary step, but it does not by itself guarantee that Parliament will sustain funding for routine medical countermeasures once the memory of COVID-19 recedes from political attention, which is precisely the failure pattern that produced the crisis in the first place.[25] Whether Canada has truly broken this cycle, or simply modernized the mechanics of a stockpile still vulnerable to the same underlying neglect, remains an open question, and one that will only be answered by how the federal government funds and prioritizes the NESS in the years after this crisis has fully faded from view.

"Whether Canada has truly broken this cycle, or simply modernized the mechanics of a stockpile still vulnerable to the same underlying neglect, remains an open question, and one that will only be answered by how the federal government funds and prioritizes the NESS in the years after this crisis has fully faded from view."

Global Supply Chain Dependency

Canada's fourth resilience gap is its dependency on foreign-manufactured pharmaceuticals and medical countermeasures, tied to NATO's fifth baseline requirement since a stockpile is only as strong as the supply chain replenishing it. No NATO member has achieved true self-sufficiency here, but Canada has taken concrete steps to narrow its gap: its 2021 Biomanufacturing and Life Sciences Strategy funded a domestic vaccine facility in Montreal and a Moderna mRNA plant in Quebec producing up to 100 million doses annually,[26] while the Canadian Critical Drug Initiative in Edmonton is building a facility explicitly designed for rapid crisis production, capable of supplying the entire country within a 100-day sprint.[27] These investments mark a significant shift from Canada's historical reliance on imports, though it remains to be seen whether this capacity is sufficient to meaningfully offset the country's broader dependency on foreign pharmaceutical inputs.

> **"A stockpile is only as strong as the supply chain replenishing it."**

NATO Ally Case Studies

Finland

Despite only joining NATO in 2023, Finland serves as an exemplary case of what national resilience could look like. Its national resilience is characterized by the systems and structures it has in place – many of which could be adapted for the Canadian context to ameliorate challenges to national public health resilience. Finnish preparedness is centered around what it considers to be Comprehensive Security, which entails authorities, businesses, NGOs, and citizens being held jointly responsible for ensuring Finnish society's necessary services in the event of a crisis.[28] While the responsibility of Canadian national resilience has largely been placed on the Federal, Provincial and Territorial governments, Finland thrives by making it a collective mission involving diverse stakeholders. While the Finnish government is still responsible for coordinating all efforts in times of crisis, NGOs may support in doing so by providing services and organizing volunteers for emergency support, and their private sector is heavily involved in processes with business operating on critical infrastructure.[29] While Canada is already taking steps to induce Federal-Provincial-Territorial coordination, perhaps including other levels of Canadian civil society into preparedness conversations would be wise. Finland also excels in its preparedness for its strategic stockpiles, which served it well during the COVID-19 pandemic.[30] They do so primarily by leveraging their private sector and by legally mandating pharmaceutical companies to stockpile pharmaceutical products and substances. Further, Finland also encourages its civilian population to procure its own medical stockpiles as an additional level of security.[31] Civilians may also support during crises by being first aid trained and by volunteering in rescues; Finland's volunteer fire brigade serves as an example of how civilians can be enlisted to support during times of crisis. Finland's model of Comprehensive Security has constantly been adapted to their security needs with World War II,[32] hence Canada could learn a lot from their long-term preparedness in national resilience strategies.

> **"While the responsibility of Canadian national resilience has largely been placed on the Federal, Provincial and Territorial governments, Finland thrives by making it a collective mission involving diverse stakeholders."**

United Kingdom

While Finland provided lessons Canada could use to address its Jurisdictional Fragmentation Problem along with its NESS challenges, the United Kingdom provides an example of developing a public health resilience-specific regulator body to ensure preparedness with their UK Health Security Agency (UKHSA). The UKHSA's goals are to 1) prepare for and prevent health security hazards, 2) respond by saving lives and reducing harm in the event of health crises and 3) build the UK's health security capacity. Moreover, the UKHSA serves as a category 1 responder with well-defined statutory duties, which include risk assessment, business continuity management, emergency planning, maintaining public awareness and arrangements to warn, inform and advise the public, cooperation and information sharing.[33] Having a clear body to look to in the event of a crisis is a system that Canada lacks, and perhaps, in addition to having Federal-Provincial-Territorial collaboration, it would be beneficial to have a designated body like the UKHSA to guide governments in the event of public health crises. Even a well-designed statutory body, however, does not guarantee smooth coordination, and the UK's own experience proves this. The UK's COVID-19 Inquiry Module 2 report found that intergovernmental collaboration between London and the devolved governments of Scotland, Wales, and Northern Ireland "did not work as well as it should" during the pandemic response, despite the UKHSA's statutory mandate to lead exactly this kind of coordination.[34] This is a useful lesson for Canada: a designated coordinating body is a necessary structural fix, but it is not sufficient on its own to resolve the deeper political tensions between different levels of government, tensions Canada already knows well through Quebec's approach to public health autonomy. What the UK model does offer, though, is a mechanism for accountability once things go wrong; the Inquiry itself, and the UK government's subsequent March 2026 commitment to improve intergovernmental machinery in direct response to its findings, show what it looks like when a statutory body's failures are actually examined and addressed, rather than quietly absorbed into the next crisis.[35] Canada currently has no equivalent mechanism, statutory or otherwise, that could produce this kind of binding, public reckoning with its own Federal-Provincial-Territorial shortcomings. If Canada is to build a body like the UKHSA, it may be equally important to build the accountability structure that forces that body to actually learn from its failures, rather than assuming the existence of a coordinating agency is itself the solution to fragmentation.

"A designated coordinating body is a necessary structural fix, but it is not sufficient on its own to resolve the deeper political tensions between different levels of government."

> **"It may be equally important to build the accountability structure that forces that body to actually learn from its failures, rather than assuming the existence of a coordinating agency is itself the solution to fragmentation."**

Policy Recommendations

1. Building a Self-Sustaining Health Workforce Pipeline While Replenishing Canada's Current Healthcare Workforce Needs with Foreign-Trained Professionals

1.1 Close the physician deficit by continuing to reduce barriers for foreign-trained professionals while gradually building domestic training capacity

Closing Canada's physician deficit requires pursuing two policy actions simultaneously rather than treating them as alternatives. In the near term, Canada should continue reducing barriers for internationally trained professionals to join the domestic workforce, building on the Foreign Credential Recognition Action Fund and the new Express Entry category for physicians. In the longer term, however, Canada must gradually increase the supply of Canadian-trained doctors by opening new medical schools and adding residency seats, following the model already underway in Ontario, Alberta, and New Brunswick. These two approaches operate on different timescales and should not be mistaken for substitutes; credential recognition offers a comparatively fast but limited gain, since it draws from a finite pool of internationally trained professionals willing to relocate, while new domestic training capacity is slow and costly but addresses the deficit at its root, producing a workforce that regenerates on its own rather than depending on continued recruitment from abroad.

1.2 Address Barriers to Nursing Retention

The nursing shortage calls for a different solution entirely, since Canada's nurse-to-population ratio already exceeds the OECD average. What Canada lacks is not trained nurses, but the working conditions to retain them, meaning policy attention should shift toward retention rather than production. British Columbia's approach, which prioritizes making nursing a more attractive profession and addressing workplace conditions problems through retention bonuses, nurse-patient ratios and flexible shift options, offers a useful starting model worth adapting more broadly across provinces.

1.3 Incentivize basic first aid training among the general public

Beyond the professional workforce, Canada could also draw on Finland's

comprehensive security model by incentivizing basic first aid training among the general public, extending resilience beyond credentialed professionals to the population itself. A public capable of managing minor emergencies independently reduces strain on the professional workforce precisely when that workforce is most stretched during times of crisis.

1.4 Continue evaluating and eventually expanding the scope of workforce studies

Finally, Canada should continue evaluating tools such as the Study, and should aim to expand its scope beyond the five professions currently examined (nursing, occupational therapy, physiotherapy, pharmacy, and physicians), since a workforce strategy built on incomplete data cannot fully account for where Canada's true gaps lie.

2. Pan-Canada Coordination for national public health resilience

2.1 Continue building on the Pan-Canadian Health Workforce Data Strategy

Coordinated national planning is impossible without shared data, and Canada's March 2026 Pan-Canadian Health Workforce Data Strategy represents a powerful first step toward correcting this. Canada should continue investing in this strategy and extend its scope beyond workforce data alone to include surveillance and supply chain information, since a stockpile, a workforce, and a supply chain all depend on the same underlying coordination problem: without shared national data, provinces and the federal government cannot plan around the same picture of Canada's needs.

2.2 Adapt the UKHSA model for Canada

The United Kingdom's Health Security Agency offers Canada a template for what a dedicated, statutorily empowered coordinating body could look like. Canada currently lacks a single, clearly defined body that provinces and territories can look to during a public health crisis, relying instead on ad hoc federal-provincial agreements negotiated case by case. Adapting a UKHSA-style body, with statutory duties spanning risk assessment, emergency planning, and public communication, would give Canada a consistent point of coordination rather than reconstructing intergovernmental cooperation from scratch with each new crisis. The UK's own experience, however, is a caution rather than a guarantee: its Health Security Agency did not prevent real coordination failures between London and its devolved governments during COVID-19, suggesting that a coordinating body alone is necessary but not sufficient, and must be paired with political willingness to cooperate, which will require significant efforts made towards the second barrier to national public health resilience, which is Federal-Provincial-Territorial Jurisdictional Fragmentation.

2.3 Continue efforts to bring Quebec Aboard National Coordination Efforts

No pan-Canadian resilience strategy can succeed while its second-most populated

province opts out entirely, as Quebec did by declining to participate in the national workforce study discussed earlier. Rather than treating Quebec's position as unchangeable, Canada should pursue a coordination model that respects Quebec's constitutional right to administer its own health system while still securing its participation in shared data collection and emergency planning, potentially through asymmetric federalism arrangements similar to those already used in other policy areas. Perhaps, it may take longer to bring Quebec to the same level of agreement as other provinces, but that does not mean efforts to encourage their participation should cease. Without Quebec's cooperation, any national coordination framework Canada builds will remain incomplete by definition.

3. A Living Stockpile: Continuous Oversight and Continuous Growth

3.1 Ensure the NESS is stocked with Routine Supplies in addition to Niche, Low-Probability, High-Consequence Assets

The 2021 Office of the Auditor General audit found that NESS had historically prioritized investment in niche countermeasures for high-consequence, low-probability events, such as chemical or nuclear threats, on the assumption that routine supplies like PPE would remain readily available on the open market. That assumption dissipated the moment COVID-19 created global competition for the same limited stock. Canada's Comprehensive Management Plan should ensure this balance is corrected permanently, treating routine supplies as core to the stockpile's mandate rather than a secondary concern behind rarer, higher-profile threats.

3.2 Secure routine funding for NESS management at a consistent or increasing level of attention for years to come

The deeper failure exposed by the pandemic was not a lack of oversight, since audits had already identified the stockpile's underfunding before COVID-19 struck, but a lack of sustained political attention to acting on those findings once identified. Canada must ensure the NESS receives stable, non-lapsing funding, so that the stockpile is prepared for the next emergency at any point in time, rather than only in the years immediately following the last one.

3.3 Introduce private sector participation in NESS preparedness through a legal mandate

Finland requires pharmaceutical companies operating within its borders to maintain their own preparedness stockpiles by law, distributing the responsibility for national resilience beyond government alone. Canada could adopt a similar legal obligation for pharmaceutical manufacturers and medical supply companies operating domestically, reducing the NESS's sole reliance on federal stockpiling and building redundancy directly into the private supply chain.

3.4 Incentivize broader corporate involvement in NESS preparedness through tax write-offs for donated supplies and funding contributions

Once again, Finland's comprehensive security model treats national preparedness as a responsibility shared across all of society, not just government and the pharmaceutical sector specifically. This inspires the idea that Canada could extend this principle by offering tax incentives to medical supply companies that donate inventory directly to the NESS, and to other corporations that contribute funding toward its upkeep, turning private sector participation into a shared national project rather than a purely regulatory burden.

3.5 Encourage the civilian population to maintain their own personal stockpiles

Extending resilience further still, Canada could promote household-level emergency preparedness, encouraging citizens to maintain basic personal stockpiles of essential medical supplies as Finland does, with the caveat that Canada adapt this plan by enforcing strict guidelines for what supplies may be included within personal emergency preparedness stockpiles. For instance, Finland allows for antibiotics to be stockpiled by households; however, the overuse of antibiotics could result in antibiotic resistance, which would later result in further challenges for national public health resilience with a lack of effective medications. Done correctly, encouraging the civilian population to maintain their own personal stockpiles reduces the burden on the NESS during the earliest, most acute phase of a crisis, when government stockpiles are still mobilizing.

3.6 Extending the Stockpile's Shelf Life: Funding Pharmaceutical Longevity Research

One of the main impediments to the NESS upkeep remains ensuring that critical medicine remains viable (within shelf-life). This means that critical medicines within the NESS must be replenished periodically before they surpass their shelf-life. For instance, if a given medicine has a shelf-life of two years, Canada will need to ensure it's replenished within the NESS regardless of whether it was used or not, leading to another expense, which competes for the same limited funding allotted to NESS upkeep. Dedicating research funding specifically toward extending pharmaceutical shelf life, whether through improved formulation, packaging, or storage conditions, would directly reduce how frequently the stockpile needs replenishing, lowering both the recurring cost of maintaining it and the risk of expired-supply failures during times of crisis.

4. Reducing Medical Products Import Dependency

4.1 Continue supporting avenues for self-sufficiency in the production of medical supplies

Canada has already taken meaningful steps toward reducing its dependency on foreign-manufactured medical countermeasures, including a domestic Moderna mRNA vaccine facility in Quebec producing up to 100 million doses annually, and the Canadian Critical Drug Initiative's Edmonton facility, designed explicitly for rapid crisis production capable of supplying the entire country within a hundred-day sprint. Canada should continue expanding these investments, since no nation, including its largest NATO allies, has achieved absolute self-sufficiency in medical supply chains, and building targeted domestic capacity for a defined list of critical countermeasures remains the most realistic path forward, rather than attempting to replicate the entire global supply chain within Canada's borders.

Sabirshah513. "Medicine, Storage, Paramedic." Pixabay. May 1, 2024. https://pixabay.com/illustrations/medicine-storage-paramedic-8730630/ .

Endnotes:

1. Health Canada, "Caring for Canadians: Canada's Future Health Workforce – The Canadian Health Workforce Education, Training and Distribution Study" (Ottawa: Health Canada, January 30, 2025), https://www.canada.ca/en/health-canada/services/health-care-system/health-human-resources/workforce-education-training-distribution-study.html.
2. Health Canada, "Caring for Canadians."
3. Signal49 Research, "Retaining Canada's Healthcare Workforce," in partnership with Future Skills Centre, April 21, 2026, https://www.signal49.ca/in-fact/canada-healthcare-workforce-retention-migration_apr2026/.
4. Canadian Federation of Nurses Unions, "New Poll: Alarming Number of Nurses Are Looking for the Exit Sign, with Early-Career Nurses Leading the March," media release, March 23, 2023, https://nursesunions.ca/new-poll-alarming-number-of-nurses-are-looking-for-the-exit-sign/.
5. Emmanuelle B. Faubert, "Which Provinces Struggle the Most to Keep Young Nurses?," Economic Note (Montreal: Montreal Economic Institute, September 2024), https://www.iedm.org/which-provinces-struggle-the-most-to-keep-young-nurses/.
6. North Atlantic Treaty Organization, "Resilience, Civil Preparedness and Article 3," last updated November 13, 2024, https://www.nato.int/en/what-we-do/deterrence-and-defence/resilience-civil-preparedness-and-article-3.
7. C.D. Howe Institute, "Health Canada Workforce Shrinks While Other Federal Public Sectors Grow by Thousands," Graphic Intelligence, October 20, 2025, https://cdhowe.org/publication/health-canada-workforce-shrinks-while-other-federal-public-sectors-grow-by-thousands/.
8. Immigration, Refugees and Citizenship Canada, "Foreign Credential Recognition," briefing document prepared for the House of Commons Standing Committee on Citizenship and Immigration, November 18, 2025, https://www.canada.ca/en/immigration-refugees-citizenship/corporate/transparency/committees/cimm-nov-18-2025/foreign-credential-recognition.html.
9. Angelina Walker, "U.S. Nurses Are Moving Out of the Country Fast, Canada Says Its $500M Plan Is Working," nurse.org, April 1, 2026, https://nurse.org/news/canada-hire-usa-trained-nurses/.
10. Sophie Mitchell, "Ontario Moves to Prioritize Residency Spots for Homegrown International Medical Graduates," Wire Service Canada, April 18, 2026, https://www.wireservice.ca/ontario-moves-to-prioritize-residency-spots-for-homegrown-international-medical-graduates/.
11. Janet French, "Alberta to Add 120 Medical School Seats, 100 Medical Residency Spots in Three Years," CBC News, March 13, 2023, https://www.cbc.ca/news/canada/edmonton/alberta-to-add-120-medical-school-seats-100-medical-residency-spots-in-three-years-1.6777823.
12. Victoria Walton, "New Francophone Medical School Seats Being Added in New Brunswick," CBC News, October 3, 2025, https://www.cbc.ca/news/canada/new-brunswick/medical-seats-increase-francophone-u-de-m-1.7650888.

