STRATEGIC Outlook

MARCH 2026 · CONFERENCE OF DEFENCE ASSOCIATIONS INSTITUTE

THE ROAD TO FIVE PERCENT 2026

STRATEGIC Outlook

THE ROAD TO FIVE PERCENT

Now in its 94th year, the Ottawa Conference on Security and Defence is Canada's premier defence and national security forum. This year's theme, *The Road to Five Percent*, reflects a defining moment in Canada's history. The federal government's commitment to increase defence spending to five percent of GDP over the next decade will have far-reaching implications for the size, structure, and readiness of the Canadian Armed Forces (CAF), as well as for our country's economy and the future of Canadian society.

The increased investments come at a time of heightened geopolitical tension for Canada and its allies. Great power competition and hostile threats both above and below-the-threshold have placed immense pressure on Canada to safeguard its sovereignty and defend the population. For the first time in decades, the overlap between economic security and national defence is deeply intertwined—underscoring the need for greater strategic autonomy.

Over the last few months, the defence community has sought to seize the moment by ensuring the right capabilities and equipment are acquired in a timely and efficient manner. At the core of this effort is the Defence Industrial Strategy's BUILD-PARTNER-BUY framework, which aims to strengthen Canada's industrial base by expanding domestic production, cementing existing and forming new trading relationships beyond the United States, and acquiring off-the-shelf capabilities when necessary. Canada's defence investments are intended not only to secure an operational advantage over our adversaries, but also to stimulate economic growth and prosperity from coast to coast to coast.

It is in this context that we present the *Strategic Outlook*. This volume brings together seven short essays authored by leading voices from across Canada's defence and security community. Each article touches on a different domain that will impact Canada's defence trajectory in the years ahead.

The volume opens with Fen Hampson examining Canada's "middle power trap" arguing the country faces a double burden: hegemonic tax from U.S. dependence and a geopolitical tax from trade diversification. Jessica West takes on the space domain, contending that Canada's security in orbit depends not on dominance, but on resilience, sustained access, and disciplined risk management. The volume then turns to Kate Todd, who assesses the shift from maritime cooperation to contestation in regions such as the Taiwan Strait, Red Sea, and Arctic, arguing that Canada's aging fleet and limited capacity leave us ill-prepared to defend our interests. Nicholas Glesby focuses on the air domain, looking specifically at next generation missile threats, arguing Canada should become a full and credible partner in the U.S.' Golden Dome initiative. On the land domain, Howard Coombs writes about lessons learned from the Russia-Ukraine War and highlights the importance of adaptive military institutions, resilient logistics, and whole-of-society defence for Canada and its allies. Grey-zone or below-the-threshold threats are captured by Dani Belo who unpacks how society, cyber, and economic vulnerability intersect with competitive multilateralism, suggesting resilience and strategic coalition-building are key to successfully deter our adversaries. Finally, Kristen Csenkey concludes the volume with a discussion on Canada's cyber and technological defence challenges, focusing on AI, quantum risks, and the need for resilience and allied coordination in 2026.

Together, these essays make an important contribution in enhancing public literacy, provoking thoughtful debate, and serving as a complementary scene-setter for the substantive discussions set to take place at the Ottawa Conference.

As Canada forges ahead with historic levels of defence investment, rigorous strategic thinking is essential to ensure that those investments are coherent, effective, and aligned with our enduring national interests. The CDA Institute remains committed to being Canada's preeminent leader in defence thinking—connecting stakeholders across the country, convening events such as the Ottawa Conference, and contributing to the national dialogue through rigorous, evidence-based research and analysis.

I hope you enjoy,

Gaëlle Rivard Pichē
Executive Director, CDA and CDA Institute

ECONOMICS

Canada's Economic Security Dilemma: Trading a Hegemonic Tax for a Geopolitical Tax[1]

Fen Osler Hampson

Prime Minister Mark Carney attends the World Economic Forum in Davos on Jan. 19.
Photo Credit: Sean Kilpatrick / The Canadian Press

Dr. Fen Osler Hampson, FRSC, is the Chancellor's Professor and Professor of International Affairs at Carleton University and Co-Chair, with the Hon. Perrin Beatty, of the Expert Group on Canada-US Relations. A graduate of the University of Toronto, the London School of Economics, and Harvard University, he is a Fellow of the Royal Society of Canada and the author and co-editor of 48 books on Canadian foreign and economic policy, as well as international relations. He is also an Honorary Degree recipient from Trinity College, University of Toronto.

In 2026, Canada finds itself caught in the "middle power trap"[2] —a strategic straitjacket that limits its ability to act independently. As the Carney government pivots from "Reliance to Resilience" to reduce the costs of a punitive *hegemonic tax*—the direct and indirect economic burdens stemming from U.S. market dominance, discretionary protectionism, loss of investment with market uncertainty, and extraterritorial rule-setting—Canadians recognize that trade diversification is not a risk-free strategy. It comes with a significant *geopolitical tax*, reflected in the financial and transactional costs of securing new trade and investment partners overseas, as well as in the added defence burdens to manage maritime instability and intensified geopolitical rivalries along extended supply chains.

This paper highlights the key elements of this economic security dilemma. It provides a framework to show that Canada is trading one set of risks and costs for another to secure its economic future and that Canada's national economic self-determination, as we have historically understood it, is severely constrained.

Tariff Wars and America's Hegemonic Tax

The *hegemonic tax* that Canada currently faces manifests itself in President Trump's weaponization of trade policy against America's northern neighbor. In this paper, *hegemonic tax* refers to the *additional* costs Canada pays by virtue of relying on a single, politically volatile hegemon for market access, security guarantees, and regulatory alignment, over and above the normal frictions of trade.

Trump's imposition of tariffs on Canadian steel, aluminum, and other strategic goods is not simply a trade dispute but a fundamental assault on the economic architecture that has sustained Canadian prosperity for generations. The United States accounts for approximately 75 percent of Canada's exports and roughly a quarter of its GDP, making Canada particularly vulnerable to American protectionist measures.[3] When Trump threatened 25 percent tariffs on all Canadian goods in early 2025, his message was unambiguous: Canada's economic prosperity is in jeopardy and subject to the president's whim. The economic impact of Trump's tariffs extends beyond immediate costs in job losses and business closures to include the chilling effect on investment, the disruption of decades-long integrated supply chains, and the broader economic and psychological toll of uncertainty about market access to Canada's major trading partner.

The precarious state of CUSMA renewal negotiations compounds this vulnerability. Trump has repeatedly signaled his willingness to abandon or fundamentally restructure CUSMA if it does not serve immediate American interests as he defines them. The agreement's built-in 2026 review mechanism is a sword of Damocles hanging over Canada's economic future. Businesses that hitherto were willing to invest in building new production facilities and supply chains have been frightened off by the prospect that a single presidential decree or a failed renegotiation could give us a "zombie deal" that would strand their investments. This uncertainty also constitutes a form of economic taxation, as risk premiums rise and investment horizons shrink in response to an increasingly unstable political and regulatory environment.[4]

The "Donroe Doctrine" is perhaps the most insidious dimension of the *hegemonic tax* that Canada now confronts.[5] This framework of American hemispheric assertiveness suggests Canada is not a sovereign partner but subordinate to an American-dominated continental system. Under this doctrine, American national security prerogatives override Canadian sovereignty in matters ranging from immigration policy to resource extraction to technology standards.[6] The doctrine implicitly means that Canada and other Western Hemisphere countries will have to align their domestic economic and foreign policies with America or face economic retaliation.

Taken together, tariff warfare, CUSMA review risk, and the Donroe Doctrine constitute the three main components of this *hegemonic tax*: pricebased penalties, uncertainty premiums, and sovereignty discounts.

This tax is not static, but dynamic and rising, as American protectionism intensifies and the Trump administration's willingness to use economic coercion as a foreign policy tool becomes more pronounced. Canada cannot indefinitely absorb these costs without severe economic consequences, including reduced investment, slower productivity growth, and diminished living standards.

The *hegemonic tax* has transformed the Canada-U.S. economic relationship from a source of prosperity into one of ongoing vulnerability. It is forcing Canadian policymakers to contemplate what was unthinkable even a decade ago: a fundamental reorientation of Canada's trade and investment ties away from its southern neighbor.

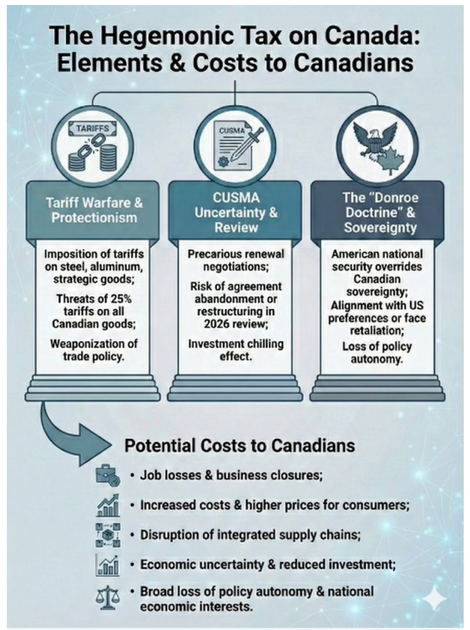

Figure 1

Trade Diversification

Mark Carney's trade and investment diversification strategy represents the government's response to this *hegemonic tax*, an attempt to reduce Canada's overreliance on the American market by cultivating alternative trade and investment relationships across the globe.[7]

The strategy rests on several pillars designed to enhance Canada's economic resilience and strategic autonomy. First, it prioritizes deepening existing trade relationships with the European Union, particularly Germany, France, and the Nordic countries that share Canada's values of multilateralism and a rules-based international order. The Comprehensive Economic and Trade Agreement (CETA) with the EU and the Canada-EU Defence and Security Partnership provide the framework for this expansion, which aims to establish deeper commercial ties, joint research initiatives, and integrated supply chains in strategic sectors, including defence procurement, clean technology, critical minerals, and advanced manufacturing.[8]

Second, the strategy emphasizes expanding trade with Canada's Indo-Pacific partners, particularly Japan, South Korea, Australia, and India. These relationships offer several advantages: significant market size and purchasing power, strong rule-of-law traditions that reduce regulatory risk, and shared concerns about Chinese economic coercion and American unpredictability. The Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) provides the foundation for many of these relationships. However, the Carney government seeks to move beyond this multilateral framework to establish bilateral partnerships that address specific Canadian export diversification needs, particularly in energy, agriculture, technology, and manufacturing. Japan's interest in Canadian liquefied natural gas, South Korea's demand for Canadian agricultural and higher agrifood products, and China's and India's demand for energy create synergies that the diversification strategy aims to exploit.[9]

Third, the diversification strategy includes a vital domestic component focused on reducing interprovincial trade barriers and regulatory fragmentation that make Canada, in effect, a series of separate small markets rather than a unified national economy. The strategy recognizes that Canada cannot effectively compete globally if Canadian companies face more obstacles to selling goods and services across provincial boundaries than they do internationally. Initiatives to harmonize regulations, mutual recognition of professional credentials, and the elimination of non-tariff barriers to interprovincial commerce are essential to making Canada an attractive platform for global investment.[10]

Finally, the Carney strategy emphasizes investment diversification alongside trade diversification by seeking to attract capital from a broad range of foreign sources while ensuring that strategic assets remain under Canadian control. This includes establishing investment partnerships with sovereign wealth funds from friendly nations, creating co-investment vehicles for critical infrastructure, and using government procurement policy to build domestic capacity in strategic sectors.[11] The strategy recognizes that trade diversification and investment diversification are both necessary for economic growth and reduced vulnerability.[12]

The Geopolitical Tax

The government's diversification strategy, however necessary and well-conceived, comes with a hefty *geopolitical tax*: the new economic, security, and governance costs Canada must pay to sustain diversified trade and investment relationships beyond the continental U.S. system. The most immediate dimension of this *geopolitical tax* involves the physical and financial challenges of trading across oceans rather than across a land border. Canadian goods destined for Asian or European markets must travel thousands of kilometers by sea, incurring substantial transportation costs and time delays as compared to the far shorter route to the U.S. market. These distance penalties for both exports and imports are not trivial: shipping costs add substantially to the delivered price of goods, while transit times measured in weeks rather than days complicate just-in-time production processes and increase inventory costs. The infrastructure investments required to facilitate this expanded overseas trade—upgraded port facilities, increased container capacity, improved rail connections to ports—represent significant capital costs that ultimately must be borne by taxpayers and/or passed on to consumers.[13]

In other words, the geopolitical tax is the premium Canada pays to substitute longer, riskier, and more politically exposed global supply chains for a single, proximate hegemonic market.

The security of maritime trade supply routes presents an even more formidable dimension of the *geopolitical tax*. As Canada shifts trade toward Asia and Europe, it becomes dependent on sea lanes that traverse some of the world's most contested waters. The South China Sea, through which much of Canada's trade with Asia must pass, is subject to competing territorial claims and to increasing Chinese naval assertiveness. The Strait of Malacca, a critical chokepoint for trade between the Indian and Pacific Oceans, is vulnerable to piracy, terrorism, and a potential blockade. The Taiwan Strait could become a flashpoint that disrupts Canadian trade flows. Even North Atlantic routes to Europe and our own Arctic waters, traditionally secure, face growing challenges from Russian submarine activity and potential harassment of commercial shipping in a deteriorating security environment.[14]

Securing these extended global supply chains requires extensive military and intelligence capabilities that Canada has allowed to atrophy over many decades. Operating a credible naval presence across three oceans, maintaining maritime domain awareness through satellite and surveillance systems, establishing secure communications with commercial vessels, and developing the capacity to respond to threats against Canadian shipping all require substantial defense investments. Canada's current naval capabilities are inadequate for this expanded role: the Royal Canadian Navy operates just twelve frigates and four submarines, a force structure designed for coastal defense and North Atlantic operations, not for protecting global supply chains. Billions in capital and operating spending will be required to develop Canada's maritime and undersea capabilities.[15] However, the precise amounts will depend on final decisions about the surface combatant fleet size, submarine replacement, and adoption of autonomous systems.[16]

These required defence outlays are not discretionary add-ons; they are the security component of the *geopolitical tax* that must be paid upfront if diversification is to be credible rather than purely rhetorical.