Endnotes:

13. British Columbia Ministry of Health, "Postgraduate Medical Education," last updated June 23, 2026, https://www2.gov.bc.ca/gov/content/health/practitioner-professional-resources/physician-compensation/postgraduate-medical-education.
14. Health Canada, "Caring for Canadians."
15. Christopher S. Cotton, Monica C. LaBarge, and Ardyn Nordstrom, "Canadian Public Health Experiences during COVID-19: A New Framework for Assessing Evidence," Frontiers in Public Health 13 (September 23, 2025): 1620514, https://doi.org/10.3389/fpubh.2025.1620514.
16. Health Workforce Canada, "Pan-Canadian Health Workforce Data Strategy" (March 2026), https://healthworkforce.ca/wp-content/uploads/2026/03/Pan-Can-Health-Workforce-Data-Strategy_EN_Mar-2026.pdf.
17. Immigration, Refugees and Citizenship Canada, "Foreign Credential Recognition."
18. Health Canada, "Working Together to Improve Health Care in Canada: Overview," last updated July 30, 2026, https://www.canada.ca/en/health-canada/corporate/transparency/health-agreements/shared-health-priorities.html.
19. North Atlantic Treaty Organization, "Resilience, Civil Preparedness and Article 3.
20. Scott Laing and Ellen Westervelt, "Canada's National Emergency Stockpile System: Time for a New Long-Term Strategy," CMAJ 192, no. 28 (July 13, 2020): E810–E811, https://doi.org/10.1503/cmaj.200946.
21. Public Health Agency of Canada, "The National Emergency Strategic Stockpile's Comprehensive Management Plan" (Ottawa: Health Canada, July 2024), https://www.canada.ca/en/public-health/services/emergency-preparedness-response/national-emergency-strategic-stockpile/comprehensive-management-plan.html.
22. Public Health Agency of Canada, "Comprehensive Management Plan."
23. Public Health Agency of Canada, "Comprehensive Management Plan."
24. Public Health Agency of Canada, "Comprehensive Management Plan."
25. Public Health Agency of Canada, "Comprehensive Management Plan."
26. Innovation, Science and Economic Development Canada, "Overview: Canada's Biomanufacturing and Life Sciences Strategy," last updated July 30, 2026, https://ised-isde.canada.ca/site/ised/en/programs-and-initiatives/health-emergency-readiness-canada/overview-canadas-biomanufacturing-and-life-sciences-strategy.
27. Applied Pharmaceutical Innovation, "Building Canada's Largest Biomanufacturing Facility: The CMPC and CCDI Impact," June 12, 2025, https://appliedpharma.ca/news/building-canadas-largest-biomanufacturing-facility-the-cmpc-and-ccdi-impact/.
28. Security Committee (Finland), "Concept of Comprehensive Security – Building National Resilience in Finland," https://turvallisuuskomitea.fi/concept-of-comprehensive-security-building-national-resilience-in-finland/.
29. Security Committee (Finland), "Concept of Comprehensive Security."

Endnotes:

30. Robin Forsberg, Aku-M. Kähkönen, and Jason C. Moyer, "Finland's Contributions to NATO: Strengthening the Alliance's Nordic and Arctic Fronts," Wilson Center, November 8, 2022, https://www.wilsoncenter.org/article/finlands-contributions-nato-strengthening-alliances-nordic-and-arctic-fronts.
31. Lauri Jauhiainen and Sarah Schiffling, "Comparing the Resilience Objectives of Finnish Comprehensive Security Model and the NATO Baseline Requirements for Resilience," Journal of Military Studies (2025), https://doi.org/10.2478/jms-2025-0003.
32. Security Committee (Finland), "Concept of Comprehensive Security."
33. UK Health Security Agency, "Emergency Preparedness, Resilience and Response: Concept of Operations," GOV.UK, updated January 15, 2025, https://www.gov.uk/government/publications/emergency-preparedness-resilience-and-response-concept-of-operations/emergency-preparedness-resilience-and-response-concept-of-operations.
34. HM Government, UK Government Response to the Covid-19 Inquiry Module 2 Report, CP 1534 (London: HM Government, March 25, 2026), https://assets.publishing.service.gov.uk/media/69c3d6bd4a06660f08544159/UK_Government_Response_to_the_Covid-19_Inquiry_Module_2_Report.pdf.
35. HM Government, UK Government Response to the Covid-19 Inquiry Module 2 Report.

Author: Maya Khachab, Junior Research Fellow

Chapter 5. Environmental and Natural Disaster Preparedness and Response

Executive Summary

Canada's environmental vulnerability is outpacing its institutional response. Climate-driven wildfires, floods and severe storms are placing sustained pressure on Operation LENTUS, the Canadian Armed Forces' (CAF) domestic disaster-response mechanism, even though it was not designed to provide routine civilian emergency capacity. At the same time, critical infrastructure is deteriorating under climate stress, large data centres are adding pressure to electricity and water systems, and major Arctic defence investments face accelerating permafrost thaw. This chapter argues that Canada's central environmental and natural disaster preparedness and response challenge is institutional, not simply a shortage of military capacity.

This chapter uses NATO's seven baseline requirements for resilience to connect the environment with public safety, infrastructure continuity and national defence.

Main Policy Recommendations

- **Establish a National Adaptation Office**, headed by an officer reporting directly to the Prime Minister, to coordinate adaptation priorities and monitor implementation.
- **Establish a federal Civilian Climate Emergency Corps** to provide trained personnel and logistics under agreed deployment arrangements. Retain Canadian Armed Forces (CAF) support for emergencies requiring military capabilities.
- **Create a dedicated resilience fund or protected funding stream for high-risk public infrastructure.**
- **Align digital growth with essential services**. Assess data centres against regional electricity, water and emergency needs. Clarify data-access, security and recovery obligations through legislation and procurement, and pilot a national data trust for selected disaster and infrastructure information, with privacy and Indigenous data-governance safeguards.
- **Strengthen Arctic resilience** through partnership. Apply lifecycle climate requirements to civilian and defence infrastructure, give Indigenous partners meaningful governance roles, and coordinate northern procurement, shipping and workforce development.

Introduction

Canada's Changing Climate Report found that Canada had warmed at about twice the global rate, while a later study found that the Arctic warmed nearly four times faster than the globe between 1979 and 2021.[1]

The consequences span a wide range of intensifying hazards, including flooding, drought, wildfire, hail, wind, snow load, permafrost loss, sea-level rise, and extreme heat. Wildfire can disrupt transportation, telecommunications and electricity; flooding can isolate communities; and thawing permafrost can undermine buildings, roads, runways and fuel infrastructure. Climate resilience is therefore a condition of public safety, economic security and national defence that must be planned for across decades, not just current seasons.

In 2025, over 6,000 wildfires burned approximately 8.3 million hectares across Canada. It was the second-worst season on record and forced over 85,000 people to evacuate.[2]

Provinces and territories submitted 17 Requests for Federal Assistance in 2025 alone. By 18 August 2026, 4,793 fires had burned 4.1 million hectares, with 582 still active. Although interim, the 2026 figures show that high operational demand has persisted after the record-setting 2023 season and severe 2025 season.[3]

Emergency management in Canada involves municipal, Indigenous, provincial, territorial and federal authorities. Passed in 2007, the Emergency Management Act[4] assigns federal coordination responsibilities to the responsible minister and requires a provincial request or an agreement permitting assistance before federal institutions respond to a provincial emergency. Effective preparedness therefore requires established assistance arrangements and sufficient capacity at each level.

NATO's seven baseline requirements cover continuity of government, energy, population movement, food and water, mass casualties and disruptive health crises, civil communications, and transport[5] They provide an organizing framework for examining how civilian systems support both public safety and defence. This chapter applies that framework qualitatively; it does not claim to conduct a formal NATO compliance assessment.

The central institutional gap is reliable civilian reinforcement when local and regional resources are insufficient. Canada already has federal coordination mechanisms and funded humanitarian partners; the concern is whether these arrangements consistently provide trained personnel, logistics and common operating procedures at the scale required. A federal civilian corps could strengthen this capacity while respecting local authority and preserving the CAF for tasks that require military capabilities.

The chapter first examines civilian disaster response, drawing on provincial and international experience to assess institutional options and recommend federal reforms. It then considers infrastructure resilience, future climate design, private finance and data-centre planning. The final substantive section applies these recommendations to the Arctic, where climate hazards, logistical constraints,

Indigenous governance and national sovereignty converge.

Civilian Disaster Response

Operation LENTUS is the Canadian Armed Forces' (CAF) operation for assisting civilian authorities during natural disasters.[6] A 2024 parliamentary report recorded approximately 50 activations between 2010 and 2023 and described deployments as having broadly doubled every five years over that period. This historical trend illustrates the pressure on military personnel, equipment and training[7].

Most climate emergencies require sustained logistics, communications, shelter, engineering and coordination with utilities and local governments. These functions depend more on continuity and community relationships than on combat capability. A standing civilian institution can retain those skills, exercise with local authorities and remain through recovery. The CAF would still provide exceptional lift, engineering, and command capacity, but would no longer be the default provider of functions that trained civilians can deliver, subject to demonstrated readiness and cost-effectiveness.

Christian Leuprecht, a professor at the Royal Military College of Canada and editor of the *Canadian Military Journal*, identifies an incentive problem: provinces may seek federal military assistance before exhausting local capacity because it offers a readily available response at limited direct provincial cost. His concern is that repeated reliance can weaken incentives to maintain civilian capacity.[8] Precautionary requests can still be appropriate when forecasts indicate serious danger. Reform should enable early assistance while clarifying responsibilities and readiness expectations.

General Wayne Eyre also warned parliamentarians that repeated domestic deployments reduced readiness and were not economically sustainable. The defence committee recommended that the government consider investing in a professional, permanent disaster-management workforce, such as a resilience corps.[9] Civilian reinforcement should be available before conditions become catastrophic, with military support requested whenever urgency, scale or specialized requirements justify it.

Existing investments provide a foundation for reform. The Humanitarian Workforce Program supports non-governmental surge capacity.[10] In May 2026, the government described a $316.7-million, five-year investment through Budget 2025 that enabled the Canadian Interagency Forest Fire Centre (CIFFC) to lease ten firefighting aircraft and two support assets. [11]A civilian corps should integrate its planning with these capabilities, rather than duplicate their specialist coordination.

Fragmented delivery can make it difficult to establish whether funded personnel, equipment and contracts will be available together during simultaneous emergencies. A national readiness framework should identify gaps in regional coverage, credentials, deployment agreements and communications. Its purpose would be to measure usable capacity rather than assume that spending totals demonstrate preparedness.

The government's response to the defence committee recognized the importance of a predictable civilian workforce[12]. A corps would add operational capacity to existing

federal coordination. Its legislation and operating agreements should specify how it works with Public Safety Canada's Government Operations Centre, humanitarian partners and CIFFC, avoiding competing chains of command.

The same fragmentation affects First Nations communities. In 2022, the Auditor General found that Indigenous Services Canada emphasized response and recovery over preparedness and mitigation[13]. Reimbursement after an evacuation is not community-controlled preparedness. A federal corps should therefore establish agreements with First Nations emergency authorities, provide direct training and equipment, and fund local responders rather than treat Indigenous governments only as aid recipients.

Provincial Approaches

Four provinces provide distinct models of civilian emergency capacity, demonstrating what Canada can transfer federally while preserving local authority.

Ontario: Networked Mobilization

Ontario Corps is a networked model that coordinates public servants, skilled volunteers and established organizations while funding equipment, training and deployment. It can expand quickly by mobilizing expertise already present in civil society. [14]

Federally, a professional core could provide planning, logistics and command while an accredited network supplies scalable personnel. Common training and standing contracts could improve availability without requiring Ottawa to employ every specialist permanently.

This matters because Ottawa already funds many such organizations without integrating them. Ontario shows how dispersed capacity can become deployable, but also that registration is not readiness: federal participation must require exercises, equipment standards, availability commitments and worker protections.

Nova Scotia: Clear Administrative Ownership

The Nova Scotia Guard model places skilled and general volunteers within a dedicated Department of Emergency Management. The province's founding announcement assigned the department responsibility for coordinating preparedness, response and recovery, providing a clear administrative home for the volunteer corps (Nova Scotia 2024)[15].

Fragmented ownership makes it difficult to determine whether failures reflect inadequate funding, training, equipment, or coordination. Nova Scotia shows that a visible workforce requires a visible institution; federally, one headquarters must answer for deployment readiness.

Quebec: A Specialist Reserve

Quebec's Réserve d'intervention d'urgence en sécurité civile (RIUSC) is a specialist reserve built largely through established search-and-rescue, firefighting and humanitarian organizations. Its activation rules are as important as its composition: municipalities first use local resources, regional coordination and mutual-aid arrangements before requesting the reserve (Quebec, Ministère de la Sécurité publique 2025)[16].

Quebec's model reinforces municipal responsibility while providing additional trained personnel when local resources are insufficient. Canada could adopt clear activation and cost-sharing rules while allowing early planning and pre-positioning when serious hazards are forecast. The objective should be timely assistance, not a requirement to wait for local systems to fail.

British Columbia: Local and First Nations Preparedness

British Columbia offers a complementary example of investment in local and First Nations preparedness through community resilience funding through their Ministry of Emergency Management and Climate Readiness 2026.[17]. Its relevance here is support for emergency planning and mitigation rather than a direct equivalent to a standing response corps.

This matters because outside responders cannot compensate for absent evacuation plans, communications or local leadership. British Columbia shows that effective federal response begins before deployment and should strengthen community institutions rather than create dependence on federal arrival.

Lessons for Federal Design

Collectively, these models offer complementary institutional elements: Ontario's networked capacity, Nova Scotia's administrative accountability, Quebec's tiered specialist reserve, and British Columbia's investment in local and First Nations preparedness. Although no province provides a complete federal template, these elements could be integrated through common credential recognition, interoperable communications, joint exercises, national logistics, and mutual aid agreements established in advance. Provincial, territorial, municipal, and Indigenous authorities would retain their jurisdiction and agreed incident-management responsibilities.

An emergency management organization (EMO) coordinates preparedness and response within a jurisdiction; it is not necessarily a deployable workforce. Ground search and rescue (GSAR) organizations provide specialist capabilities but do not replace a comprehensive disaster service. The absence of a named corps should therefore not be treated as evidence that a province or territory has no civilian capacity.

NATO Ally Case Studies

These NATO member states offer different elements that could inform a Canadian civilian emergency-response system. Canada does not need to reproduce any model in full; it can instead draw on the institutional features most compatible with its federal structure, domestic needs and civil-military relationships.

Germany

Germany's Federal Agency for Technical Relief, the Technisches Hilfswerk (THW), provides the most transferable workforce structure. A small professional administration supplies doctrine, equipment, training and command to locally based technical volunteers, turning public participation into verified operational units. [18]

Canada could draw on this professional-core-and-reserve structure when designing a civilian corps. Provincial, territorial and Indigenous agreements could support locally based units, while federal training, equipment and readiness standards would allow them to operate together. A similar structure would provide national scale without requiring Ottawa to employ every responder permanently.

United States

The Federal Emergency Management Agency (FEMA) is a relevant federal comparator, although it is primarily a coordinating agency rather than a single operational corps.[19] Its responsibilities extend across mitigation, preparedness, response and recovery. FEMA supports state, local, Tribal and territorial authorities through funding, training, logistical coordination and deployable personnel, including on-call reservists organized into specialized cadres.

Public warnings are another part of preparedness. FEMA's Integrated Public Alert and Warning System represents a great international comparator.[20] Canada's Alert Ready system already distributes urgent messages through television, radio and compatible wireless devices.[21]

FEMA offers Canada a useful example of how permanent federal coordination can be combined with scalable personnel and subnational delivery. Canada would benefit from developing comparable federal capacity while ensuring national funding and personnel reinforce rather than replace provincial, municipal, and Indigenous responders. FEMA also demonstrates the importance of treating mitigation and recovery as part of the same institutional system as emergency response.[22]

Governments should pair warnings with regular testing, accessible instructions, multilingual communication where needed and alternatives for places with unreliable connectivity. Warning people is effective only when they can understand the message and act on it.

Sweden

The Swedish Civil Defence and Resilience Agency coordinates a whole-of-society "total defence" model in which civilian and military systems support one another while civilian authorities remain responsible for essential services. [23]

Sweden provides lessons for clarifying Canada's civil-military division of responsibilities. More regular planning and exercises among governments, businesses, civil society and the CAF would help civilian institutions remain operational during crises while preserving military assistance for emergencies that exceed civilian capabilities.

Finland

Finland's comprehensive-security model assigns continuing preparedness responsibilities to public authorities, businesses, organizations and citizens. Its strength is that relationships and duties exist during normal conditions rather than being assembled after an emergency declaration. [24]

Canada could apply this approach through standing continuity agreements with utilities, telecommunications providers, transport operators and humanitarian organizations. Operators should establish emergency responsibilities before a crisis, including contact points, backup arrangements, information sharing and participation in exercises.