Beyond physical security, the *geopolitical tax* includes the regulatory and political complexities of doing business in diverse markets with different legal systems, business practices, and political risks.[17] Each of these challenges imposes costs in the form of legal fees, compliance expenses, risk management, and the opportunity cost

of management time diverted to navigating foreign regulatory systems. These frictions are a regulatory surcharge on each transaction Canadian firms conduct in diversified markets, in effect a hidden but significant component of the *geopolitical tax*.[18]

Canadian exporters also face monopsony risk when a single market, such as China for canola or other commodities, becomes dominant enough to dictate prices or weaponize trade access in response to political disagreements. Diversifying trade relationships can mitigate this exposure, but substituting one dependency for another merely changes the source of vulnerability without reducing it. China's ability to weaponize market access and investment turns every major export contract or greenfield project into a potential geopolitical liability, adding a strategic dependence premium to the *geopolitical tax*.

Beyond market concentration, other costs emerge from China's state-directed industrial policy, i.e., the risk of product dumping into the Canadian market, particularly as Chinese firms lose access elsewhere. This poses a direct threat to domestic producers and high-value manufacturing jobs. On the investment side, Canada must balance the economic benefits of Chinese capital inflows with the security risks of allowing foreign influence in strategic sectors such as critical minerals and advanced technologies. Together, these pressures, along with the potential reputational costs of getting too close to authoritarian regimes, impose a significant *geopolitical tax* on Canada manifested in constrained strategic choices, higher compliance and risk management costs, and potentially the long-term erosion of economic independence.[19]

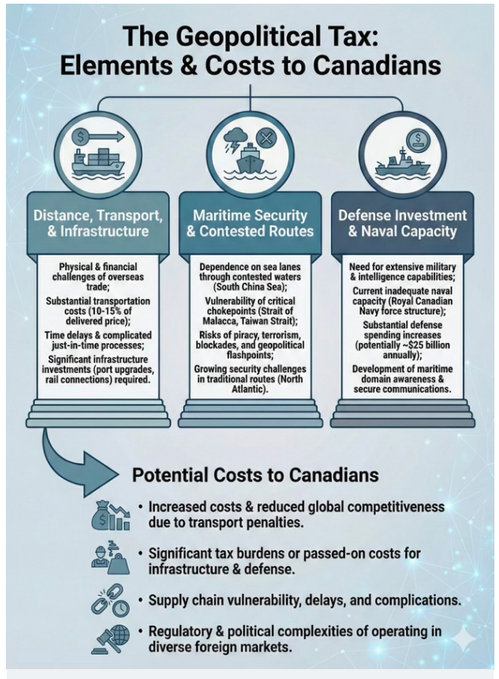

Figure 2

Canada's internal divisions compound the challenges of implementing an effective diversification strategy. Provincial governments jealously guard their constitutional prerogatives over natural resources and economic development, often pursuing contradictory trade and investment policies that undermine federal strategy. These internal tensions represent a self-imposed dimension of the *geopolitical tax*, as political fragmentation will prevent Canada from effectively realizing its full economic potential.

Integrating Security Policy with Economic Policy

As trade shifts away from the United States, national security policy must be integrated into Canada's trade policies and commercial agreements. Economic statecraft becomes inseparable from defense policy when supply chains cross contested sea lanes and traverse regions of geopolitical competition. Canada must expand intelligence sharing and maritime domain awareness with its partners, including Japan, South Korea, and the European Union, to ensure security of supply. This means participating in multilateral maritime security initiatives, sharing satellite intelligence on shipping movements, and contributing naval assets to coalition operations protecting sea lanes. The era of treating trade policy and defense policy as separate domains must end, replaced by integrated national security planning that recognizes economic and military security as mutually reinforcing.

As Canada moves away from U.S.-centric supply chains, its ports, transportation corridors, telecommunications networks, and energy grids will become increasingly attractive targets for adversaries seeking to disrupt them. This will require significant investments in cybersecurity, physical security, and redundancy for systems essential to economic resiliency.

Foreign investment screening must also evolve to reflect these new realities. A more effective use of the Investment Canada Act is required to encourage foreign investment while simultaneously preventing state-owned enterprises from hostile regimes from controlling the development of critical resources and infrastructure. The goal is not economic nationalism for its own sake but ensuring that Canada retains control over assets vital to its economic security.

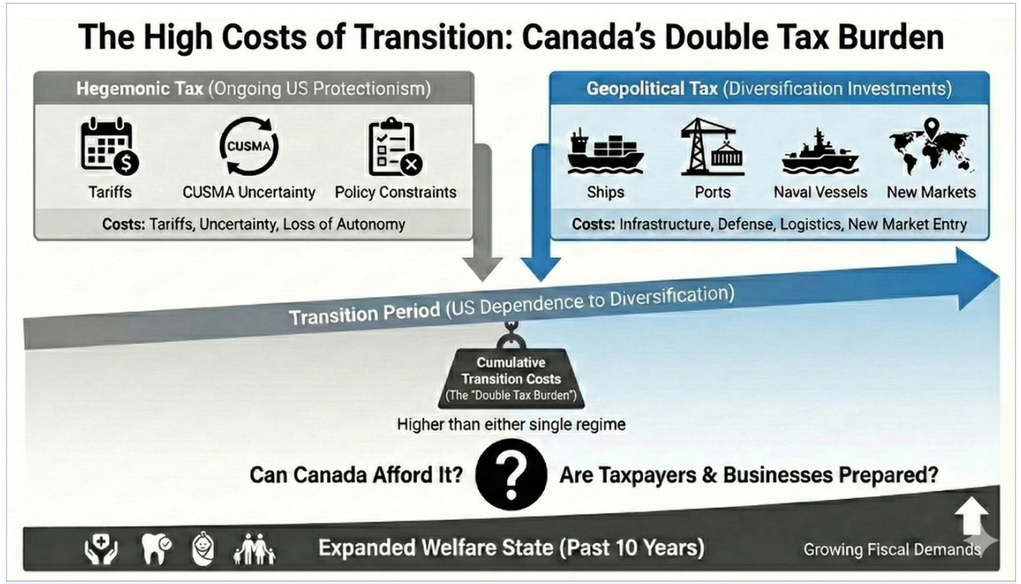

Figure 3

The Double Tax Burden

The transition from a primary reliance on the United States toward a more diversified global trade and investment strategy presents its own formidable fiscal and structural challenges. Canada thus faces a double tax burden: a *hegemonic tax* levied by dependence on a single, unpredictable superpower, and a *geopolitical tax* associated with the costs of building and securing a diversified network of alternative trading partners. These latter costs involve massive investments in maritime infrastructure, global supply chain security, and a significant expansion of naval and defense capabilities. During the transition, however, Canadian taxpayers and firms will pay *both* taxes simultaneously: higher risk premiums and sovereignty costs in the U.S. market, and substantial capital, security, and governance premiums in new markets. Ultimately, this raises a critical question regarding national capacity: at a time when the welfare state has expanded significantly over the last decade, can the Canadian economy, its taxpayers, and its business community afford the massive fiscal demands and prolonged uncertainty inherent in such a fundamental reorientation of its global standing? This is not just Hobson's choice; it is the illusion that we lack any real choices at all.