Norway

Norway's 2025 white paper on total preparedness connects national defence with defined responsibilities for municipalities, civil society and the business sector. Its dispersed northern communities, harsh conditions and long supply lines make its experience particularly relevant to Canada.[25]

Canada could learn from Norway's combination of national standards and locally grounded delivery, particularly in northern and remote regions. Federal institutions can provide resources and consistency, while local and Indigenous authorities bring geographic knowledge, trusted relationships, and operational experience that centralized systems may lack.

Lessons for Canada

Taken together, Canada could learn from Germany's workforce structure, FEMA's federal coordination and mitigation role, Sweden's civil-military planning, Finland's continuing preparedness duties and Norway's locally grounded delivery. Combining these elements would produce a system tailored to Canadian institutions rather than a direct copy of any single foreign model.

Institutional Options and Adaptation Leadership

The Green Helmets Initiative and Its Potential Contribution

Dr. Rémy-Claude Beaulieu, Author of *The Green Helmets Initiative (GHI): The International Dimensions*, proposes a more organized role for disaster assistance in Canada and internationally. [26] Drawing on the symbolism of the United Nations' Blue Helmets, it envisages specialized personnel responding to natural disasters. Its national component considers a civil-defence role for the Canadian Armed Forces, while its international component proposes a division potentially situated within the United Nations. Beaulieu identifies requirements such as humanitarian expertise, early planning, transport, water purification and equipment for floods and other emergencies (Beaulieu 2024, 1–2).

The proposal makes a useful contribution by treating disaster assistance as a capability that must be organized and prepared in advance. A coordinated international mechanism could pool specialist expertise and equipment, help countries whose resources are overwhelmed and support cooperation across borders. For Canada, it could provide a framework for contributing disaster-response skills abroad and drawing on external assistance during major emergencies. These potential benefits warrant further development and evaluation.

Canada's existing cooperation illustrates the value of international reinforcement. Through the Canadian Interagency Forest Fire Centre (CIFFC) and international arrangements, Canada shares firefighting personnel and resources with other countries. The August 2026 federal update reported assistance from firefighters from Mexico, Costa Rica, New Zealand and Australia.[27] A Green Helmets mechanism could build on this experience by examining how comparable arrangements might support a wider range of disasters.

Translating the concept into dependable capacity would require further institutional design. Beaulieu also identifies unresolved questions about the division's position within the UN, financing and the mobilization of trained, properly equipped contingents (Beaulieu 2024, 1, 4). For Canada, an implementation assessment should also clarify deployment authority, coordination with provincial and Indigenous responders, and the balance between domestic and overseas commitments. It should examine how the initiative would complement existing international assistance, including the Disaster Assistance Response Team.[28] Its cost effectiveness would need to be demonstrated through a cost model and operational exercises.

The remaining domestic challenge is to provide continuing civilian capacity for preparedness, response and recovery across Canadian jurisdictions. Expanding the CAF's disaster role would still leave these functions dependent on military availability unless accompanied by investment in civilian institutions. A federal civilian corps could

address that need while supporting future international cooperation. **Developing domestic capacity and exploring the Green Helmets Initiative can therefore be complementary: further work should establish how their personnel, mandates and resources could reinforce one another.**

The Case for Civilian Capacity

The principal justification for a civilian corps is not that civilians can perform every task assigned to the CAF. **Distributing preparedness across civilian institutions would strengthen national resilience, sustain essential services, and reduce routine dependence on the CAF.**

Second, a civilian institution would better suit Canada's federal structure and support community legitimacy. Pre-negotiated agreements could recognize provincial authority, municipal emergency plans and Indigenous jurisdiction. Personnel could establish relationships with utilities, health authorities and non-governmental organizations and remain during recovery, when military deployments typically conclude. Effective response depends on both rapid deployment and continuity of essential services.

The principal risks are bureaucratic duplication and the displacement of local capacity. The corps should therefore remain limited in scope, comprising a small professional core and an accredited reserve activated through pre-negotiated agreements or federal authority. It should supplement rather than replace firefighters, paramedics, provincial emergency organizations or Indigenous responders.

Gaps in Adaptation Coordination

Canada's 2023 National Adaptation Strategy establishes a shared framework across disaster resilience, health, nature, infrastructure, and the economy.[29] Its effectiveness depends on departments and other orders of government translating that framework into funded actions and measurable results.

These concerns reveal two distinct institutional needs. **Disaster response requires trained personnel and reliable deployment arrangements, while adaptation requires sustained coordination of prevention and investment across portfolios.** Strengthening operational capacity alone would leave the wider implementation problem unresolved.

Recommendations for Civilian Preparedness

Establish a Civilian Climate Emergency Corps

Parliament should establish a federal Civilian Climate Emergency Corps with responsibility for deployable technical teams, disaster logistics, common training standards and a trained reserve. Its mandate should cover environmental and natural disasters, including events that are not attributable to climate change. A professional core should coordinate contracted and reserve capacity, with paid training and

deployment arrangements that make participation dependable. This develops the civilian-workforce option considered by the defence committee.[31]

Public Safety Canada should lead a two-year establishment phase to appoint an operational head, map existing capabilities, negotiate deployment agreements and conduct regional exercises. Initial functions should include logistics, emergency telecommunications, engineering support and incident management. Agreements must define activation thresholds, cost-sharing, credentials, worker protection, liability and command relationships. Aerial assistance should be coordinated with CIFFC rather than transferred automatically to the corps.

The establishment phase should produce a costed implementation plan and independently assessed readiness targets, not a promise of full national coverage within two years. Expansion should depend on exercises, staffing and agreements demonstrating that units can deploy reliably. Parliament should receive annual measures of personnel availability, activation times, regional gaps, service continuity and tasks completed without CAF assistance.

Create a National Adaptation Office

The federal government should establish a National Adaptation Office, with a National Adaptation Officer reporting directly to the Prime Minister. Its mandate should be to coordinate priorities, maintain an implementation plan and report progress under the existing National Adaptation Strategy. Public Safety Canada should retain responsibility for federal emergency coordination, while the corps would deliver operational support.

The office should work with Public Safety Canada; Housing, Infrastructure and Communities Canada; Environment and Climate Change Canada; the Standards Council of Canada; the National Research Council; and National Defence, including the CAF. Its mandate should provide access to implementation information and a process for resolving gaps between federal portfolios. Reporting to the Prime Minister would not itself confer authority over ministers or other governments. Standing arrangements with provincial, territorial and Indigenous governments should establish shared objectives while respecting their responsibilities.

Within its first year, the office should publish a prioritized action plan identifying accountable departments, delivery dates and measures of risk reduction. Annual public reporting should identify delays and corrective action, with unresolved federal issues referred to Cabinet. A review after three years should assess whether the office improves implementation or duplicates existing machinery.

Effective environmental and natural disaster preparedness requires more than deployable personnel. A civilian corps would still manage preventable emergencies if the infrastructure supporting essential services remained vulnerable to climate hazards.

Climate-Resilient Infrastructure

The infrastructure challenge is converting known climate risks into funded work. In May 2026, the Commissioner of the Environment and Sustainable Development found that only 3 per cent of federal critical assets identified as facing significant climate risks had resilience plans in 2024-25. Earlier commitments had been replaced with objectives extending to 2035 and beyond, without interim targets. The three audited departments managed 67 per cent of federal physical asset value.[32]These findings support time-bound implementation and reporting, rather than repeated assessment without action.

The Canadian Climate Institute's corrected 2026 analysis estimates that proactive adaptation would require about $4.1 billion annually and generate annual savings of $4.1 billion to $8.6 billion in infrastructure maintenance and replacement costs.[33] The modelling addresses rising heat and extreme rainfall for selected public infrastructure, not every climate hazard. Municipalities own and operate more than 60 per cent of public infrastructure and would bear 72 per cent of the modelled adaptation investment costs. Federal support is therefore needed where local fiscal capacity is insufficient.

Infrastructure planning should account for projected conditions over the next 25, 50 and 75 years, with the planning horizon matched to each asset's service life. Feltmate's call for flood maps that anticipate conditions 25 or 50 years ahead illustrates the importance of forward-looking information for development decisions. [34]Assessments should test a range of plausible climate scenarios and specify when projections and design assumptions must be updated. Historical observations remain useful, but they should be combined with forward-looking assessments to guide decisions about long-lived assets.

Resilience should be assessed at the design stage, when project teams can compare alternative sites, materials and engineering requirements before construction. The case for proactive adaptation is supported by the Canadian Climate Institute's modelling, although the scale of savings depends on the hazard, asset and investment period.[35] Procurement should compare lifecycle costs, avoided disruption and maintenance needs instead of assuming a uniform cost or financial return for every resilience measure.

Federal infrastructure programs should provide practical training for builders, developers, project-finance officers, insurers and pension funds on assessing physical climate risks. Training should connect financing decisions to engineering requirements, operating plans and the essential services on which an asset depends. This would help those funding and delivering infrastructure evaluate whether resilience measures are adequate over the asset's service life.

Data Centres and Essential Services

Critical infrastructure is interdependent. Electricity supports telecommunications, health care, water treatment and fuel distribution, while transportation networks sustain evacuation and resupply. Failure in one system can therefore disrupt several essential services. Federal resilience planning should assess these systems collectively and test

their ability to operate during simultaneous disruptions.

In early 2026, the federal government invited proposals for sovereign artificial intelligence (AI) data centres with planned capacities above 100 megawatts; that call has closed.[36]

Ontario's Independent Electricity System Operator projects that data centres could account for 8.6 per cent of provincial electricity demand in 2050 under its reference scenario. These are planning assumptions, not guaranteed outcomes. Approval decisions should assess each project's energy, cooling-water and land requirements against regional constraints and emergency needs.[37]

The central policy question is how governments allocate the costs and risks created by large new loads. Approval processes should determine whether developers or ratepayers finance required infrastructure, assess performance during peak demand, drought and wildfire, and disclose expected electricity use, water consumption and public subsidies.

The relevant resilience test is whether data centres can maintain reliable services without undermining essential electricity and water supplies. Physical capacity should be considered alongside data governance: who controls access, where backups are held and how public institutions recover information after disruption.

Recommendations for Infrastructure Resilience

Fund Infrastructure Adaptation

The federal government should establish a dedicated National Infrastructure Resilience Fund, or an equivalent protected funding stream within existing programs, for high-consequence municipal and Indigenous projects. Before creating another administrative structure, it should map the eligibility, remaining capacity and coverage of existing infrastructure and disaster-mitigation programs, including funding for natural infrastructure and housing-related water systems. This assessment should identify which high-risk assets remain unsupported and whether a protected funding stream could address those gaps. Awards should prioritize demonstrable risk reduction, service continuity and communities with limited fiscal capacity.

Funding should follow credible implementation plans and include the technical support needed to prepare them. This reduces the risk that application requirements exclude communities with the fewest planning resources. Reporting should distinguish completed adaptation measures from assessments and announcements.

Require Future Climate Design and Informed Financing

Federal procurement and infrastructure funding should require climate-risk

assessments over each asset's service life, using suitable 25-, 50- or 75-year horizons and longer periods where necessary. Engineering requirements should use current projections, document uncertainty and specify when reassessment is needed. Governments should work with standards bodies and provincial and territorial authorities to incorporate these requirements into applicable codes and approval processes.

Federal support for privately financed critical infrastructure, including loan guarantees, tax incentives and procurement contracts, should be conditional on independent resilience assessments, maintenance funding and continuity plans. Training for developers, lenders, pension funds and insurers should explain how to evaluate physical risks and service dependencies. Financing contracts should identify who pays for adaptation and how performance will be monitored. Private capital should supplement public investment without making essential community projects dependent on commercial returns.

Integrate Data-Centre Growth into Regional Planning

Federal incentives and provincial approvals for large data centres should be conditional on independent electricity, water, land-use and climate-resilience assessments. Utilities should identify the generation, transmission and backup requirements of approved projects and disclose how those requirements affect reliability, ratepayers and emergency operations.

Implementation requires cooperation among federal industry and environment departments, provincial utility regulators, municipalities and Indigenous governments. A common assessment template would permit regional comparison without imposing a single national capacity limit. Approval conditions should be enforceable through connection agreements, permits and funding contracts rather than expressed only as voluntary sustainability commitments.

This approach is preferable to either unrestricted development or a single national capacity cap. It tests each project against regional constraints, allows governments to support strategically valuable facilities and prevents private loads from silently displacing public resilience priorities.

Strengthen Data Governance

A national data trust could be piloted as a governed mechanism for sharing selected disaster-risk and infrastructure information. It should begin with a defined use case, such as authorized access to hazard maps and service-dependency data, rather than a centralized collection of all institutional information. Privacy safeguards, Indigenous data governance, security testing and an independent evaluation should precede expansion. These measures would connect digital sovereignty to practical disaster preparedness.

The same requirements apply with particular urgency in the Arctic, where climate hazards, limited construction capacity and national-security objectives converge.

Arctic Preparedness and Resilience

The Arctic connects environmental preparedness directly to sovereignty. In March 2026, Prime Minister Mark Carney announced investing $32 billion at Forward Operating Locations in Yellowknife, Inuvik, and Iqaluit, and at Deployed Operating Base 5 Wing Goose Bay and two new Northern Operational Support Hubs (NOSHs) at Whitehorse and Resolute, and two new Northern Operational Support Nodes (NOSNs) at Cambridge Bay and Rankin Inlet, backed by an investment of $2.67 billion.[38] These upgrades to northern defence infrastructure will build both military power and economic strength as well as improve surveillance, logistics and presence.

These investments will enable the CAF to defend the Arctic without depending on the help of Allies, allowing Canada to take more control of arctic security. This includes infrastructure upgrades such as airfield upgrades; new or repurposed hangars; ammunition and fuel facilities; and buildings and equipment for accommodations, warehousing, IT, and general support. Their strategic value, however, depends on roads, runways, buildings, fuel systems, telecommunications and community services that remain functional in a warming climate.[39]

Moreover, thawing permafrost can destabilise the ground supporting buildings, roads, runways and pipelines. A circumpolar study estimated that, by mid-century, nearly 70 per cent of infrastructure in permafrost regions across the Arctic could be exposed to thawing near the ground surface (Hjort et al. 2018). Infrastructure planning must therefore incorporate site-specific ground assessments, ongoing monitoring and maintenance strategies.[40]

Climate-resilient design should be mandatory at the beginning of a project, when site selection and engineering choices can still change. Standards should account for ground temperature, drainage, erosion, wildfire and supply-chain disruption; require long-term monitoring; and establish who pays for adaptation when conditions change. Applying these requirements after construction is both more expensive and less effective.

Inuit Partnership and Dual-Use Infrastructure

Resilient infrastructure depends on both sound engineering and effective partnerships with the communities it serves. Northern communities often depend on the same airport, power plant, telecommunications link and fuel storage system that support federal operations. A project that serves military needs but leaves community systems fragile cannot create durable sovereignty. Conversely, reliable housing, transportation, communications, health services and energy strengthen both community safety and Canada's ability to operate in the region.

Inuit Tapiriit Kanatami (ITK), the national representative organisation for Inuit in Canada, connects Canadian sovereignty with the security and well-being of Inuit

communities in its 2025 position paper.[41] This perspective reinforces the need to involve Indigenous leaders from the earliest stages of infrastructure planning, before project priorities and locations are determined.

Governance agreements should establish Inuit roles in project selection, environmental monitoring, data governance and the distribution of benefits. Partnerships with northern First Nations and Métis should similarly reflect their distinct rights and governance structures. Indigenous knowledge should inform project decisions with the consent of knowledge holders and clear agreements governing its use and disclosure. These arrangements can help ensure that infrastructure investments advance Arctic security while addressing the priorities of the people who live there.

Canada has created a $1-billion Arctic Infrastructure Fund for dual-use transportation projects.[42]

To achieve its security purpose, the fund and related defence spending should be governed by common climate-resilience standards and transparent community-benefit criteria. Federal departments should also coordinate procurement and construction schedules so that scarce labour, shipping capacity and materials are not bid against one another or diverted from urgent community needs.

Northern Delivery and Canada-Nordic Cooperation

Short construction and shipping seasons make coordination central to northern delivery. Federal departments should maintain a shared, multi-year schedule of defence, transport, housing, energy and communications projects, developed with territorial and Indigenous partners. Coordinated procurement, shipping and site assessments could reduce competition for scarce capacity. Longer contracts, local training and funded maintenance would help retain technical skills within communities.

Canada should establish a civilian-resilience exchange with Norway, Sweden, Finland and Iceland, building on existing cooperation. Topics should reflect each partner's expertise, including remote communications, evacuation, backup energy, cold-region engineering and volunteer training. Permafrost research could involve Nordic and other Arctic specialists where relevant. Municipal, Indigenous, infrastructure and emergency-management representatives should shape exercises and evaluate which practices suit Canadian conditions.

Co-Govern Infrastructure for a Thawing Climate

The federal government should make lifecycle climate requirements binding through the funding and procurement conditions for defence and dual-use Arctic projects. These requirements should cover siting, construction, monitoring and maintenance. Agreements with Inuit and other northern Indigenous partners should establish meaningful governance roles appropriate to their rights and territories, including how Indigenous knowledge influences decisions.

Parliament should direct National Defence, Transport Canada, Housing, Infrastructure and Communities Canada, and Natural Resources Canada to develop a common northern climate-risk protocol with territorial and Indigenous partners. Legislation should formalize these planning duties where necessary, supported by implementation funding. Regional governance bodies should review monitoring plans and receive results, while project budgets should provide for long-term operations and maintenance.

Preparedness communication should explain persistent climate risks in accessible terms for northern and southern audiences, while making clear that emissions reductions still limit future harm. Feltmate has also emphasized practical education on protecting homes from floods and wildfires.[43] Public information should translate local projections into actions for housing, travel, evacuation and essential services. Guidance should be developed with local partners, use relevant languages and distinguish well-established risks from uncertainties that require monitoring.

This recommendation protects the value of major defence investments while recognizing that sovereignty depends on functioning communities and infrastructure. It advances NATO's requirement for resilient energy, transportation and communications and gives practical effect to the principle that northern security must be built with the people who live there.

Conclusion

Canada's environmental and natural disaster preparedness and response requires institutions that connect prevention, deployable civilian capacity and continuity of essential services. Existing military, humanitarian and infrastructure programs provide a foundation, but their effectiveness depends on clear responsibilities and demonstrated readiness.

A National Adaptation Office would coordinate priorities and track delivery across government. A Civilian Climate Emergency Corps would provide operational reinforcement under established agreements. Distinguishing these roles is essential: strategic oversight cannot substitute for trained responders, and a response workforce cannot compensate for continued underinvestment in prevention.

Operators should establish continuity and emergency responsibilities before a crisis rather than relying on ad hoc cooperation after one begins.

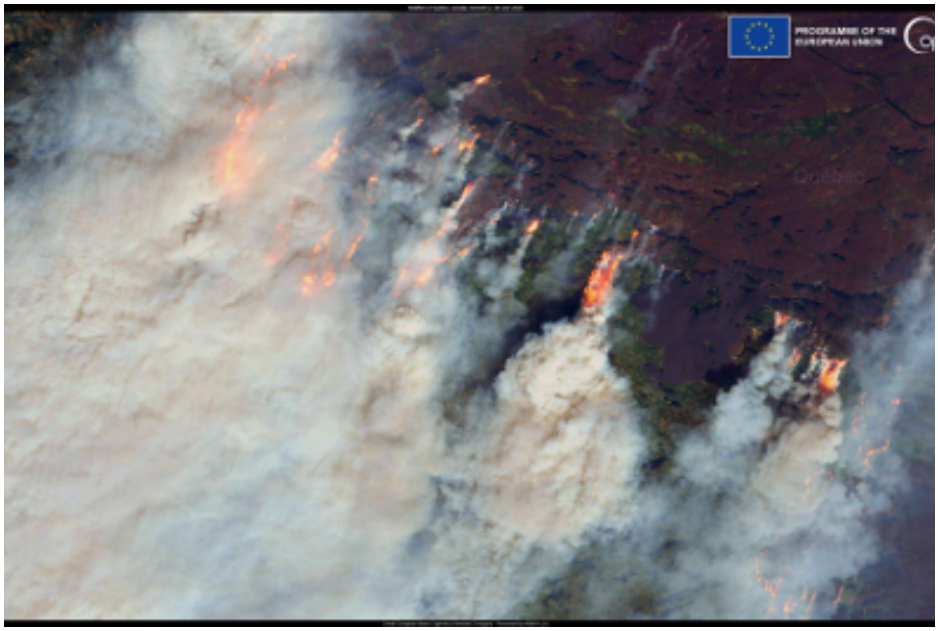
Infrastructure reform should combine future climate design, implementation funding and informed private investment. Data-centre approvals should account for regional resource constraints and public-service continuity. Northern projects should apply these principles through Indigenous partnership, coordinated delivery and long-term maintenance.

Mitigation means reducing greenhouse gas emissions or disaster risks; adaptation means adjusting systems to actual or expected climate conditions. Surge capacity is additional trained personnel and resources available when normal services are

stretched. These distinctions matter because preventing harm, preparing for unavoidable impacts and responding to emergencies require related but different policies.

Success should be measured through faster assistance, reliable cross-jurisdictional deployment, fewer avoidable service disruptions, completed adaptation work and functioning northern infrastructure. These outcomes would strengthen civilian safety and the essential systems on which Canadian defence and NATO resilience depend.

European Space Agency. "Raging Wildfires in Ontario, Canada." Wikimedia Commons. July 14, 2026. https://commons.wikimedia.org/wiki/File:Raging_wildfires_in_Ontario,_Canada_ESA524185.jpg.



European Union, Copernicus Sentinel-2 imagery. "Canada Wildfire Season Sets Alarming Record." Wikimedia Commons. July 1, 2023. https://commons.wikimedia.org/wiki/File:Canada_Wildfire_Season_Sets_Alarming_Record.jpg.

Endnotes:

1. Rantanen, Mika, Alexey Yu. Karpechko, Antti Lipponen, Kalle Nordling, Otto Hyvärinen, Kimmo Ruosteenoja, Timo Vihma, and Ari Laaksonen. 2022. "The Arctic Has Warmed Nearly Four Times Faster than the Globe since 1979." Communications Earth & Environment 3: 168. https://www.nature.com/articles/s43247-022-00498-3
2. Public Safety Canada. 2025. "Government of Canada Provides Update on 2025 Wildfires as Support Continues." October 30. https://www.canada.ca/en/public-safety-canada/news/2025/10/government-of-canada-provides-update-on-2025-wildfires-as-support-continues.html
3. Public Safety Canada. 2026. "The Government of Canada Provides an Update Regarding the 2026 Wildfire Season — August Update." August 18. https://www.canada.ca/en/public-safety-canada/news/2026/08/the-government-of-canada-provides-an-update-regarding-the-2026-wildfire-season--august-update.html
4. Canada. 2007. Emergency Management Act. S.C. 2007, c. 15. https://laws-lois.justice.gc.ca/eng/acts/e-4.56/page-1.html
5. "NATO Resilience, Civil Preparedness and Article 3," NATO, updated November 13, 2024, https://www.nato.int/en/what-we-do/deterrence-and-defence/resilience-civil-preparedness-and-article-3
6. Department of National Defence. 2026c. "Operation LENTUS." Government of Canada. Updated July 30. https://www.canada.ca/en/department-national-defence/services/operations/military-operations/current-operations/operation-lentus.html.
7. House of Commons Standing Committee on National Defence. 2024. Providing Aid to the Civil Power: Disaster Relief and the Canadian Armed Forces' Domestic Operations. Report 13. 44th Parliament, 1st Session. https://www.ourcommons.ca/documentviewer/en/44-1/NDDN/report-13/page-75
8. Forster, Sam. 2025. "Canadian Forces Face 'Mission Creep' as Domestic Deployments Surge." Canadian Affairs, August 20. https://www.canadianaffairs.news/2025/08/20/domestic-operations-strain-canadian-forces/
9. House of Commons Standing Committee on National Defence. 2024. Providing Aid to the Civil Power: Disaster Relief and the Canadian Armed Forces' Domestic Operations. Report 13. 44th Parliament, 1st Session. https://www.ourcommons.ca/documentviewer/en/44-1/NDDN/report-13/page-75
10. Public Safety Canada. 2023. "Government of Canada Continues to Build Disaster Response Capacity to Large-Scale Disasters." July 11. https://www.canada.ca/en/public-safety-canada/news/2023/07/government-of-canada-continues-to-build-disaster-response-capacity-to-large-scale-disasters.html
33. Public Safety Canada. 2026. "Government of Canada Funds 10 New Wildfire-Firefighting Aircraft and Two Firefighting Support Assets to Boost Nationwide Response Capacity." May. https://www.canada.ca/en/public-safety-canada/news/2026/05/government-of-canada-funds-10-new-wildfire-firefighting-aircraft-and-two-firefighting-support-assets-to-boost-nationwide-response-capacity.html

Endnotes:

12. Government of Canada. "Government Response to the Thirteenth Report of the Standing Committee on National Defence." October 2024. https://www.ourcommons.ca/content/Committee/441/NDDN/GovResponse/RP13330741/441_NDDN_Rpt13_GR_PDF/441_NDDN_Rpt13_GR-e.pdf
13. Auditor General of Canada. "Report 8—Emergency Management in First Nations Communities—Indigenous Services Canada." Reports of the Auditor General of Canada to the Parliament of Canada, 2022. https://www.canada.ca/en/auditor-general/our-work/audit-reports/parl-oag-202211-08-e.html.
14. Ontario. 2024. "Premier Doug Ford Launches Ontario Corps." December 13. https://news.ontario.ca/en/release/1005493/premier-doug-ford-launches-ontario-corps
15. Nova Scotia. 2024. "Nova Scotia Guard, New Department Will Improve Emergency Readiness." March 28. https://news.novascotia.ca/en/2024/03/28/nova-scotia-guard-new-department-will-improve-emergency-readiness
16. Quebec, Ministère de la Sécurité publique. "200 membres de la Réserve d'intervention d'urgence en sécurité civile prêts à être déployés lors de sinistres majeurs." April 2025. https://www.quebec.ca/nouvelles/actualites/details/proteger-les-quebecois-et-les-quebecoises-200-membres-de-la-reserve-dintervention-durgence-en-securite-civile-prets-a-etre-deployes-lors-de-sinistres-majeurs-61717.
17. British Columbia, Ministry of Emergency Management and Climate Readiness. "Strengthening Community Resilience in Climate Emergencies." April 30, 2026. https://news.gov.bc.ca/releases/2026EMCR0022-000482.
18. Federal Agency for Technical Relief. n.d. "Federal Agency for Technical Relief." Accessed September 11, 2026. https://www.thw.de/EN/homepage/homepage_node.html
19. Federal Emergency Management Agency. "How FEMA Works." Accessed September 11, 2026. https://www.fema.gov/about/how-fema-works
20. Federal Emergency Management Agency. "Integrated Public Alert and Warning System." Accessed September 11, 2026. https://www.fema.gov/emergency-managers/practitioners/integrated-public-alert-warning-system
21. Environment and Climate Change Canada. 2021. "Alert Ready: Emergency Alerting System." June 3. https://www.canada.ca/en/environment-climate-change/services/weather-general-tools-resources/alert-ready-emergency-system.html
22. Asgary, Ali. 2023. "Canada Urgently Needs a FEMA-like Emergency Management Agency." The Conversation, June 12. https://theconversation.com/canada-urgently-needs-a-fema-like-emergency-management-agency-207400.
23. Swedish Civil Defence and Resilience Agency. "Our Mission." Accessed August 24, 2026. https://www.msb.se/en/about-msb/our-mission/.
24. Lynes, Matt. 2026. "How Finland's Comprehensive Security Model Became Europe's New Standard." Patria Magazine, June 22. https://www.patriagroup.com/newsroom/patria-magazine/situation/how-finlands-comprehensive-security-model-became-europes-new-standard.

Endnotes:

25. Norway, Ministry of Justice and Public Security. 2025. Total Preparedness — Prepared for Crises and War. Meld. St. 9 (2024–2025). https://www.regjeringen.no/en/documents/meld.-st.-9-20242025/id3082364/
26. Beaulieu, Rémy-Claude. 2024. The Green Helmets Initiative (GHI): The International Dimensions. Technical Note 1. March. https://www.editionsphileas.ca/documents/2.%20The%20Green%20Helmets%20Initiative-%20The%20International%20Dimensions%20Framed.pdf
27. Public Safety Canada. 2026. "The Government of Canada Provides an Update Regarding the 2026 Wildfire Season — August Update." August 18. https://www.canada.ca/en/public-safety-canada/news/2026/08/the-government-of-canada-provides-an-update-regarding-the-2026-wildfire-season--august-update.html
28. Department of National Defence. n.d. "Disaster Assistance Response Team (DART)." Accessed September 11, 2026. https://www.canada.ca/en/department-national-defence/services/operations/military-operations/types/dart.html
29. Environment and Climate Change Canada. 2023. Canada's National Adaptation Strategy. https://www.canada.ca/en/services/environment/weather/climatechange/climate-plan/national-adaptation-strategy/full-strategy.html
30. Wand, Eleanor. 2026. "Canada's Progress on Climate Adaptation Too Slow, Unfocused, Say Experts: 'We Have to Get Moving.'" The Hill Times, September 5. https://www.hilltimes.com/2026/09/05/canadas-progress-on-climate-adaptation-too-slow-unfocused-say-experts-we-have-to-get-moving/516800/.
31. House of Commons Standing Committee on National Defence. 2024. Providing Aid to the Civil Power: Disaster Relief and the Canadian Armed Forces' Domestic Operations. Report 13. 44th Parliament, 1st Session. https://www.ourcommons.ca/documentviewer/en/44-1/NDDN/report-13/page-75
32. Commissioner of the Environment and Sustainable Development. 2026. Climate Resilience of Federal Assets and Services. May 4. https://www.canada.ca/en/auditor-general/our-work/audit-reports/commissioner-environment-sustainable-development-202605-climate-resilience-federal-assets-services.html
33. Canadian Climate Institute. 2026. Prepare or Repair: How Climate-Proofing Public Infrastructure Pays Off. Updated April 2026. https://climateinstitute.ca/reports/prepare-or-repair-canada-infrastructure/
34. Wand, Eleanor. 2026. "Canada's Progress on Climate Adaptation Too Slow, Unfocused, Say Experts: 'We Have to Get Moving.'" The Hill Times, September 5. https://www.hilltimes.com/2026/09/05/canadas-progress-on-climate-adaptation-too-slow-unfocused-say-experts-we-have-to-get-moving/516800/.

Endnotes:

35. Linden-Fraser, Ross, Dave Sawyer, Franziska Förg, Brad Griffin, and Arthur Zhang. 2026. Independent Assessment: 2025 Progress Report on the 2030 Emissions Reduction Plan. Canadian Climate Institute. February. https://climateinstitute.ca/wp-content/uploads/2026/02/Climate-Institute-440-Megatonnes-Independent-Assessment-2026-2025-Progress-Report-2030-Emissions-Reduction-Plan.pdf.
36. Innovation, Science and Economic Development Canada. 2026. "Enabling Large-Scale Sovereign AI Data Centres." June 4. https://ised-isde.canada.ca/site/ised/en/enabling-large-scale-sovereign-ai-data-centres
37. Independent Electricity System Operator. 2026. "2026 Annual Planning Outlook in 5 Graphs and a Map." https://ieso.ca/Sector-Participants/Planning-and-Forecasting/Annual-Planning-Outlook/2026-APO-Summary
38. Prime Minister of Canada. 2026. "Prime Minister Carney Announces Ambitious New Plan to Defend, Build, and Transform the North." News release, March 12. https://www.pm.gc.ca/en/news/news-releases/2026/03/12/prime-minister-carney-announces-ambitious-new-plan-defend-build-and
39. Department of National Defence. 2026. "Appearance Before the Standing Senate Committee on National Security, Defence and Veterans Affairs (SECD): Mandate, Priorities, and NATO 2% — 27 April 2026." https://www.canada.ca/en/department-national-defence/corporate/reports-publications/proactive-disclosure/2026/secd-mandate-priorities-nato-2percentage.html
40. Hjort, Jan, Olli Karjalainen, Juha Aalto, Sebastian Westermann, Vladimir E. Romanovsky, Frederick E. Nelson, Bernd Etzelmüller, and Miska Luoto. 2018. "Degrading Permafrost Puts Arctic Infrastructure at Risk by Mid-Century." Nature Communications 9: 5147. https://www.nature.com/articles/s41467-018-07557-4
41. Inuit Tapiriit Kanatami. 2025. An Inuit Vision for Arctic Sovereignty, Security and Defence. June 16. https://itk.ca/an-inuit-vision-for-arctic-sovereignty-security-and-defence/
42. Transport Canada. 2026. "Arctic Infrastructure Fund Applicant Guide." Updated March 24. https://tc.canada.ca/en/programs/arctic-infrastructure-fund/arctic-infrastructure-fund-applicant-guide
43. Wand, Eleanor. 2026. "Canada's Progress on Climate Adaptation Too Slow, Unfocused, Say Experts: 'We Have to Get Moving.'" The Hill Times, September 5. https://www.hilltimes.com/2026/09/05/canadas-progress-on-climate-adaptation-too-slow-unfocused-say-experts-we-have-to-get-moving/516800/

Authors: Dr. John Walsh, Professor, Associate Professor, University of Guelph
Darren Sargent, Program Manager, University of Guelph

Chapter 6. Education and Information Resilience

Executive Summary

Canada's ability to withstand future crises depends on the strength of its civic institutions and an informed, resilient society. As hybrid threats, disinformation, cyberattacks, and geopolitical competition become increasingly prominent, education and information resilience have become integral components of national security. This chapter argues that education and information resilience should be understood as mutually reinforcing dimensions of Canada's resilience under Article 3 of the North Atlantic Treaty. Schools, universities, and other educational institutions play a vital role in developing the knowledge, critical thinking, democratic values, and public trust required to sustain effective governance during crises. An all-of-Canada defence culture will therefore require stronger democratic literacy and greater resistance to mis- and disinformation. It will also depend upon sustained cooperation between educational institutions and government, and upon protecting the institutions and habits of judgement by which a democratic society distinguishes truth from manipulation. Such cooperation must preserve academic freedom and institutional independence.