Conclusion

Ultimately, Canada's strategic position in 2026 reflects the dissolution of the post-Cold War liberal international order that provided the framework for Canadian prosperity. That order, characterized by open markets, rules-based dispute resolution, and American security guarantees, allowed Canada to prosper as a trading nation without bearing the full costs of securing its own economic interests and its own defence. As that order fragments under the pressure of great power competition, populist nationalism, and American abdication of its traditional leadership role, Canada must adapt to a harsher environment where economic security requires military capacity, where trade relationships demand new political alignments, and where prosperity cannot be achieved without incurring major new costs. The transition is not from dependency to autonomy but from one strategic constraint to another. Whether Canada emerges from this transition with its prosperity and sovereignty intact will depend on the wisdom of its leaders, the resilience of its institutions, and the willingness of its citizens to bear the costs of a more uncertain world.

Notes

1 The author would like to thank the Hon. Perrin Beatty, Lawrence Herman, Vincent Rigby, and Tim Sargent for their helpful comments on this paper.

2 The term has been used by a variety of scholars to describe the different structural dilemmas experienced by so-called “middle powers.” See, for example, João Paulo Nicolini Gabriel who coined the term in his doctoral thesis, “The Middle Power Trap and the Struggle for Status: How the Nonproliferation Regime Hampered the Aspirations of Emerging Regional Powers” (PhD thesis, Universidade Federal de Minas Gerais, 2023), https://repositorio.ufmg.br/handle/1843/68117; Chris Alden et al., “Shaping a New World? Middle Powers and Global Governance,” Policy Center for the New South, May 13, 2025, https://www.policycenter.ma/publications/shaping-new-world-middle-powers-and-global-governance ; Yaroslav Lissovolik, “The ‘Golden Middle’ of the World Economy,” BRICS+ Analytics, September 16, 2025,

https://brics-plus-analytics.org/the-golden-middle-of-the-world-economy/; “Can Canada Afford to Choose Between the U.S. and China?,” McGill Journal of Political Studies, February 4, 2026,

https://www.mjemcgill.com/articles/2phhznteukp35slc9qo469k1bb5sfw; “Hanwha’s Overreach Shows How to Misplay US–China Power Game,” Asia Times, October 31, 2025, https://asiatimes.com/2025/11/hanwhas-overreach-shows-how-to-misplay-us-china-power-game/.

3 Expert Group on Canada–US Relations, Broken Trust: Managing an Unreliable Ally (Ottawa: Carleton University, Norman Paterson School of International Affairs, and Canadian Global Affairs Institute, 2025), https://carleton.ca/npsia/wp-content/uploads/Broken-Trust_Report_Embargoed-until-Tuesday-April-1-202572355341.pdf.

4 For the 2026 review clause and potential termination if no extension is agreed, see Joshua P. Meltzer, “2026 CUSMA Review,” Brookings Institution, June 17, 2024, https://www.brookings.edu/articles/2026-cusma-review/; on the design of the review mechanism and the risk of serial annual reviews creating prolonged uncertainty, see Christopher Sands et al., “USMCA Review 2026,” Center for Strategic and International Studies, August 17, 2025, https://www.csis.org/analysis/usmca-review-2026; on Trump’s threats to allow USMCA/CUSMA to lapse or withdraw from it, see “U.S. Businesses Love CUSMA. Why Is Donald Trump Threatening to Pull Out?,” CBC News, December 6, 2025, https://www.cbc.ca/news/world/trump-tariffs-canada-us-mexico-agreement-cusma-usmca-trade-9.7004814; Grant Thornton, “Trump Administration Sets Table for USMCA Rewrite in 2026,” December 22, 2025, https://www.grantthornton.com/insights/newsletters/tax/2025/hot-topics/dec-23/trump-administration-sets-table-for-usmca; and on how this uncertainty is already depressing investment and raising risk premiums for North American supply chains, see “Canada Needs a Framework for CUSMA Renewal Soon,” C.D. Howe Institute Trade Crisis Working Group, August 17, 2025, https://cdhowe.org/publication/before-the-window-closes-canada-needs-a-framework-for-cusma-renewal-soon; “North America Prepares for 2026 USMCA Review and Potential Renegotiation,” White & Case, November 13, 2024, https://www.whitecase.com/insight-alert/north-america-prepares-2026-usmca-review-and-potential-renegotiation.

5 White House, National Security Strategy of the United States of America (Washington, DC: The White House, November 2025), 15, https://www.whitehouse.gov/wp-content/uploads/2025/12/2025-National-Security-Strategy.pdf.

6 See, for example, Diane Francis, “The Donroe Doctrine,” Diane Francis on America and the World (Substack), July 21, 2025, https://dianefrancis.substack.com/p/the-donroe-doctrine. On the doctrine’s hemispheric reach and its implications for Canada’s sovereignty and economic choices, see “Trump Wants the Western Hemisphere—Canada Included,” Maclean’s, January 13, 2026, https://macleans.ca/politics/trump-wants-the-western-hemisphere-canada-included/; “A Veteran Diplomat Explains the ‘Donroe Doctrine,’” CBC Radio Front Burner, January 12, 2026, https://www.cbc.ca/radio/frontburner/a-veteran-diplomat-explains-the-donroe-doctrine-9.7042917.

7 On Prime Minister Mark Carney’s policy of reducing Canada’s overreliance on the U.S. market through trade and investment diversification, see “Carney Says Diversifying Trade Relationships with Europe, Asia Among Key Fall Objectives,” CBC News, September 10, 2025, https://www.cbc.ca/news/politics/carney-caucus-address-fall-priorities-1.7630250; “Canada’s Carney Visits Asia to Forge New Alliances and Reduce US Dependence,” Reuters, October 24, 2025, https://www.reuters.com/world/china/canadas-carney-visits-asia-forge-new-alliances-reduce-us-dependence-2025-10-24/; “Prime Minister Carney Strengthens Trade and Investment Partnerships,” Office of the Prime Minister, November 23, 2025, https://www.pm.gc.ca/en/news/news-releases/2025/11/23/prime-minister-carney-strengthens-trade-and-investment-partnerships; “Canada’s Carney Aims to Lead New Global Trading Order Less Reliant on US,” Reuters, January 20, 2026, https://www.reuters.com/world/china/canadas-carney-aims-lead-new-global-trading-order-less-reliant-us-2026-01-20/; Mark Carney, “Special Address by Mark Carney, Prime Minister of Canada,” World Economic Forum, Davos, January 26, 2026, https://www.weforum.org/stories/2026/01/davos-2026-special-address-by-mark-carney-prime-minister-of-canada.

8 For the Comprehensive Economic and Trade Agreement (CETA), see Government of Canada, “Canada–European Union Comprehensive Economic and Trade Agreement (CETA),” Global Affairs Canada, https://www.international.gc.ca/trade-commerce/trade-agreements-accords-commerciaux/agr-acc/ceta-aecg/index.aspx; and Canada–European Union Comprehensive Economic and Trade Agreement Implementation Act, S.C. 2017, c. 6, https://laws-lois.justice.gc.ca/eng/acts/c-4.8/index.html. For the Canada–EU Security and Defence Partnership, see European External Action Service, “Security and Defence: EU and Canada Sign Security and Defence Partnership,” June 24, 2025, https://www.eeas.europa.eu/eeas/security-and-defence-eu-and-canada-sign-security-and-defence-partnership_en; and Government of Canada, “Canada-European Union Security and Defence Partnership,” June 23, 2025, https://europa.eu/!hnkY69.

9 On the CPTPP as the framework for Canada’s trade relationships in the IndoPacific, see Government of Canada, “Comprehensive and Progressive Agreement for TransPacific Partnership (CPTPP),” Global Affairs Canada, https://www.international.gc.ca/trade-commerce/trade-agreements-accords-commerciaux/agr-acc/cptpp-ptpgp/index.aspx; and “Comprehensive and Progressive Agreement for TransPacific Partnership – Statement on Implementation,” Canada Gazette, October 17, 2020, https://gazette.gc.ca/rp-pr/p1/2020/2020-10-17/html/supl-eng.html. For Japan’s interest in Canadian LNG, see “Japan to Import Canadian LNG in Bid to Diversify Energy Supply,” Japan Forward, July 7, 2025, https://japan-forward.com/japan-to-import-canadian-lng-in-bid-to-diversify-energy-supply/. For South Korea’s demand for Canadian agricultural products, see Agriculture and AgriFood Canada, “Sector Trend Analysis – Meat Trends in South Korea,” September 2, 2025, https://agriculture.canada.ca/en/international-trade/reports-and-guides/sector-trend-analysis-meat-trends-south-korea. On China’s and India’s demand for Canadian energy, see “Canada, China Release Plan for Energy Cooperation,” CTV News, January 15, 2026, https://www.ctvnews.ca/politics/article/canada-china-release-plan-for-energy-co-operation/; and “Canada’s Energy Minister Argues for New Pipeline to Pacific Coast,” The Deep Dive, February 5, 2026, https://thedeepdive.ca/canadas-energy-minister-argues-for-new-pipeline-to-pacific-coast/.

10 On how internal trade barriers and regulatory differences fragment Canada into “a series of small markets” and undermine competitiveness, see Government of Canada, “Advancing Internal Trade,” February 20, 2025, https://www.canada.ca/en/intergovernmental-affairs/services/internal-trade/federal-investments-internal-trade.html; Government of Canada, “Government of Canada Removes Barriers to Interprovincial Trade and Labour Mobility,” November 16, 2025, https://www.canada.ca/en/one-canadian-economy/news/2025/11/government-of-canada-removes-barriers-to-interprovincial-trade-and-labour-mobility.html; and Anita Anand, “Government of Canada Removing More Than Half of Federal Exceptions Under the Canadian Free Trade Agreement,” February 20, 2025, https://www.canada.ca/en/intergovernmental-affairs/news/2025/02/government-of-canada-removing-more-than-half-of-federal-exceptions-to-the-canadian-free-trade-agreement-to-strengthen-interprovincial-trade.html. For analysis of mutual recognition of regulations and professional credentials as the most effective tool to liberalize internal trade, see Trevor Tombe, “Liberalizing Internal Trade Through Mutual Recognition,” MacdonaldLaurier Institute, September 19, 2022, https://www.trevortombe.com/publication/mli_trade/; Montreal Economic Institute, “The Promise of Reciprocal Mutual Recognition in Interprovincial Trade,” June 5, 2025, https://www.iedm.org/bilateral-breakthroughs-in-canada-the-promise-of-reciprocal-mutual-recognition-in-interprovincial-trade/; and “Canada’s Internal Trade Barriers Are Finally Coming Down, but Patchwork of Government Approaches Could Create New Challenges,” Canadian Federation of Independent Business, June 30, 2025, https://www.cfib-fcei.ca/en/media/canada-internal-trade-barriers-finally-coming-down-but-patchwork-of-government-approaches-could-create-new-challenges.

11 Government of Canada, “Prime Minister Carney to build strategic partnerships, diversify Canada’s trade, and attract new investment in visits to the People’s Republic of China and Switzerland,” 7 January 2026, https://wwwpm.gc.ca/en/news/news-releases/2026/01/07/prime-minister-carney-build-strategic-partnerships-diversify-canadas; Government of Canada, “From reliance to resilience: Budget 2025 delivers new investments to Buy Canadian and empower small and medium-sized businesses to strengthen Canada’s economy,” 10 November 2025, https://financeyahoo.com/news/reliance-resilience-budget-2025-delivers-160000987.html).[1].

12 Tony Keller, “Mark Carney’s survival plan: Canada and other ‘middle powers’ in an age of weaponized interdependence,” The Globe & Mail, 24 January 2026, https://www.theglobeandmail.com/business/commentary/article-carney-davos-speech-canada-trade-middle-powers/.

13 On distance and transport costs as a key handicap for Canadian trade with distant markets, see Walid Hejazi, “Understanding Canada’s International Trade under the TransPacific Partnership,” Canadian Public Policy 43, no. 3 (2017): 262–280, which shows a large negative elasticity of trade with respect to distance, implying higher costs and lower trade volumes as distance rises. For qualitative evidence on the challenges Canadian exporters face in serving Asian markets, including long transit times, logistics complexity and higher delivered costs, see Asia Pacific Foundation of Canada, Atlantic Canada Business in Asia Consultation Report, 2023, https://www.asiapacific.ca/sites/default/files/filefield/business_consultation_report_english.pdf. On the need for major investments in port capacity, containers and rail links to handle growing overseas trade, and the associated capital costs, see Transport Canada, Ports Modernization Review – Submission of the Railway Association of Canada, https://tc.canada.ca/sites/default/files/migrated/railwayassociationofcanada.pdf; and House of Commons Standing Committee on Transport, Infrastructure and Communities, Addressing Port Infrastructure Expansion, Committee Report No. 14, 44th Parl., 1st sess., September 2023, https://www.ourcommons.ca/Content/Committee/441/TRAN/Reports/RP12567825/tranrp14/tranrp14-e.pdf.