Main Policy Recommendations

- **Develop a National Education and Information Resilience Strategy** that integrates education, democratic literacy, public communication, institutional trust, and responses to mis- and disinformation.
- **Strengthen coordination** between governments, educational institutions, and civil society through a national Article 3 Education and Information Resilience Table.
- **Integrate democratic resilience, information literacy, source criticism,** and an understanding of contemporary information threats into educational programs.
- **Invest in research, Serving Scholar-style programs**, and other initiatives that strengthen democratic resilience while safeguarding academic freedom and institutional independence.

Introduction

The renewed emphasis on national resilience within NATO has forced democratic societies to think again about the civil foundations of defence. For much of the post-Cold War period, public discussions of security in Canada tended to divide the hard from the soft, the military from the civilian, the strategic from the social, and defence from education. Security was often imagined in terms of platforms, procurement, deployments, alliances, Arctic presence, critical infrastructure, intelligence, and emergency response. Education, by contrast, was treated as a social good, an economic asset, a path to individual opportunity, or a driver of innovation. These descriptions are not wrong, but they are incomplete. They miss the deeper truth that a country's ability to withstand crisis depends not only on what it can deploy in an emergency, but on what it has formed in peace.

NATO's understanding of resilience under Article 3 of the North Atlantic Treaty begins from the recognition that collective defence requires capable societies. Resilience is not simply the possession of military force. It is also the ability of a state and its people to prepare for, absorb, resist, respond to, and recover from shocks. Those shocks may be military, but they may also be cyber, informational, economic, biological, environmental, infrastructural, or political. Modern conflict and crisis do not respect tidy distinctions between civilian and military systems.[1] A cyberattack can begin as a technical intrusion and quickly become a hospital, communications, and public-trust crisis; a campaign of disinformation may pass through public health or an election before presenting itself as a crisis of democratic legitimacy. Even a flood may test transportation, food supply, and military support at once.

Resilience is not merely a technical condition. It is also a civic and educational condition. It depends on trained people, trusted institutions, habits of judgement, social cohesion, democratic confidence, communication capacity, and a shared understanding that national preparedness is not the responsibility of government and the military alone.

Hardening systems will accomplish little if Canada neglects the institutions that form the people who must operate, defend, interpret, repair, and legitimate them. Equipment may protect assets, but it cannot by itself cultivate democratic judgement; technical detection may identify falsehoods, but it cannot restore confidence in the possibility of truth. Sovereignty itself becomes hollow when the social, informational, and educational foundations of sovereign agency are allowed to weaken.

This chapter argues that education and information resilience should be treated as mutually reinforcing dimensions of Canada's Article 3 resilience. Together, they answer a single strategic question: can Canada form a society capable of understanding threats, resisting manipulation, sustaining warranted trust, supporting democratic institutions, and exercising judgement under pressure? The answer lies in the institutions and habits Canada chooses to build in peace.

The phrase that best captures this deeper alignment is the old union of arms and letters: *arma et litterae*. Arms and letters do not name two rival worlds. They name two necessary dimensions of sovereign citizenship. Arms without letters risk becoming mere force; letters without arms risk becoming abstraction without responsibility. A democratic society requires both the capacity to defend itself and the capacity to understand what is being defended. For Canada, the renewal of arms and letters is a practical doctrine of democratic resilience.

Education must not be turned into an instrument of military policy or state messaging. The point is rather to recognize it as one of the institutions through which a free society forms the judgement, competence, memory, service ethic, and public trust upon which defence ultimately depends. In an age of hybrid threats, mis- and disinformation, cyber vulnerability, public distrust, strategic competition, and renewed geopolitical danger, education is not peripheral to national security. It is one of the places where resilience is constructed.

From Defence Policy to Sovereign Capacity

Canada often discusses defence in measurable but incomplete terms: spending, procurement, ships, aircraft, recruitment, readiness, Arctic presence, ammunition stocks, industrial capacity, and alliance contribution. These are necessary. A serious country must possess the instruments of defence, and Canada has too often permitted gaps between its rhetoric and its capacity on this count. But defence policy alone does not exhaust the meaning of sovereignty.

Defence protects sovereignty. Sovereignty is the deeper condition: the ability of a political community to govern itself, interpret the world through its own institutions, make decisions under pressure, preserve democratic legitimacy, sustain essential functions in crisis, and act as a serious ally rather than a protected dependent. A state may own equipment and still lack strategic sovereignty if it cannot form judgement, coordinate institutions, preserve trust, mobilize citizens, interpret threats, or sustain public consent. Conversely, a state may speak constantly of sovereignty while leaving the practical and civic instruments of sovereign agency neglected.

> **"The central danger for a middle power such as Canada is not only military weakness. It is the more subtle danger of mistaking participation for agency, protection for sovereignty, and alliance membership for national seriousness. NATO membership is indispensable to Canada's defence, but it cannot become an alibi for diminished domestic capacity."**

Article 3 matters because it insists that each NATO member must maintain and develop its own capacity to resist armed attack. Collective defence depends upon national resilience, and national resilience depends upon the capabilities of the society as a whole.

That society-wide capacity is not only military, industrial, or infrastructural. It is educational, informational, institutional, and civic. A country that cannot interpret the world through institutions of its own will eventually borrow not only military capacity, but strategic imagination. It will see crises through the categories of others, respond through borrowed doctrines, and mistake its presence inside collective structures for the possession of sovereign agency. Canada's contribution to NATO must therefore be understood not only in terms of what Canada can deploy, but in terms of what Canada can sustain: judgement, infrastructure, trust, expertise, public will, institutional continuity, and democratic legitimacy.

This is the point at which education becomes a security issue. Education is not security in the narrow sense, and it must not be reduced to security policy. But a sovereign democracy requires educated citizens and institutions capable of judgement. It requires people who can distinguish evidence from manipulation, understand the responsibilities of citizenship, communicate under pressure, serve in public roles, and sustain confidence in democratic life. These are not luxuries. They are the conditions that allow free societies to remain governable under stress.

Equipment can be purchased and strategies announced far more quickly than public judgement or institutional trust can be formed. Emergency plans may be drafted in months; the civic habits required to make them work are the product of years. Education is therefore the slow-forming infrastructure of national endurance, and its strategic value is often most visible only after it has been neglected.

Education as Strategic Infrastructure

Every requirement of national resilience ultimately depends upon human capacity. Systems do not operate, interpret, repair, or legitimate themselves. They depend upon people formed through educational institutions: public servants, engineers, health professionals, scientists, communications specialists, legal advisers, researchers, teachers, technicians, and local leaders. Education therefore sits upstream from the technical and institutional capacities upon which resilience depends.

Schools, colleges, and universities form the citizens and professionals who will later operate the country's systems. They do not merely transmit information. At their best, they cultivate habits of attention, discipline, evidence, disagreement, ethical reasoning, historical memory, and public responsibility. They help students understand that citizenship is not passive belonging, but participation in a shared political order that sometimes makes claims upon them.

In the Canadian context, higher education deserves particular attention. Universities and colleges are major regional institutions, combining laboratories and technical expertise with health and food services, communications networks, libraries, archives,

residences, and large student populations. They educate much of the professional and civic workforce upon which resilience depends, from engineers, health professionals, and public servants to researchers, journalists, military officers, reservists, and community leaders. They are not defence institutions in the narrow sense. They are nevertheless institutions of national capacity because they form the knowledge and human capability on which resilience rests. Yet Canada does not consistently regard them in this way. Higher education is generally discussed in economic, administrative, or social terms: enrolment, employment, student experience, research funding, innovation, access, and equity. Each of these matters, but none exhausts the sector's public significance. A university is one of the few institutions in Canadian life that teaches the young while also producing research, training professionals, preserving memory, interpreting public events, convening disagreement, and maintaining a substantial regional presence. To leave such institutions outside national resilience planning is not neutrality. It is a failure to recognize one of the country's major civil assets.

This failure is partly structural. Education in Canada is primarily provincial, while defence and national security are federal.[2] Responsibility for national resilience crosses federal, provincial, municipal, Indigenous, private-sector, and civil-society domains. As a result, education falls between policy categories. Universities and colleges produce capacities of national significance, but they are funded, regulated, and governed largely through provincial systems. The federal government needs the human capacity they form but does not govern the sector directly. Provinces govern and fund education but may not always frame it in relation to NATO obligations or national resilience. Institutions themselves often lack a vocabulary that connects their educational mission to national endurance.

The result is not a lack of capacity, but a lack of alignment. Canada possesses enormous educational resources relevant to resilience, but those resources remain implicit, fragmented, unevenly organized, and often disconnected from defence and national resilience planning. Thus, the task is to recognize education as a strategic civil foundation of democratic resilience.

Information Resilience: The Defence of Judgement

The most urgent reason to expand the frame beyond traditional education is the rise of information disorder. Mis- and disinformation are not simply communications problems. They are attacks on judgement, trust, and democratic coordination.

Misinformation may be false or misleading information spread without malicious intent. Disinformation is false or misleading information spread deliberately to deceive, manipulate, divide, destabilize, or exhaust.[3] The distinction matters, but the deeper issue is not merely whether particular claims are true or false. Information resilience is not simply the capacity to correct falsehoods. It is the capacity of a society to preserve public reason under conditions of informational stress.

The strategic purpose of disinformation is often not persuasion but corrosion. It does not need every citizen to believe a lie. It only needs enough citizens to doubt whether truth, expertise, government, journalism, science, law, elections, universities, or democratic institutions can be trusted at all. The goal is not always to replace one belief with another. It is to make judgement itself seem impossible.[4]

A society loses information resilience not when it encounters falsehood, but when it loses confidence in its own capacity to judge. When expertise appears indistinguishable from propaganda, when disagreement becomes indistinguishable from bad faith, when institutions are assumed to be fraudulent before they speak, and when every public claim is treated as manipulation, democratic coordination becomes almost impossible. In that condition, a society may remain formally free while becoming functionally ungovernable under stress.

This is why information resilience must be treated as a core national security issue. Public-health guidance depends on trust. Emergency response depends on trust. Elections depend on trust. Military support depends on trust. Infrastructure protection depends on trust. Allied commitments depend on trust. A society that cannot trust enough to act cannot be resilient, no matter how sophisticated its infrastructure may be.

Public trust is not sentimental. It is operational. Without it, warnings are ignored, expertise is rejected, emergency measures are suspected, institutions are delegitimized, and hostile actors can turn openness against itself. The defence of trust is therefore not a soft cultural preference. It is part of national preparedness.[5]

Education has a central role here, but not in the superficial sense of adding a few media-literacy modules to existing curricula. The challenge is deeper. Citizens need source criticism, historical reasoning, scientific literacy, statistical understanding, ethical analysis, language competence, public communication, civic knowledge, and the ability to distinguish argument from assertion. They need to understand how institutions work, why disagreement is not the same as collapse, why uncertainty is not the same as deceit, and why expertise is not infallible but still indispensable.

The humanities and social sciences matter profoundly to this task. Technical systems may defend networks, but humanistic and social knowledge helps defend judgement, legitimacy, meaning, and democratic cohesion. A cyber specialist may identify an intrusion; a historian may explain why a society is susceptible to a particular narrative; a linguist may interpret the cultural resonance of hostile messaging; a political scientist may identify institutional vulnerabilities; a sociologist may track patterns of polarisation; a philosopher may clarify the ethical limits of state response; a classicist may remind us that republics often decay not first from invasion, but from the loss of civic seriousness. None of these forms of knowledge is sufficient alone. Together, they form the intellectual ecology of a resilient democracy.

The temptation in policy is to respond to information disorder through communications strategy alone: better messaging, faster correction, stronger monitoring, more digital tools, more platform accountability. These responses have value, but they are

downstream responses. The upstream response is civic formation. A country that wishes to resist manipulation must form citizens who are harder to manipulate. It must cultivate habits of mind and trust before hostile actors seek to exploit their absence.

Correction, however necessary, cannot by itself produce information resilience. A correction reaches citizens only through institutions, authorities, and forms of expertise whose credibility may already have been weakened by the original campaign.[6] Nor does the strategic problem consist solely in the circulation of individual falsehoods. Contemporary information operations can exploit genuine grievances, amplify existing divisions, place authentic facts within deliberately misleading narratives, and overwhelm the public sphere with such volume and contradiction that verification becomes exhausting. Their object is often not to establish a durable alternative account of reality, but to make every account appear interested, every institution compromised, and every judgement provisional.

The emergence of generative artificial intelligence intensifies this difficulty. Synthetic text, images, audio, and video can be produced rapidly, varied endlessly, and distributed through networks of apparently independent voices. The strategic advantage lies not only in the credibility of any single fabrication, but in the cumulative uncertainty produced when citizens can no longer assume that what they see or hear has a stable human source. Information resilience must therefore include an understanding of provenance, platform incentives, automated amplification, synthetic media, and the conditions under which digital evidence can reasonably be trusted.[7]

Yet democratic resilience also requires precision. Not every error is disinformation; not every disagreement is manipulation; not every criticism of an institution is evidence of hostile influence. A democracy that treats dissent as disinformation would damage the very freedom it claims to defend. The task is to preserve a public sphere in which criticism remains possible while organized deception remains identifiable: a society capable of scepticism without cynicism, trust without credulity, and disagreement without epistemic collapse.

Education and the Formation of Civic Responsibility

Education has never been concerned solely with the acquisition of private advantage. It also prepares individuals to enter a shared political and institutional world. Students are future professionals, voters, researchers, officials, teachers, service members, and custodians of institutions whose continuity depends upon their judgement. A resilient democracy must therefore educate people not merely to succeed within society, but to assume responsibility for the conditions that allow society to endure.

This is where education and public service must be brought closer together. Educational institutions should not be so distant from defence and national service that military obligations appear alien to civic life. Serving students, reservists, veterans, and military family members are natural bridges between education and national resilience. Their presence makes visible the fact that democratic citizenship can include

disciplined service to the public order and that intellectual formation and public obligation need not belong to separate worlds.

The goal is not to collapse education into service. It is to restore the idea that education is itself preparation for public responsibility. A democracy is weakened when education teaches people only to succeed privately, consume critically, or express themselves politically, but not to deliberate, build, protect, remember, and serve. Resilience requires more than awareness. It requires formation.

Arma et Litterae: The Civic Alignment of Education and Defence

> **"The old formula arma et litterae—arms and letters—captures the relationship Canada now needs to renew between learning, service, and sovereignty."**

It places military service within democratic civic life and education within the formation of citizens capable of judgement, responsibility, and public service.

> **"Arms without letters become mere force. Letters without arms may become abstraction without responsibility."**

The soldier must remain connected to the civic and moral world in whose name service is rendered. The scholar must remember that free inquiry is protected by institutions that must sometimes be defended. In this sense, arms and letters are not rival languages. They are the two grammars of sovereign citizenship.

> **"The estrangement between military service and civilian intellectual life is a quiet vulnerability in many democracies."**

Military service may be publicly honoured but privately misunderstood. Universities may support individual students who serve, but often treat military obligations as scheduling complications rather than civic obligations. Faculty and students may respect the military in the abstract while having little understanding of its role, culture, demands, or connection to democratic life. Conversely, the military may become socially and intellectually distant from the civilian institutions whose freedoms it protects.

Neither condition is healthy. A military isolated from civilian learning risks becoming culturally remote from the democracy it serves. A university alienated from defence risks strategic innocence—the ability to critique power without understanding the

conditions that preserve the freedom to critique it. A democratic society requires neither militarized campuses nor anti-military campuses. It requires mature civic reciprocity between service and learning.

The purpose is to re-civicize defence and re-sovereignize education. Defence must be understood not as an alien activity outside public life, but as one form through which citizenship accepts risk on behalf of the common order. Education must be understood not merely as private advancement or critical distance, but as preparation for judgement, responsibility, and service. A free society requires citizens who can think seriously about force without worshipping it, and who can criticize power without forgetting the conditions that protect their freedom to do so.

> **"At the University of Guelph, we have sought to give this principle institutional form through the Serving Scholar Program.[8]"**

The program emerged from a practical difficulty that revealed a larger civic problem. Students serving in the Canadian Armed Forces and the Primary Reserve belong to two demanding institutions, each of which places legitimate claims upon their time, discipline, and loyalty. Yet universities and the Armed Forces have not always possessed a common language through which those obligations could be understood. Training exercises, operational requirements, and periods of service could appear within academic administration merely as absences or scheduling complications, while the intellectual and civic value of military service remained largely invisible within university life. Serving students were therefore expected to move between two worlds that too rarely understood one another.

The Serving Scholar Program was created to bridge that divide. It recognizes students who combine academic study with service in the Canadian Armed Forces, helps educational institutions understand the distinctive obligations attached to that service, and provides a framework through which academic responsibility and military duty can be reconciled without diminishing either. Its purpose is not to excuse students from academic standards or to treat service as a substitute for scholarship. It is to ensure that students are not institutionally disadvantaged because they have accepted public obligations beyond the campus. Through recognition, communication, appropriate academic accommodation, experiential learning, mentorship, and a visible community of serving students, the program makes military service intelligible within the university while affirming that those who serve remain full members of its intellectual life.

We have learned through the program that the distance between education and defence is neither inevitable nor especially difficult to narrow. It often persists because institutions have never been asked to consider how their procedures, language, and assumptions appear to those who inhabit both worlds. A modest institutional framework can therefore produce consequences larger than its administrative dimensions. It tells serving students that their obligations are understood as civic

commitments rather than private inconveniences. It reminds civilian students and faculty that military service is undertaken by members of their own academic community. It enables the Armed Forces to see universities not merely as sources of credentials or recruits, but as partners in the formation of reflective, educated, and democratically grounded service members.