14 On Canada’s growing reliance on IndoPacific sea lanes and the vulnerability of its trade to instability in the South China Sea, see JeanFrédéric LégaréTremblay, “From the South China Sea to the Arctic: Linking Canada’s Interests,” Network for Strategic Analysis, April 20, 2022, https://ras-nsa.ca/from-the-south-china-sea-to-the-arctic-linking-canadas-interests/; and Canadian Global Affairs Institute, “Energy, Trade and Geopolitics in Asia: The Implications for Canada,” October 31, 2016, which notes that Canada already routes a significant share of its IndoPacific trade through the South China Sea, a region that ranks among the world’s busiest and most contested waterways, https://www.cgai.ca/energy_trade_and_geopolitics_in_asia_the_implications_for_canada. On the Strait of Malacca as a critical chokepoint exposed to piracy and disruption, see “Alarming Surge in Piracy Across Malacca and Singapore Straits,” Security Logistics Worldwide, August 27, 2025, https://dailymare.com/news/alarming-surge-in-piracy-across-malacca-and-singapore-straits,1729; and “Piracy and Armed Robbery Surge in the Straits of Malacca and Singapore,” The Guardian, August 25, 2025, https://www.theguardian.com/world/2025/aug/26/piracy-straits-of-malacca-singapore. On the Taiwan Strait as an increasingly risky shipping lane, see “Taiwan Tensions Raise Risks in One of Busiest Shipping Lanes,” Supply Chain Brain, August 2025, https://www.supplychainbrain.com/articles/35419-taiwan-tensions-raise-risks-in-one-of-busiest-shipping-lanes; and coverage of PLA exercises and associated shipping advisories in “Shipping Faces Incidental Risks as TaiwanAdjacent Drills Expand,” Kuehne+Nagel, December 30, 2025, https://mykn.kuehne-nagel.com/news/article/shipping-faces-incidental-risks-as-taiwan. For emerging threats to North Atlantic routes and undersea infrastructure from Russian submarine activity, see “Russian Submarines Prowl North Atlantic; NATO Allies UK, Norway Step Up Hunt,” Eurasian Times, December 4, 2025, https://www.eurasiantimes.com/n-russian-submarines-threaten-north-atlantic/; and Sam LaGrone, “Russian Nuclear Sub, Frigate with LongRange LandAttack Missiles Operating Off East Coast,” USNI News, June 11, 2024, https://news.usni.org/2024/06/11/russian-nuclear-sub-frigate-with-long-range-land-attack-missiles-operating-off-east-coast.

15 Office of the Parliamentary Budget Officer, The Fiscal Implications of Meeting the NATO Military Spending Target (Ottawa: PBO, 29 October 2024), https://www.pbo-dpb.ca/en/publications/RP-2425-020-S--fiscal-implications-meeting-nato-military-spending-target--repercussions-financieres-respect-cible-depenses-militaires-otan.

16 David Perry, “What Spending Two Per Cent of GDP on National Defence Means for Canada,” Canadian Global Affairs Institute, February 27, 2025, https://www.cgai.ca/what_spending_two_per_cent_of_gdp_on_national_defence_means_for_canada; Boston Consulting Group, “Getting the Most from Canada’s Defense Spending Surge,” October 19, 2025, https://www.bcg.com/publications/2025/getting-the-most-from-canadas-defense-spending-surge.

17 See, Fen Osler Hampson and Robert I. Rotberg, Grand Corruption: Curbing Kleptocracy Globally (London: Routledge, 2024).

18 On how differing legal systems, regulations, and nontariff measures raise the cost of doing business for Canadian firms in emerging markets, see House of Commons Standing Committee on International Trade, NonTariff Barriers to Trade: Some Canadian Perspectives, 44th Parl., 1st sess., May 2024, which highlights testimony from Canadian exporters that foreign regulations, standards and certification requirements significantly increase compliance costs and complexity, especially in Asia, https://www.ourcommons.ca/Content/Committee/441/CIIT/Reports/RP12791651/ciitrp14/ciitrp14-e.pdf. On India’s burdensome regulatory environment and slow contract enforcement, see World Bank, Doing Business 2020: Comparing Business Regulation in 190 Economies, which ranks India 163rd globally on enforcing contracts, with average commercial disputes taking more than 1,400 days to resolve, https://documents1.worldbank.org/curated/en/636621574941404453/pdf/Doing-Business-2020-Comparing-Business-Regulation-in-190-Economies.pdf. For broader evidence that nontariff measures, regulatory divergence and governance risks in AsiaPacific markets add 8–9 per cent to trade costs and can be two to three times as costly as tariffs, see Asia Pacific Foundation of Canada, Exploring NonTariff Barriers in CanadaAsia Pacific Trade, October 3, 2023, https://www.asiapacific.ca/publication/exploring-non-tariff-barriers-canada-asia-pacific-trade. On corruption and governance risks raising the cost of doing business in many emerging markets, see World Bank Group, Global Program on Anticorruption for Development, https://www.worldbank.org/en/programs/anticorruption-for-development.

19 On China’s use of economic leverage and trade coercion against Canada, including canola, see Expert Group on Canada–US Relations, Between the Eagle and the Dragon: Managing Canada–China Relations in a Shifting Geopolitical Reality (Ottawa: Norman Paterson School of International Affairs, Canadian Global Affairs Institute, and University of Calgary School of Public Policy, 2025), https://carleton.ca/npsia/wp-content/uploads/sites/77/2025/08/Expert-Group_Canada-China_August-25-2025.pdf; and “Canada Needs New Playbook for Relations with China amid Chaos,” Max Bell School of Public Policy, August 25, 2025, https://www.mcgill.ca/maxbellschool/max-policy/playbook-china-chaos-report. On Beijing’s weaponization of canola imports and the broader risk of monopsony power, see “CSIS Warned Beijing Weaponized Canola and Elections in Canada,” The Bureau, January 18, 2026, https://www.thebureau.news/p/analysis-csis-warned-beijing-weaponized; and “Canola Seeds [Canada–China],” Economic Coercion Project Case Study, March 30, 2019, https://economiccoercion.com/2019/03/31/canola-seeds-canada-china/. For evidence on China’s statedirected industrial overcapacity and dumping risks, including EVs, steel and aluminum, see Department of Finance Canada, “Canada Implementing Measures to Protect Canadian Workers and Key Economic Sectors from China’s Unfair Trade Practices,” August 26, 2024 https://www.canada.ca/en/department-finance/news/2024/08/canada-implementing-measures-to-protect-canadian-workers-and-key-economic-sectors-from-unfair-chinese-trade-practices.html; Sabrina A. Bandali et al., “Canada Responds to China’s Electric Vehicle, Steel and Aluminum Overcapacity,” Bennett Jones, September 5, 2024, https://www.bennettjones.com/Insights/Blogs/Canadas-Initial-Tariff-Response-to-Chinese-EVs-Steel-and-Aluminum-Overcapacity. On the nationalsecurity risks of Chinese investment in critical minerals and advanced technologies, see Hugo Cyr, “Has Canada Gone Too Far in Blocking Mining Investments from Chinese Companies?,” Centre for International Policy Studies, March 11, 2024, https://www.cips-cepi.ca/2024/03/11/has-canada-gone-too-far-in-blocking-mining-investments-from-chinese-companies/.

SPACE

Space Defence in an Age of Ambiguity: Access, Risk, and Restraint in a Contested Environment

Jessica West

Sapphire, Canada's first military satellite.
Photo Credit: Sergeant Gaetan Racine.Copyright: © 2012 DND-MDN Canada

Dr. Jessica West is a Senior Researcher at Project Ploughshares and a Senior Fellow at the Centre for Governance Innovation (CIGI). A Canadian expert on space security and the governance of emerging military technologies, her work focuses on arms control, escalation risk, strategic stability, and the implications of new technologies for defence policy and international security.

Space is no longer peripheral to defence priorities. It underpins how Canada sees, communicates, detects and tracks activity, responds to emergencies, and provides critical infrastructure across civil and military, domestic and allied contexts. As a result, disruption to space-enabled services would have immediate consequences for both military operations and the civilian systems that underpin Canadian society.[1]

For Canada, this reliance creates a distinctive security challenge. Canadian defence operations rely on a tightly integrated mix of military, civil, allied, and commercial space systems, many of which are not under exclusive national control. This integration provides access to capabilities that would be costly to sustain independently, but disruption rarely affects military systems alone. Interference can propagate simultaneously across defence, public safety, economic activity, and alliance operations, often under conditions of limited attribution and shared responsibility.