Convocation Ceremony for Lt Aksh Sharma in the 11th Field Regiment, RCA Officers' Mess. Photo credits: University of Guelph

The Serving Scholar Program is not offered as a complete model of national resilience. It is a limited but instructive example of how an institutional separation can be identified and a durable bridge built across it. Its wider significance lies in the principle it embodies: a university can preserve its independence, intellectual pluralism, and critical purpose while recognizing that some of its students have assumed direct responsibility for the defence of the political order within which those freedoms exist. The same principle could be adapted across Canada, according to the circumstances of individual institutions, as part of a broader effort to restore military service to democratic civic life and public responsibility to the purposes of education.

This alignment of education and defence also includes remembrance. Remembrance is not mere ceremony, nor nostalgia for sacrifice. It is the disciplined recovery of the human cost by which present freedoms were preserved. At its best, remembrance forms citizens who understand that sovereignty is not an abstraction and peace is not a natural condition. It teaches the difference between honouring service and glorifying war. It also inoculates against the simplifications of both militarism and complacency: war is neither glorious nor irrelevant; it is terrible, consequential, and sometimes bound to the survival of free institutions.

A democracy that cannot remember seriously will struggle to defend seriously. Historical memory is therefore a resilience asset. Societies that forget the costs of their own political order become vulnerable to strategic innocence, civic fatigue, and moral confusion. In this sense, archives, memorials, military history, battlefield study, and institutional remembrance are not peripheral to resilience. They are part of the education of a sovereign people.[9]

Remembrance Day at the University of Guelph. Photo credits: Laurel Jarvis

The Serving Scholar Program is not offered as a complete model of national resilience. It is a limited but instructive example of how an institutional separation can be identified and a durable bridge built across it. Its wider significance lies in the principle it embodies: a university can preserve its independence, intellectual pluralism, and critical purpose while recognizing that some of its students have assumed direct responsibility for the defence of the political order within which those freedoms exist. The same principle could be adapted across Canada, according to the circumstances of individual institutions, as part of a broader effort to restore military service to democratic civic life and public responsibility to the purposes of education.

Information Resilience as Democratic Culture

Information resilience cannot be reduced to government communication. It must become a democratic culture: a shared capacity among citizens, institutions, educators, journalists, researchers, and public authorities to preserve meaningful judgement under conditions of uncertainty and manipulation. Governments have an essential role, but they cannot alone produce social trust, form civic judgement, or sustain public legitimacy. Nor can they counter disinformation effectively if citizens regard every public institution as inherently fraudulent before it speaks.

This challenge is especially important in a pluralistic democracy. Social cohesion cannot mean sameness, enforced consensus, or the suppression of disagreement. A resilient society is not one in which everyone thinks alike. It is one in which disagreement remains disciplined by shared commitments to truth, legality, democratic legitimacy, and public responsibility. Dissent is not the enemy of resilience. Bad faith,

organized manipulation, institutional collapse, and civic nihilism are. The task is not to eliminate disagreement, but to preserve the conditions under which disagreement remains compatible with common action.

> **"In this sense, education and information resilience are inseparable. Education forms citizens capable of disagreement without disintegration. Information resilience protects the public sphere in which disagreement can remain meaningful."**

Defence provides the ultimate guarantee that democratic life will not be surrendered to coercion. These are not separate matters. They are parts of a single civic architecture.

NATO Ally Case Studies

Canada need not invent this architecture from nothing. Several NATO members offer lessons in media literacy, psychological defence, digital resilience, and the relationship between education and national security. These examples should not be imported mechanically. Canada's geography, federalism, Indigenous realities, bilingualism, regional diversity, political culture, and threat perception are distinct. But Allied examples can help clarify what Canada has underdeveloped.

1. Finland offers the clearest example of media literacy treated not as an emergency response to particular campaigns, but as a durable educational capacity.[10] Critical engagement with media, digital information, and source credibility is situated within a wider culture of learning rather than confined to occasional public-awareness initiatives. The significance of this approach lies less in any single curriculum than in the assumption beneath it: citizens become more difficult to manipulate when habits of interpretation, verification, and critical judgement have been cultivated long before they are tested. No educational system can eliminate disinformation, but it can reduce the ease with which public uncertainty is converted into political paralysis.

2. Sweden approaches the problem through the institutional language of psychological defence.[11] Its purpose is not merely to rebut false claims after they appear, but to strengthen the ability of public authorities, journalists, civil society, and citizens to recognize and resist malign information influence. Government communication matters, but it cannot substitute for public understanding, credible institutions, or independent media.

3. Estonia's experience begins from a different premise and treats digital systems as inseparable from sovereignty itself.[12] A state whose public life, administration, communications, and democratic processes depend heavily upon digital infrastructure cannot treat resilience as a purely technical matter. Cyber capacity must be joined to public trust, educational competence, and institutional clarity.

The defence of networks and the defence of judgement are therefore not parallel tasks, but parts of the same strategic problem.

4. The United Kingdom offers a different kind of lesson. Defence is studied openly in Canada, within universities, military colleges, research institutes, professional education, and publications such as this one. The British example is useful not because it reveals an activity absent from Canada, but because it shows what can emerge when that activity is sustained across several kinds of institution over a long period. RUSI provides a forum for independent public analysis; King's College London has made the study of war a broad intellectual field; and the Royal College of Defence Studies and the Joint Services Command and Staff College bring officers, civil servants, scholars, and international partners into sustained consideration of strategy and statecraft.[13] The significance lies in the habit of exchange among them. Military experience is brought into conversation with history, politics, ethics, and criticism, while civilian scholarship encounters the practical burdens of command and public responsibility. Canada already possesses many of the elements of such a conversation. The lesson is that they should be connected more deliberately and sustained more consistently, without sacrificing the independence that gives each institution its value.

The common lesson is that resilient societies do not wait until crisis to teach citizens how information systems function, how manipulation operates, or why democratic institutions matter. They cultivate judgement and information resilience as public habits, not merely as emergency responses. Canada has many of the necessary institutional assets, but it has not yet aligned them with sufficient seriousness.

Policy Directions for Canada

A serious Canadian approach to education and information resilience should begin with recognition. Canada should explicitly recognise education and information resilience as mutually reinforcing dimensions of national resilience. This recognition should not subordinate education to defence. It should acknowledge that the capacities formed by educational institutions are indispensable to democratic judgement, institutional trust, and national endurance.

First, Canada should develop a national education and information resilience strategy. This strategy should connect education policy, public communication, mis- and disinformation response, democratic literacy, research, media and AI literacy, and defence culture. It should be built across federal, provincial, Indigenous, educational, civil-society, media, and private-sector partners. Its core purpose would be to strengthen the social and informational conditions under which Canada can act coherently in crisis.

Second, Canada should establish an Article 3 education and information resilience table. This body would bring together federal departments, provincial education ministries, universities, colleges, schools, the Canadian Armed Forces, Indigenous partners, civil society, journalists, public communicators, and information-resilience

experts. Its task would be coordination, not command: mapping existing capacity, identifying gaps, sharing best practices, advising on information resilience, and connecting education more deliberately to national resilience. Third,

> **"Canada should develop national education modules on NATO, democratic resilience, and information resilience. These should be adaptable for high schools, colleges, universities, public-service training, and community organizations."**

They should avoid propaganda and partisan messaging. Their purpose should be civic formation: helping Canadians understand democratic institutions, alliance obligations, disinformation, source credibility, synthetic media, public trust, and the responsibilities of citizenship.

Fourth, Canada should fund interdisciplinary research clusters on information resilience and democratic trust. These clusters should bring together computer science, communications, psychology, political science, history, linguistics, law, philosophy, public health, data science, education, and defence studies. Research should address disinformation, AI-generated manipulation, hostile influence, public trust, institutional legitimacy, strategic communication, civic education, platform dynamics, synthetic media, and democratic resilience under stress.

Fifth, Canada should expand Serving Scholar-style programs nationally. These programs would support students who serve, recognize military obligations as civic obligations, connect service to experiential learning, strengthen civil-military literacy, and help educational institutions see service as part of democratic formation. They would make military service intelligible within academic and civic life.

Sixth, any national information-resilience strategy must protect academic freedom and institutional independence. This is essential. Universities must retain the right to criticize government policy, conduct independent research, maintain ethical review processes, debate defence and security openly, and resist inappropriate politicisation. Academic freedom is not an obstacle to resilience. It is one of the reasons universities can contribute to resilience. Trusted institutions must not appear to be mere instruments of state messaging. Their independence gives their expertise credibility.[14]

The goal is not to make universities speak for the state. The goal is to ensure that, in moments of crisis, the state is supported by institutions capable of speaking truthfully, independently, and seriously. A mature democracy should not fear independent universities. It should understand them as part of its resilience.

Conclusion: The Formation of a Sovereign People

Canada's Article 3 obligations require more than hardened infrastructure, defence procurement, cyber tools, and military readiness. They require a society capable of judgement, trust, service, and coordinated action under pressure. That capacity is formed in classrooms, campuses, public institutions, research communities, civic rituals, and the habits through which a democracy learns to distinguish truth from manipulation and disagreement from disintegration. Education and information resilience are therefore not marginal to national security. They are part of the architecture of national endurance. A society that cannot preserve public reason, sustain warranted trust, or maintain confidence in its own capacity to judge will remain vulnerable no matter how sophisticated its material systems become.

The alignment of education and military service must be understood within this broader all-of-Canada frame. Its purpose is to renew the civic relationship between learning, service, sovereignty, and democratic responsibility. Arms and letters must not be estranged. A country that educates without reference to sovereignty risks producing intelligence without public purpose. A country that defends without reference to education risks producing force without civic depth.

Canada needs both. It needs the instruments of defence, but also the institutions that form citizens capable of understanding, sustaining, questioning, and supporting those instruments. It needs military readiness, but also public trust. It needs cyber capacity, but also judgement. It needs information systems, but also citizens capable of interpreting them. It needs education not merely as the transmission of knowledge, but as formation for public responsibility. It needs information resilience not merely as fact-checking, but as the defence of democratic reason itself. For Canada, the renewal of arma et litterae is Article 3 realism.

> **"A sovereign democracy must be able to defend itself, but long before that moment it must be able to think, teach, remember, judge, trust, and serve."**

The defence of Canada begins not only in arsenals, bases, command centres, and cabinet rooms, but also in the educational and civic institutions where the habits of a sovereign people are formed.

Endnotes:

1. North Atlantic Treaty Organization, The North Atlantic Treaty, April 4, 1949, art. 3, https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/1949/04/04/the-north-atlantic-treaty; North Atlantic Treaty Organization, "Strengthened Resilience Commitment," June 14, 2021, https://www.nato.int/en/about-us/official-texts-and-resources/official-texts/2021/06/14/strengthened-resilience-commitment; North Atlantic Treaty Organization, "Resilience, Civil Preparedness and Article 3," last updated November 13, 2024, https://www.nato.int/en/what-we-do/deterrence-and-defence/resilience-civil-preparedness-and-article-3.
2. Constitution Act, 1867 (UK), 30 & 31 Vict, c 3, s 93, reprinted in RSC 1985, app II, no 5, https://laws-lois.justice.gc.ca/eng/Const/page-3.html; Council of Ministers of Education, Canada, "Education in Canada: An Overview," accessed August 5, 2026, https://www.cmec.ca/299/Education-in-Canada-An-Overview/index.html.
3. Claire Wardle and Hossein Derakhshan, Information Disorder: Toward an Interdisciplinary Framework for Research and Policymaking, Council of Europe report DGI(2017)09 (Strasbourg: Council of Europe, 2017), https://rm.coe.int/information-disorder-toward-an-interdisciplinary-framework-for-researc/168076277c; Privy Council Office, Countering Disinformation: A Guidebook for Public Servants (Ottawa: Government of Canada, 2024), https://www.canada.ca/content/dam/di-id/images/pcdi/guide-eng.pdf.
4. On Soviet "active measures" and the use of disinformation not merely to persuade but to produce confusion, corrode institutional authority, and impair the possibility of settled judgement, see Thomas Rid, Active Measures: The Secret History of Disinformation and Political Warfare (New York: Farrar, Straus and Giroux, 2020); Christopher Paul and Miriam Matthews, The Russian "Firehose of Falsehood" Propaganda Model: Why It Might Work and Options to Counter It, PE-198-OSD (Santa Monica, CA: RAND Corporation, 2016), https://doi.org/10.7249/PE198; W. Lance Bennett and Steven Livingston, "The Disinformation Order: Disruptive Communication and the Decline of Democratic Institutions," European Journal of Communication 33, no. 2 (2018): 122–39, https://doi.org/10.1177/0267323118760317.
5. Public trust is not simply a favourable attitude toward institutions; it affects whether citizens will accept guidance, comply with legitimate decisions, and cooperate under conditions of uncertainty. Trust is therefore both a democratic good and a practical capacity of government. See OECD, Building Trust to Reinforce Democracy: Main Findings from the 2021 OECD Survey on Drivers of Trust in Public Institutions (Paris: OECD Publishing, 2022), https://doi.org/10.1787/b407f99c-en; OECD, OECD Survey on Drivers of Trust in Public Institutions – 2024 Results: Building Trust in a Complex Policy Environment (Paris: OECD Publishing, 2024), https://doi.org/10.1787/9a20554b-en.

Endnotes:

6. Correction does not necessarily erase the influence of the original falsehood. Misinformation may continue to shape inference and recollection even after it has been explicitly retracted, particularly when the correction fails to supply a coherent alternative explanation. See Stephan Lewandowsky et al., "Misinformation and Its Correction: Continued Influence and Successful Debiasing," Psychological Science in the Public Interest 13, no. 3 (2012): 106–31, https://doi.org/10.1177/1529100612451018. More broadly, fact-checking has a measurable corrective effect, but its efficacy varies according to the form of the correction and may be diminished by prior beliefs, ideology, and existing knowledge. See Nathan Walter et al., "Fact-Checking: A Meta-Analysis of What Works and for Whom," Political Communication 37, no. 3 (2020): 350–75, https://doi.org/10.1080/10584609.2019.1668894; see also Ullrich K. H. Ecker et al., "The Psychological Drivers of Misinformation Belief and Its Resistance to Correction," Nature Reviews Psychology 1, no. 1 (2022): 13–29, https://doi.org/10.1038/s44159-021-00006-y.
7. Generative artificial intelligence alters the scale and economics of information manipulation. Its importance lies not merely in the production of convincing individual fabrications, but in the capacity to generate, vary, personalize, and distribute synthetic material at speed, thereby weakening ordinary assumptions about authorship and provenance. See Alfonsas Juršėnas et al., The Double-Edged Sword of AI: Enabler of Disinformation (Riga: NATO Strategic Communications Centre of Excellence, 2021), https://stratcomcoe.org/publications/the-double-edged-sword-of-ai-enabler-of-disinformation/221; Gundars Bergmanis-Korāts and Joshua Chia Tee Hiang, Beyond Spam Bots: The Rise of AI-Powered Disinformation Machines and the Imperative for Strategic Response (Riga: NATO Strategic Communications Centre of Excellence, 2026), https://stratcomcoe.org/publications/beyond-spam-bots-the-rise-of-ai-powered-disinformation-machines-and-the-imperative-for-strategic-response/342.
8. The account presented here draws upon the authors' direct involvement in the creation and administration of the Serving Scholar Program. For the program's current structure, experiential-learning opportunities, and institutional activities, see University of Guelph, "Serving Scholar Program."
9. On the social formation of memory, see Paul Connerton, How Societies Remember (Cambridge: Cambridge University Press, 1989); on the transformation of wartime death into public myth and civic meaning, see George L. Mosse, Fallen Soldiers: Reshaping the Memory of the World Wars (New York: Oxford University Press, 1990); and on mourning, commemoration, and the cultural memory of the Great War, see Jay Winter, Sites of Memory, Sites of Mourning: The Great War in European Cultural History (Cambridge: Cambridge University Press, 1995).

Endnotes:

10. Finnish National Agency for Education, "Multiliteracy and Media Literacy," accessed August 5, 2026, https://www.oph.fi/en/education-and-qualifications/multiliteracy-and-media-literacy; Saara Salomaa and Lauri Palsa, Media Literacy in Finland: National Media Education Policy, Publications of the Ministry of Education and Culture, Finland 2019:39 (Helsinki: Ministry of Education and Culture, 2019), https://urn.fi/URN:ISBN:978-952-263-676-8.
11. Jesper Falkheimer and James Pamment, eds., Psychological Defence and Information Influence: A Textbook on Theory and Practice (Swedish Psychological Defence Agency, 2026), https://mpf.se/psychological-defence-agency/publications/archive/2026-01-19-psychological-defence-and-information-influence---a-textbook-on-theory-and-practice.
12. Inger Klesment, Estonia's Media Literacy Report: November 2022–October 2025 (Republic of Estonia Ministry of Education and Research and University of Tartu, December 2025), https://becid.eu/wp-content/uploads/2026/06/Estonias-Media-Literacy-Report-from-November-2022-to-October-2025_December_2025.pdf.
13. Royal United Services Institute, "Our Mission and Values," October 8, 2025, https://www.rusi.org/about/our-purpose/mission-and-values; Lizzie Ellen et al., "The History of the Department of War Studies," King's College London, September 2, 2021, https://www.kcl.ac.uk/the-history-of-the-department-of-war-studies; Defence Academy of the United Kingdom, "Royal College of Defence Studies," accessed August 5, 2026, https://www.da.mod.uk/study-with-us/colleges-and-groups/royal-college-of-defence-studies/; Defence Academy of the United Kingdom, "Joint Services Command and Staff College," accessed August 5, 2026, https://www.da.mod.uk/study-with-us/colleges-and-groups/joint-services-command-and-staff-college/. See also Michael Howard, "The Use and Abuse of Military History," Royal United Services Institution. Journal 107, no. 625 (1962): 4–10, https://doi.org/10.1080/03071846209423478.
14. Academic independence is not merely a privilege claimed by universities against public authority. It is the institutional condition that allows their research and criticism to possess credibility beyond the immediate purposes of government. UNESCO accordingly treats institutional autonomy as the institutional form of academic freedom and as a necessary condition for higher-education institutions and their teaching personnel to fulfil the functions entrusted to them. See, UNESCO, Recommendation Concerning the Status of Higher-Education Teaching Personnel, adopted November 11, 1997, paras. 17–19, https://www.unesco.org/en/legal-affairs/recommendation-concerning-status-higher-education-teaching-personnel.

Authors: Rudy Yuan, Junior Research Fellow
Laiba Awan, Junior Research Fellow

Chapter 7. Youth Engagement and Civil Preparedness

Executive Summary

Canada's long-term national resilience depends on preparing the next generation to contribute actively to their communities before crises occur. While Canadian youth demonstrate strong interest in civic engagement, volunteering, and public service, existing federal policies provide few pathways to translate this engagement into meaningful contributions to national resilience. This chapter argues that youth should be viewed as essential partners in strengthening Canada's preparedness for future emergencies. Drawing on lessons from NATO allies, it recommends expanding opportunities for civic participation, service, and preparedness while deferring any introduction of compulsory national service, for which there is presently no groundwork. By strengthening youth engagement through volunteerism, civil defence initiatives, and partnerships with civil society organizations, Canada can cultivate a resilient societal landscape that is better prepared to respond to future crises.

Main Policy Recommendations

- **Expand the Canada Service Corps** and other service programs to strengthen civic participation and support civil preparedness initiatives.
- **Develop a national framework for civil preparedness** education in partnership with provinces, integrating emergency preparedness, digital literacy, first aid, and active citizenship into schools.
- **Establish a national fund for community-based initiatives** that strengthens local resilience.
- **Create new pathways linking education, volunteerism, and public service** to encourage long-term participation in national resilience.

Youth Engagement

Introduction

On March 10, 2026, the House of Commons Standing Committee on Procedure and House Affairs began a series of hearings on the state of civic resilience in Canada.[1] These hearings reflected a growing public and political interest in civil preparedness, both domestically and across NATO allied countries, during a time of increased global uncertainty. Witnesses and committee members emphasized fostering youth engagement and participation in Canada's democratic process as a priority, considering issues ranging from effective online youth engagement to promoting quality Canadian journalism. This high-level interest indicates that youth engagement is relevant to national resilience, but youth engagement cannot remain an insular consideration. Rather, youth engagement must be continually and proactively considered in the elaboration of national resilience policy.

Effective civil preparedness underpins all seven of NATO's 2016 Warsaw Summit Baseline Requirements for National Resilience. Youth engagement in society is vital for ensuring continuity and legitimacy of government in an age of increased disinformation and disruption. Beyond the Baseline Requirements, however, youth engagement is vital to the wellbeing of any democratic society.[2] Common political challenges across NATO allied states and the wider democratic world include political polarization, the threat of terrorism, and populist extremism.[3] Though statistics show a decline in volunteerism in Canada,[4] which may appear to suggest that public engagement with civil society is regressing, Canada's 2021 State of Youth Report indicates that youth hold a generally positive view of the future and hope for additional opportunities to lead and participate in society.[5] Indeed, Canada's youth actively seek leadership and service opportunities. A majority of youth express an interest in politics, vote in federal elections, and engage in community or school organizations.[6] Nevertheless, much of Canadian youth engagement with politics happens online, through activities like signing online petitions or resharing political posts on social media.[7]

Canada's youth are interested in and engaged with politics and society. The task for policymakers is, therefore, to mobilize this interest in ways that directly enhance national resilience and to redirect youth engagement from online spaces to real life. 10 of NATO's 32 member states maintain some form of conscription,[8] which is sometimes presented as a policy option for driving youth engagement in national resilience. While a prima facie case based on opinion polling may exist for introducing some form of national service in Canada, Canada has neither the broad cultural acceptance nor the institutional-legal framework for such a policy.[9] The potential ramifications of introducing conscription or alternative national service frameworks will also be examined within this chapter.

Policy Overview and Evaluation

The Government of Canada has a blank slate for youth engagement policy. At the federal level, there is a lack of formal policy initiatives directed specifically at fostering

youth engagement. Canada's Youth Policy was unveiled in 2019 and established a four-year reporting cycle for the state of youth in Canada.[10] However, there has been no follow-up to the inaugural 2021 State of Youth Report to date, nor have there been any further revisions or updates to the 2019 Youth Policy. The primary policy priority is therefore the elaboration of a national policy for youth engagement with respect to national resilience. Such a policy must consider the shortcomings of the 2019 Youth Policy and insights from Government of Canada reports, as well as civil society studies on the state of youth engagement.

The landscape of Canadian youth engagement with politics and civil society is, by nature, diverse and heterogeneous. 81.5 per cent of youth engagement programs are administered by NGOs, compared to only 15.3 per cent by governments of all levels. This heterogeneity should not be treated as a weakness, nor should this landscape be considered fragmented as a consequence. Instead, policy aimed at invigorating youth engagement in civil preparedness for national resilience should complement the efforts of civil society organizations.

Youth voter turnout and participation at various stages of the democratic process is often considered an indicator for the health of youth engagement. Independent studies show that 18-to-23-year-olds consistently vote the least in Canadian elections and express less interest in elections and politics than Canadians over 30.[11] Youth are less likely to donate to a political party or charity, but are more likely to volunteer in their communities or boycott products for political reasons.[12] Policies to increase youth voter turnout should be developed and implemented in concert with organizations already dedicated to this cause, such as CIVIX and New Majority.[13] Likewise, policies to increase youth engagement with service-based clubs should support and revitalize the work of existing organizations. Civil defence, however, is an area where federal policy could create new opportunities for youth engagement under novel organizations.

Canada's Youth Policy 2019

Canada's Youth Policy (CYP) of 2019 establishes six youth-identified priorities: leadership and impact, health and wellness, innovation, skills and learning, employment, Truth and Reconciliation, and environment and climate action. While national resilience is not an explicit focus, CYP acknowledges that "treating young people as equal members of society will strengthen social cohesion and help build stronger communities" and "supporting young leaders and encouraging them to be socially and civically engaged will help build an inclusive and resilient nation."[14] CYP points to the Canada Service Corps and the Federal Student Work Experience Program as examples of federal initiatives aimed at increasing youth opportunity.

CYP's main limitations are its overall brevity — the document is merely 16 pages long — and its lack of concrete policy steps to promote youth engagement. The only new commitment CYP introduces is mandating 75 per cent of Crown corporations to have a young person on their boards. CYP largely reframes previous government action and initiatives to make them appear to have been designed with youth engagement in mind. Yet, the initiatives presented therein predate CYP. This is emblematic of a policymaking

approach which has traditionally viewed youth engagement as an afterthought, and not as a core component of policy design. Any federal policy on national resilience will need to include youth engagement as an integral component.

State of Youth Report 2021

The inaugural State of Youth Report (SOYR) analyzes each priority area within the context of the COVID-19 pandemic. The SOYR identifies challenges in healthcare access, leadership and mentorship opportunities, meaningful and long-term employment, and access to skills training as stressors for youth.[15] It is consistent in identifying these as barriers to greater youth engagement in society. Though the age of the publication limits its usefulness as a snapshot of the state of Canadian youth in 2026, it reiterates that the health of youth engagement in society is linked to the ability of youth to participate in society to the fullest.

NATO Ally Case Study

Germany: Tensions with Youth and Conscription

Germany maintained a policy of universal male conscription between 1957 and 2011, with the possibility of alternative civilian service in civil defence organizations including the Federal Agency for Technical Relief and the German Red Cross.[16] In December 2025, Germany took steps towards the reintroduction of male conscription by passing a new federal law on military service establishing a military service questionnaire for all citizens turning 18 years old, which is mandatory for men to complete. Mandatory call-ups to military recruitment centres are planned to be introduced in 2027.[17]

Despite a long history of conscription and national civilian service, these steps towards the reintroduction of conscription have produced some degree of alienation among German youth.[18] By June 2026, five months after the first military service questionnaires were sent out, around 300,000 in number, the German military only recruited 530 new members.[19] Prominent school strikes and youth protests have also emerged since the passage of the law. Though some of these protests are tied to extremist groups, German youth have expressed that they felt left out of high-level debates on conscription and mandatory service.[20]

Germany serves as a cautionary case study that contemporary attempts to introduce conscription, even in NATO countries with long histories of the policy, can result in greater discord among youth than fostering increased resilience. In both Germany and Canada, youth support for conscription is much lower than support from older generations.[21] Youth are skeptical of mandatory service opportunities, and there is little evidence to indicate that mandatory service is a youth-proposed policy. Rather, youth continuously express a desire for opportunities to independently pursue meaningful societal engagement.[22]

Opportunities for Policy Development

Policies to foster greater youth engagement, and indeed broader societal engagement, with national resilience must preserve and prioritize individual agency. Canadians of all ages should be empowered to contribute to national resilience in a manner of their choosing.

The Canada Service Corps is one of the Government of Canada's flagship initiatives in youth engagement, to which CYP also refers.[23] The Canada Service Corps already identifies "strengthening youth resilience" as a salient goal.[24] Instead of becoming the primary provider of youth programming, the Canada Service Corps can become a comprehensive listing of youth programming offered by civil society groups and NGOs. An expanded Canada Service Corps additionally provides the necessary institutional groundwork for any future exploration of a mandatory youth national service scheme.

There are no whole-of-Canada initiatives, measures, or consortia to establish a framework for civil defence education at any level. Civil defence education encompasses digital literacy, first aid training, and measures for active citizenship. Civil defence classes could include sessions on informational resilience, visits by emergency response personnel and local Canadian Armed Forces units, and experiential learning through civil society programs and the Canada Service Corps. Such a partnership should emulate the framework of the Pan-Canadian Joint Consortium for School Health, consisting of representatives of the health and education ministries of all provincial and territorial governments and the Public Health Agency of Canada.[25] For civil defence education, a similar consortium which unites provincial public safety and education ministries with Public Safety Canada should be established.

Civil society studies on youth engagement have repeatedly identified the need to "engage youth where they are" to foster grassroots engagement.[26] A national fund for youth engagement initiatives would fit well into the current heterogenous landscape of Canadian youth engagement. These funds should be available to both youth-led initiatives and existing organizations working with youth, while prioritizing the former in order to centre youth voices and perspectives. Such an approach builds inclusiveness by giving youth agency over their engagement with society and encourages youth to identify with nationally-funded, youth-started initiatives.

Civil Preparedness

Introduction

As the frequency and complexity of security threats continue to evolve, civil preparedness has become an essential component of national resilience. Climate change, cyberattacks, pandemics, and critical infrastructure failures blur the distinction between civilian emergencies and national security challenges. This has required governments to strengthen their ability to anticipate, withstand, respond to, and recover from crises. In Canada, Public Safety Canada defines emergency preparedness as the proactive planning, training, exercising, and coordination[27] undertaken before disasters

occur. These efforts are carried out in partnership with federal, provincial, territorial, and local governments to build safer and more resilient communities. Within NATO, civil preparedness extends beyond emergency management to serve as a critical pillar of collective defence under Article 3 of the North Atlantic Treaty.[28] Recognizing that military effectiveness depends heavily on resilient civilian infrastructure, including energy, transportation, communications, food, and water systems, NATO emphasizes strengthening civilian preparedness as part of its broader defence and deterrence strategy.[29] The Alliance established seven Baseline Requirements for National Resilience at the 2016 Warsaw Summit to guide member states in strengthening their preparedness.[30]

Policy Overview and Evaluation

Canada has taken important steps to strengthen its civil preparedness through the national emergency management initiative,[31] although implementation challenges remain. The Emergency Management Strategy for Canada: Toward a Resilient 2030 establishes a whole-of-society approach to resilience.[32] It outlines federal, provincial, and territorial priorities for improving risk assessment, prevention and mitigation, preparedness, response, and recovery. The strategy also emphasizes stronger collaboration among governments, Indigenous communities, and civil society.[33] Complementing this framework, Canada's National Disaster Mitigation Strategy emphasizes that mitigation measures reduce the human, economic, and infrastructure costs associated with increasingly frequent natural disasters.[34] The strategy prioritizes leadership and coordination, public awareness, research, and sustained mitigation investments to foster resilient communities before disasters occur.[35] Together, these initiatives demonstrate Canada's commitment to strengthening resilience; however, NATO's civil preparedness is needed for a more resilient nation. Public Safety Canada's 2026-2027 Departmental Plan[36] highlights persistent gaps in Canada's national security and resilience objectives. Several departmental performance indicators remain below their targets, requiring Canada to strengthen its security measures. For instance, public confidence that the Government of Canada respects individual rights while ensuring national security remains below the department's 70 percent target[37], while part satisfaction with Public Safety Canada's policy leadership and operational coordination has also fallen short. These gaps reinforce the need to strengthen Canada's civil preparedness capabilities with NATO's resilience framework.

Assessment of NATO's Baseline Requirements

The following analysis assesses Canada's Civil preparedness by examining its performance against NATO's 2016 Baseline Requirements for National Resilience. It encompasses an evaluation of current capabilities, an identification of gaps, a comparison of Canada's approach with those of NATO Allies, and policy recommendations to strengthen national resilience.

Baseline Requirement 1: Assured Continuity of Government & Critical Government Services

NATO's first Baseline Requirement for National Resilience emphasizes the ability of

governments to maintain essential functions during crises, including the capacity to make timely decisions, communicate with citizens, and ensure the continuity of critical public services. In Canada, continuity of government is primarily supported through emergency management structures led by Public Safety Canada. The Government Operations Centre serves as the federal government's central coordination hub for national emergencies,[38] providing constant situational information, facilitating information-sharing between federal departments and agencies, and coordinating responses between provincial, territorial, and other stakeholders during events of national significance. These capabilities Canada's ability to sustain government services during prolonged crises depends heavily on the capacity of existing departments.

Canada also maintains systems to communicate critical information to the public during emergencies through the National Public Alerting System (NPAS), known as Alert Ready. The system enables federal, provincial and territorial authorities to issue emergency alerts concerning immediate threats to life and safety, through wireless devices, television, and radio.[39] Despite these existing capabilities, Canada faces several gaps in meeting NATO's expectations for civil preparedness. Canada's emergency management system follows a decentralized model where municipalities and provinces respond first, with federal assistance provided when local resources are overwhelmed. While this approach allows responses to be tailored to regional needs, it faces increased challenges when multiple jurisdictions face simultaneous emergencies or when disasters exceed provincial capacity. The increasing frequency of wildfires, floods, and other climate-related disasters has placed additional pressure on national response capabilities. In these circumstances, the Canadian Armed Forces have become a critical component of domestic emergency response through Operation LENTUS, which provides military assistance during national disasters when requested by provincial or territorial authorities.[40] Operation LENTUS has supported responses to wildfires, floods, ice storms, and other emergencies by providing personnel, equipment, and logistical support to affected communities. However, reliance on military resources for domestic disaster responses highlights a key vulnerability in Canada's civil preparedness framework. **Canada lacks a dedicated federal civilian disaster response force comparable to NATO Allies that maintain broader civil defence structures and reserve emergency response capabilities.**

Both Canada and Finland demonstrate a commitment to maintaining continuity of government[41] and essential services during crises, however, their approaches differ significantly. While Canada has developed effective mechanisms through systems like Alert Ready and increased military involvement during crises, Finland's Comprehensive Security Model requires all levels of society to contribute to national resilience. A key example of Finland's system of mandatory preparedness planning across government ministries and critical sectors,[42] where authorities, businesses, and organizations are assigned responsibilities for maintaining vital societal functions during disruptions. Finland also maintains a National Emergency Supply Agency, which coordinates security of supply by working with private-sector partners, such as companies connected to electricity and fuels, food and water, transport, and other critical

infrastructure[43] to maintain essential goods, energy supplies, technology, and infrastructure resilience during emergencies. These mechanisms, among others, allow Finland to maintain continuity of government and essential services through a proactive approach, whereas Canada's system remains more focused on coordinating responses after crises occur. Canada must expand civilian emergency management capabilities by investing in dedicated response personnel and strengthening continuity planning across government institutions.