These dynamics are now reflected in defence planning and public debate, including recent calls to dedicate a defined share of Canada's defence spending to space.[2] The creation of the Defence Investment Agency and the adoption of a new "Build–Partner–Buy" framework further signal that space is being treated as a sovereign capability within Canada's defence industrial strategy.[3] Such proposals reflect recognition that space capabilities are no longer optional add-ons, but foundational to national defence, security, and sovereignty. But increased investment, on its own, does not resolve the strategic problem space presents.

The harder question is *what kind of space posture actually strengthens Canadian security*. Unlike traditional military domains, space does not offer clear pathways to decisive defence. It is a congested, technologically ambiguous, and environmentally fragile operating environment, where actions taken for defence purposes can have wide and lasting consequences.

In space, spending more does not automatically translate into greater security. Security is produced by the ability to sustain access to critical capabilities and information, to interpret activity under conditions of uncertainty, to protect systems without accelerating escalation, and to coordinate effectively across allied, civil, and commercial actors. In a domain defined by interdependence and ambiguity, the central challenge for Canadian defence is not dominance in space, but disciplined management of risk within it. This is ultimately a question of strategic posture, not simply of spending.

Canada in Space Today: Dependence, Integration, and Risk

Canada enters today's space security environment with long-standing national capabilities, deep technical expertise, and a high degree of operational dependence on allied and commercial systems. Canadian defence operations rely on a mix of military, civil, and commercial space capabilities – including satellite communications, Earth observation, and space situational awareness – supported by a growing domestic space sector. These capabilities are real but limited in scale and deeply interconnected with allied and commercial systems.

Rather than pursuing autonomous control of space infrastructure, Canada's space posture has evolved through close alliance relationships and integrated civil–military and commercial arrangements. This integration underpins defence effectiveness by providing access to capabilities that would be difficult and costly to sustain independently, but it also creates exposure to disruption that can propagate across defence, public safety, and economic systems, limiting unilateral control during incidents.

Recent defence policy reflects growing recognition of these conditions. Space is increasingly treated as critical infrastructure for Arctic awareness, sovereignty, and continental defence, with emphasis placed on sensing, data integration, and information advantage.[4]

Planned Northern Operational Support Hubs and associated infrastructure underscore that space-enabled sensing and communications will anchor Canada's Arctic defence posture.[5] Space also features prominently in NORAD modernization, where Canadian contributions focus on surveillance, tracking, and interoperability with allies,[6] reinforcing a posture built around shared awareness and coordinated response.

Within this framework, Canada has begun to place greater emphasis on selective sovereign space capabilities, signalling a modest but meaningful shift in orientation. The initial focus on assured access to space – particularly through launch[7] – reflects an understanding that sovereignty in space is exercised first through the ability to place and sustain capabilities in orbit when required. The ongoing development of the first Canadian military space doctrine further signals an effort to clarify how space capabilities are to be used and protected in a contested environment. Space control now forms part of the operational mandate of 3 Canadian Space Division,[8] and Canada's participation in alliance frameworks such as Operation Olympic Defender reflects a posture in which space effects, including temporary and reversible measures, are increasingly considered alongside access and resilience.[9]

Taken together, Canada's space defence posture reflects an increasingly operationalized domain, but one structured around integration, selective sovereignty, and risk management rather than dominance. These characteristics shape how Canada experiences competition in orbit and frame the strategic choices that expanded defence investment will require.

The Space Threat Environment: Strategic Competition Below the Threshold

Space is now widely recognized as a core domain of strategic competition. States increasingly view access to, and influence over, space systems as integral to military effectiveness, economic resilience, and national power.[10] Defence and intelligence assessments across allied states as well as NATO consistently characterize space as a contested environment in which rivals seek to exploit dependence on space-enabled capabilities.[11] For Canada, this matters not because competition in space is new, but because its scale, intensity, and consequences have expanded.

High-end threats dominate public attention. Anti-satellite capabilities are no longer rare, and multiple states have demonstrated the ability to destroy satellites in orbit. The 2021 destruction of a satellite in low Earth orbit illustrated the indiscriminate and enduring consequences of kinetic anti-satellite activity, generating long-lived debris and imposing shared risks across the space community, including on Canada and its allies.[12]

Concerns have also emerged about the potential pursuit of nuclear counterspace capabilities. U.S. officials have warned that Russia may be exploring a space-based nuclear capability; an act that would violate the Outer Space Treaty and cause widespread, non-selective harm to space systems.[13] Such a capability would not only target individual satellites but degrade space as an operating environment, with cascading military and civilian effects.[14] These risks matter because space systems are deeply entangled with nuclear deterrence and extended deterrence architectures: space-enabled sensing, early warning, communications, and command and control underpin strategic stability and alliance assurance. Interference with certain space systems is therefore widely understood as potentially escalatory, regardless of intent.[15]

At the same time, the risks Canada is most likely to confront arise through persistent competition below the threshold of armed conflict. A growing number of states possess non-destructive counterspace capabilities, and the use of some of these – most notably signal interference and cyber operations targeting ground infrastructure – has become widespread and persistent.[16] More advanced capabilities, such as rendezvous and proximity operations —where a satellite manoeuvres near another object—are increasingly demonstrated and can underpin ambiguous forms of interference or coercion.[17] These activities are deliberately calibrated to remain reversible and difficult to attribute, allowing actors to impose friction, test thresholds, and manage escalation while operating beneath traditional markers of conflict.[18]

For Canada, this pattern of competition is particularly consequential. Canadian defence capabilities depend heavily on space-enabled services embedded within civilian, commercial, and allied ecosystems, over which Canada does not always exercise direct control. Disruption in space therefore rarely affects military systems alone; it can simultaneously degrade critical infrastructure, emergency response, economic activity, and alliance operations. Reliance on shared systems also limits unilateral authority over protection, restoration, and response during incidents, shaping risk through the distributed nature of responsibility in space.

The principal risk Canada faces is therefore not sudden catastrophic attack, but persistent disruption, uncertainty, and erosion of confidence in systems on which both defence and society depend – conditions under which misinterpretation and escalation become more likely.

The Operating Environment as a Source of Insecurity

Beyond strategic competition, insecurity in space is shaped by the characteristics of the operating environment itself. Space is physically fragile, globally shared, and highly interdependent. These features create conditions in which disruption, misinterpretation, and escalation can occur even in the absence of deliberate hostile intent. In this sense, instability in space is not only the product of adversary behaviour, but of an environment that systematically obscures intent and amplifies the consequences of error.

Space systems operate in a harsh environment. Radiation, space weather, and congestion affect performance in ways that are difficult to diagnose and may resemble intentional interference.[19] As constellations grow and manoeuvring becomes more frequent, anomalies and close approaches are becoming more common, increasing the risk that routine events are misread as hostile actions.

These risks are compounded by the dual-use and dual-purpose character of many space systems. Satellites designed for communications, navigation, Earth observation, or on-orbit servicing often support both civilian and military functions.[20] Benign or commercially motivated activities can appear indistinguishable from preparations for interference, complicating intent assessment under uncertainty.