Baseline Requirement 2: Resilient Energy Supply

NATO's second Baseline Requirement for National Resilience emphasizes the importance of ensuring reliable energy supplies and maintaining contingency measures to manage disruptions. Energy resilience is a critical component of civil preparedness because modern societies depend on energy sources to maintain essential services, including healthcare, transportation, communications, and emergency response systems. NATO recognizes that Allies must not only possess sufficient energy capacity but also develop backup plans, protect critical energy infrastructure, and reduce vulnerabilities[44] that could arise from geopolitical instability, cyberattacks, natural disasters, or supply chain disruptions. Canada benefits from substantial energy resources and remains a major global producer of oil, natural gas, and electricity. However, unlike several NATO Allies, Canada does not maintain a federally controlled strategic energy reserve of emergency oil stockpiles,[45] instead relying on domestic production, commercial inventories, and market mechanisms. This creates vulnerabilities during prolonged disruptions affecting supply chains. Canada's decentralized energy governance, where provinces maintain significant authority over energy systems,[46] also presents coordination challenges during national emergencies.

Norway provides a valuable comparison for Canada under NATO's second Baseline Requirement on resilience energy supplies. As a major energy-producing NATO ally, Norway demonstrates how energy security can be strengthened through both reliable supply management and broader civil preparedness planning. Following disruptions in European energy markets after Russia's full-scale invasion of Ukraine, Norway has increased its focus on maintaining stable oil and natural gas production while protecting critical energy infrastructure[47] that supports both domestic needs and European energy security. They have collaborated with various stakeholders to increase energy policy and civil preparedness, which has allowed Norway to maintain continuity of essential services during crises. Additionally, Norway's Total Defence approach integrates civilian and military resources to ensure that critical sectors can continue operating during major crises.[48] This model is coordinated between civilian authorities, such as the Norwegian Directorate for Civil Protection, and defence institutions, allowing civilian capabilities and military resources to support one another during major emergencies. This highlights the importance of cooperation between government institutions, private-sector actors, and infrastructure operators in maintaining essential services. Compared to Canada, which benefits from significant energy resources, but lacks a federal strategic energy reserve, Norway demonstrates how energy-producing states can strengthen resilience through coordinated planning, infrastructure protection, and crisis preparedness.

Baseline Requirement 6: Resilient Civil Communications Systems

NATO's sixth Baseline Requirement for National Resilience emphasizes the importance of ensuring that telecommunications and cyber networks can continue operating during crises. Reliable communications systems are essential for maintaining government operations, emergency response, public safety, and the delivery of critical services. NATO highlights the need for resilient telecommunications infrastructure, secure 5G networks, backup capacity, and the ability to rapidly restore communications[49] following disruptions caused by cyberattacks, physical damage, or other emergencies.

Canada has developed important measures to strengthen communications resilience, recognizing telecommunications networks as critical infrastructure that support essential government, economic, and public services. The National Cyber Security Strategy identifies the protection of critical digital systems as a national priority and regards cooperation[50] between government, industry, and infrastructure operators as essential to reduce cyber risks. Canada has also taken steps to improve the security of its 5G networks by restricting the use of equipment from high-risk vendors,[51] including Huawei and ZTE, due to concerns related to national security and potential vulnerabilities within telecommunications infrastructure. Despite these measures, gaps remain in Canada's ability to ensure communications continue during large-scale disruptions. Canada's telecommunications networks are primarily operated by private-sector companies, creating dependencies on commercial infrastructure during emergencies. This leads to a vulnerability with cyber security, and while cyber security regulations provide protection, NATO requires the ability to maintain communications through backup systems and rapid restoration capabilities. A major disruption affecting telecommunications networks, power systems, or digital infrastructure could impact emergency response and government communication.

The Netherlands provides a comparison for Canada's approach to resilient civil communications systems through its C2000 emergency communications network. C2000 is a dedicated national digital communication system used by police, fire services, ambulance services, the Ministry of Defence, and other emergency organizations.52 The system allows emergency responders to communicate securely with one another and with control centres during daily operations, major incidents, and disasters. Unlike standard commercial networks, C2000 is designed specifically for emergency services and remains available during periods of high demand,[53] providing reliable communications when public networks are overrun. Compared with Canada's reliance on privately operated telecommunications networks, the Dutch model highlights the value of maintaining specialized emergency communications systems that provide security and assurance when conventional networks experience disruption. Strengthening Canada's alignment with NATO's sixth Baseline Requirement will require continued investment in telecommunications systems and emergency restoration capabilities.

Baseline Requirement 7: Resilient Transport Systems

NATO's seventh Baseline Requirement for National Resilience emphasizes the need for transportation systems that can support both civilian needs and defence requirements during crises. Allies must ensure that roads, railways, ports, and air networks remain functional services to continue enabling the rapid movement of NATO forces across Alliance territory.[54] Resilience transportation systems are a critical component of civil preparedness as they allow governments, emergency responders, and communities to maintain essential functions during disasters.

Canada has significant transportation capabilities that support both civilian resilience and national defence requirements. The CAF depends on civilian transportation infrastructure, including airports, railways, highways, and ports to support domestic operations and meet NATO commitments.[55] Canada's defence policy recognizes the importance of infrastructure readiness for the movement of personnel and equipment during emergencies and military operations. However, Canada faces vulnerabilities due to its geography and dependence on key transportation corridors. For instance, the 2021 British Columbia floods severely damaged highways and rail infrastructure,[56] disrupting the movement of goods.. This vulnerability demonstrates the significance of transportation resilience as a civil preparedness concern.

Germany provides a comparison for Canada due to its central role in NATO military mobility and its transportation infrastructure. As a key transit country for NATO forces, Germany has invested in improving its roads, railways, and infrastructure networks[57] to support the rapid movement of allied forces while maintaining civilian needs. This approach highlights the importance of integrating civilian infrastructure planning with defence requirements, ensuring that transportation systems can support both everyday societal functions and crisis response. This provides a lesson for Canada, where vast distances and limited transportation corridors create challenges for moving resources and responding to emergencies. Strengthening alternative routes, improving infrastructure resilience and increasing coordination between civilian transportation authorities and defence organizations would help Canada reach NATO's seventh Baseline Requirement.

Recommendations

Canada has developed important capabilities in emergency management, critical infrastructure protection, and national resilience. However, comparisons with NATO Allies demonstrate several areas where additional investment can strengthen Canada's ability to meet NATO's Civil Preparedness Baseline Requirements. The following recommendations aim to improve Canada's resilience by addressing gaps:

1. Create a national strategic energy resilience framework, including contingency reserves, and stronger coordination with energy providers
    a) To ensure continuity of essential energy supplies during major disruptions
2. Develop a dedicated emergency communications network for first responders and government authorities.

a) To ensure reliable communication during crises when commercial telecommunications systems are disrupted

3. Integrate climate risks into civil preparedness planning

a) To ensure that infrastructure investments account for increasing threats from floods, wildfires, extreme weather, and other climate-related disruptions.

Munn, Conor R.G. "Member of Canadian Cadet Organization participates as a flag bearer during the rehearsal of the closing ceremony of Invictus Games Vancouver Whistler 2025 at Rogers Arena, Vancouver, British Columbia on 15 February 2025." Canadian Forces Combat Camera / Canadian Armed Forces Photo, February 15, 2025. https://www.combatcamera.forces.gc.ca/gallery/cc_photos/detail/?filename=20250215ETF0050D001&assetId=1600207.

I"SJ52-2019-0058-063." Canadian Forces Combat Camera / Canadian Armed Forces Photo, n.d. https://www.combatcamera.forces.gc.ca/gallery/cc_photos/detail/?filename=SJ52-2019-0058-063&assetId=211102. Accessed September 14, 2026.

Endnotes:

1. House of Commons Standing Committee on Procedure and House Affairs, "Current State of Civic Resilience in Canada," House of Commons of Canada, April 23, 2026. https://www.ourcommons.ca/committees/en/PROC/StudyActivity?studyActivityId=13387543.
2. Laura Stephenson et al., "Understanding and Advancing Youth Civic Engagement in Canada," 6–8, in Youth Civic Engagement in Canada: A Study in Three Parts (Max Bell Foundation, 2025). https://www.maxbell.org/wp-content/uploads/2025/07/Youth-Civic-Engagement-in-Canada-A-Study-in-Three-Parts-ENGLISH.pdf.
3. B. Guy Peters and Jon Pierre, "A Typology of Populism: Understanding the Different Forms of Populism and Their Implications," Democratization 27 (6) (2020): 928. https://doi.org/10.1080/13510347.2020.1751615; James A. Piazza, "Politician Hate Speech and Domestic Terrorism." International Interactions 46 (3) (2020): 435–437, 442–443. https://doi.org/10.1080/03050629.2020.1739033.
4. "Volunteering and charitable giving in Canada, 2018 to 2023," Statistics Canada, June 23, 2026. https://www150.statcan.gc.ca/n1/daily-quotidien/250623/dq250623b-eng.htm.
5. State of Youth Report Youth Advisory Group, Canada's first State of Youth Report: For youth, with youth, by youth (Department of Canadian Heritage, 2021), 82. https://www.canada.ca/en/canadian-heritage/campaigns/state-youth/report.html#a10d.
6. Stephenson et al., "Understanding Youth Engagement," 18, 31–34, 20–21.
7. Ibid, 18–19.
8. Namely: Croatia, Denmark, Estonia, Finland, Greece, Latvia, Lithuania, Norway, Sweden, and Turkey; Patrick Jackson and Emma Brancatisano, "Which European countries have mandatory or voluntary military service," BBC News, December 5, 2025. https://www.bbc.com/news/articles/cvgj4npzp53o.
9. Rudy Yuan, "Conscription if necessary? Learnings for Canada from Germany's reintroduction of conscription," NATO Association of Canada, October 17, 2025. https://natoassociation.ca/conscription-if-necessary-learnings-for-canada-from-germanys-reintroduction-of-conscription/.
10. "Canada's Youth Policy," Government of Canada, 2019, 16. https://www.canada.ca/content/dam/y-j/documents/YP-ENG.pdf.
11. Stephenson et al., "Understanding Youth Engagement," 18, 26.
12. Ibid, 19–21.
13. Ibid, 43–60.
14. "Canada's Youth Policy," 7, 10.
15. Youth Advisory Group, "State of Youth Report."
16. "Wie funktioniert die Wehrpflicht?" [How does conscription work?] Bundeszentrale für politische Bildung, December 8, 2025. https://www.bpb.de/kurz-knapp/hintergrund-aktuell/550475/wie-funktioniert-die-wehrpflicht/.

Endnotes:

17. "Neuer Wehrdienst: Freiwilliger Einsatz für Deutschlands Sicherheit," [New military service: Voluntary commitment for Germany's security] Bundeswehr, n.d., accessed August 23, 2026. https://www.bundeswehr.de/de/menschen-karrieren/neuer-wehrdienst; "Was das neue Gesetz zum Wehrdienst vorsieht," [What the new law on military service stipulates] Tagesschau, August 27, 2025. https://www.tagesschau.de/inland/innenpolitik/faq-wehrdienst-100.html.
18. Ben Knight, "German high school students protest against military service," Deutsche Welle, May 3, 2026. https://www.dw.com/en/german-high-school-students-protest-against-military-service/a-76236452.
19. Eva Maria Braungart, "Bundeswehr verschickt 300.000 Fragebögen: Bisher nur 530 Freiwillige rekrutiert," [Bundeswehr sends out 300,000 questionnaires: Only 530 volunteers recruited to date] Berliner Zeitung, June 25, 2026. https://www.berliner-zeitung.de/article/neuer-wehrdienst-bundeswehr-rekrutierung-10131951.
20. Martin Bieber, "Jugendproteste gegen den Wehrdienst," [Youth protests against military service] Konrad-Adenauer-Stiftung, December 18, 2025. https://www.kas.de/de/kurzum/detail/-/content/jugendproteste-gegen-den-wehrdienst.
21. Yuan, "What Canada can learn from Germany's conscription."
22. Youth Advisory Group, "State of Youth Report," 46–50, 56–57.
23. "Canada's Youth Policy," 10.
24. "About the Canada Service Corps," Government of Canada, July 29, 2024. https://www.canada.ca/en/services/youth/canada-service-corps/about.html.
25. "About Us," Joint Consortium for School Health, n.d., https://www.jcsh-cces.ca/en/about-us/. Accessed August 23, 2026.
26. Stephenson et al., "Understanding Youth Engagement," 71.
27. Public Safety Canada, "Emergency Preparedness," Government of Canada, July 28, 2026. https://www.publicsafety.gc.ca/cnt/mrgnc-mngmnt/mrgnc-prprdnss/index-en.aspx
28. Ibid.
29. Ibid.
30. NATO, "Resilience, Civil Preparedness and Article 3," North Atlantic Treaty Organization, https://www.nato.int/en/what-we-do/deterrence-and-defence/resilience-civil-preparedness-and-article-3
31. Public Safety Canada, "Emergency Management Strategy for Canada: Toward a Resilient 2030," Government of Canada, https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/mrgncy-mngmnt-strtgy/index-en.aspx
32. Ibid.
33. Ibid.
34. Public Safety Canada, "National Disaster Mitigation Strategy," Government of Canada, https://www.publicsafety.gc.ca/cnt/mrgnc-mngmnt/dsstr-prvntn-mtgtn/ntnl-dsstr-mtgtn-strtg-en.aspx
35. Ibid.

Endnotes:

36. Public Safety Canada, "Departmental Plan 2026–27," Government of Canada, https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/dprtmntl-pln-2026-27/index-en.aspx#a3.1
37. Ibid.
38. Public Safety Canada, "Government Operations Centre," Government of Canada, https://www.publicsafety.gc.ca/cnt/mrgnc-mngmnt/rspndng-mrgnc-vnts/gvrnmnt-prtns-cntr/index-en.aspx
39. Environment and Climate Change Canada, "Alert Ready Emergency Alert System," Government of Canada, https://www.canada.ca/en/environment-climate-change/services/weather-general-tools-resources/alert-ready-emergency-system.html
40. Department of National Defence, "Operation LENTUS," Government of Canada, https://www.canada.ca/en/department-national-defence/services/operations/military-operations/current-operations/operation-lentus.html
41. Andrew McDougall, "Continuity of Constitutional Government during a Pandemic: Considering the Concept in Canada's Emergency Management Act," Canadian Journal of Political Science 53, no. 2 (2020): 293–98, doi: 10.1017/S0008423920000293; Jarmo Laine, "Parliamentarism in Finland," ThisisFINLAND, April 2015, last edited June 2019, https://finland.fi/life-society/parliamentarism-in-finland/
42. Finnish Government, "Preparedness, Security and Situation Awareness," https://valtioneuvosto.fi/en/preparedness-security-and-situation-awareness
43. National Emergency Supply Agency, "The National Emergency Supply Agency," https://www.huoltovarmuuskeskus.fi/en/organisation/the-national-emergency-supply-agency
44. North Atlantic Treaty Organization, "Resilience, Civil Preparedness and Article 3," https://www.nato.int/en/what-we-do/deterrence-and-defence/resilience-civil-preparedness-and-article-3
45. International Energy Agency, "Canada Oil Security Policy," https://www.iea.org/articles/canada-oil-security-policy-2
46. International Energy Agency, Canada 2022: Energy Policy Review, 2022, https://www.iea.org/reports/canada-2022
47. Felicity Bradstock, "Norway Doubles Down on Oil and Gas as Europe Scrambles for Supply," OilPrice.com, May 23, 2026, https://oilprice.com/Energy/Energy-General/Norway-Doubles-Down-on-Oil-and-Gas-as-Europe-Scrambles-for-Supply.html
48. Norwegian Directorate for Civil Protection, "Total Defence," https://www.dsb.no/en/risk-vulnerability-and-preparedness/Total-Defence/
49. North Atlantic Treaty Organization, "Resilience, Civil Preparedness and Article 3," https://www.nato.int/en/what-we-do/deterrence-and-defence/resilience-civil-preparedness-and-article-3

Endnotes:

50. Public Safety Canada, "National Cyber Security Strategy," Government of Canada, https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/index-en.aspx
51. Innovation, Science and Economic Development Canada, "Policy Statement—Securing Canada's Telecommunications System," Government of Canada, May 19, 2022, https://www.canada.ca/en/innovation-science-economic-development/news/2022/05/policy-statement--securing-canadas-telecommunications-system.html
52. Government of the Netherlands, "C2000 Communication System for Emergency Services," https://www.government.nl/themes/justice-security-and-defence/counterterrorism-and-national-security/c2000-communication-system-for-emergency-services
53. Ibid.
54. North Atlantic Treaty Organization, "Resilience, Civil Preparedness and Article 3," https://www.nato.int/en/what-we-do/deterrence-and-defence/resilience-civil-preparedness-and-article-3
55. Department of National Defence, "Canada's Defence Policy," Government of Canada, https://www.canada.ca/en/department-national-defence/corporate/reports-publications/canada-defence-policy.html
56. Senate of Canada, Treading Water: The Impact of and Response to the 2021 British Columbia Floods, https://sencanada.ca/en/info-page/parl-44-1/agfo-treading-water-the-impact-of-and-response-to-the-2021-british-columbia-floods/
57. Konrad Wolfenstein, "Germany as a Military Logistics Hub: The NATO New Force Model: Massive Troops as a New Reality," Xpert.Digital, June 24, 2025, https://xpert.digital/en/massive-troops-as-a-new-reality/