Deeper integration of commercial space services into military operations further expands exposure and shifts risk onto civilian users and private operators. Commercial satellite communications, Earth observation, and data services now underpin operational resilience and flexibility, while expanding the range of assets exposed to disruption and further entangling civilian infrastructure and private actors in strategic competition.[21] Interference with commercial systems can therefore generate military effects while shifting risk onto civilian users and private operators.[22]

These challenges are exacerbated by persistent gaps in situational awareness, interpretation, and communication. Although the volume of data on objects and activity in space has increased, access to high-quality, timely space situational awareness remains concentrated among a limited number of states and commercial providers. Analytic authority is fragmented across military, civil, and private actors operating under different mandates and assumptions, leaving no single shared picture of events in orbit.[23] In such conditions, routine or ambiguous activity is more likely to be misinterpreted as hostile. While efforts to improve space traffic management are important, from a defence perspective, the core challenge is not traffic rules themselves, but how congestion and proximity amplify ambiguity and escalation risk.[24]

Finally, these risks are magnified by the absence of widely accepted operational practices for managing incidents in space. While international law establishes broad principles, there are limited shared expectations governing routine operations, interference below armed conflict, or crisis communication.[25] In this environment, ambiguity is not accidental – it is structural.

What Five Percent Enables and What It Must Prioritize

A defence spending target of five percent of GDP would mark a structural shift in Canada's military posture. In the space domain, it would move decisions beyond incremental upgrades toward choices that shape how Canada secures access, manages risk, and contributes to collective defence. The central question is therefore not whether Canada should invest more in space, but how expanded investment can strengthen security in practice rather than amplify instability.

As the preceding sections have shown, space competition is defined less by decisive attack than by persistent disruption, ambiguity, and escalation risk. Defence effectiveness therefore depends on the ability to operate

through disruption, interpret events accurately, coordinate with partners, and manage escalation under pressure.

1. Secure and Sustainable Access to Space-Enabled Capabilities and Information

The core priority for Canadian space defence is secure and sustainable access to the space-enabled capabilities and information on which defence, sovereignty, and alliance operations depend. This includes surveillance, communications, navigation, and data services essential to Arctic awareness, military operations, emergency response, and collective defence.

The designation of space as a sovereign capability in Canada's Defence Industrial Strategy creates an opportunity to define sovereignty narrowly and strategically. In space, sovereignty is not synonymous with national control or even full-spectrum autonomy. It is best understood as assured access to critical capabilities; meaningful control over key data and software; and the ability to sustain operations independently if allied or commercial services are degraded.

For Canada, this requires resilience combined with selective national capability. Investments that reduce reliance on single points of failure—such as assured access to space launch, resilient sensing and data pathways, and the ability to integrate or substitute allied and commercial services—directly limit the strategic payoff of interference.[26] Emphasizing redundancy, degraded-mode operations, and security-by-design across ground infrastructure, software, and data strengthens deterrence by denial without escalating competition.

In software-defined and AI-enabled space systems, sovereignty increasingly resides in access to source code, update pathways, and data rights. Procurement decisions that prioritize intellectual property access and lifecycle control may do more to secure Canadian autonomy than ownership of physical platforms alone.

2. Understanding and Interpreting Activity in Space

In a congested and contested environment, security depends on the ability to understand what is happening in space and why. Disruption, environmental effects, and deliberate interference can appear similar, particularly under conditions of limited attribution and time pressure. For Canada, interpretive capacity is therefore central to managing risk and avoiding miscalculation.

This places a premium on space situational awareness, data integration, and analytic capacity across military, civil, and commercial sources. More data alone is insufficient; what matters is the ability to fuse information, assess intent, and communicate uncertainty clearly. Investments in interpretive capacity reduce the risk that ambiguity is mistaken for aggression and enable earlier, more measured responses.[27]

3. A Cautious Approach to Protection and Counterspace

Protection is essential, but in a congested and dual-use domain, how systems are protected matters as much as whether they are protected. For Canada, defence investment must prioritize protection measures whose benefits clearly outweigh the strategic, environmental, and escalation risks they introduce.

This consideration is increasingly important as allies explore "active defence" approaches in space, including on-orbit protective systems and space-based interceptor concepts.[28] Highly visible or irreversible measures are unlikely to meaningfully deter the forms of competition Canada is most likely to face. Below-threshold interference such as signal disruption, cyber activity, or ambiguous proximity operations, is deliberately designed to remain deniable, reversible, and persistent.[29] Capabilities whose use would be overtly escalatory or politically constrained are poorly suited to countering these dynamics.

The distinction between kinetic and non-kinetic counterspace is therefore decisive. Destructive anti-satellite weapons and space-based interceptors generate long-lived debris, impose indiscriminate harm on civilian and allied systems, and would be widely understood as escalatory and self-damaging.[30] Limited engagement with non-kinetic space effects may arise within alliance contexts, but only as a bounded, reversible, and tightly controlled measure, subordinate to the broader goals of sustained access, resilience, and escalation management. Because space systems underpin civilian infrastructure globally, effective defence must incorporate assessment of second-order effects and civilian exposure.

Industrial sovereignty and escalatory posture are not the same. Strengthening domestic space manufacturing, launch, analytics, and secure communications can enhance resilience without requiring Canada to adopt destabilizing counterspace doctrines. The "Build–Partner–Buy" framework should therefore distinguish clearly between building sovereign industrial capacity and pursuing counterspace capabilities whose use could accelerate escalation.

4. Acting Together: Allies, Civilians, and the Private Sector

Effective space defence depends on coordination across military, civil, allied, and commercial actors. Shared systems are a source of resilience, but fragmentation creates gaps that can be exploited during competition. Defence investment should therefore treat coordination itself as a capability,[31] supporting information sharing, common operating pictures, and agreed incident-response processes.

Canada's participation in Operation Olympic Defender illustrates that space control and crisis response are increasingly coordinated through alliance frameworks rather than exercised unilaterally. Defence investment must support institutionalized information-sharing, exercised communication pathways, and shared escalation-management frameworks alongside technical capability.

5. Mitigating Escalation in Space

Even temporary and reversible space effects can generate escalation if intent is misread, civilian infrastructure is disrupted, or responses are poorly coordinated. This sensitivity reflects both the complexity of the operating environment,[32] and the enduring influence of nuclear-era escalation thinking on space security governance.[33] Mitigating escalation therefore requires investment in interpretation, communication channels, escalation analysis, and exercised response mechanisms. Dedicated incident-communication pathways, secure information-sharing platforms, and trained points of contact are essential for managing ambiguity before it becomes crisis.

Conclusion

Space is indispensable to Canadian defence, but it is not a domain in which security can be achieved through dominance, insulation, or technological overmatch. The risks Canada faces arise less from isolated attacks than from persistent disruption, ambiguity, and the potential for escalation in a fragile and interdependent operating environment.

Under a five-percent defence trajectory, the central question is therefore not how much Canada spends on space, but what kind of space defence posture that investment enables. Effective space defence depends on sustained access, interpretive capacity, restrained protection measures, and coordinated action across allied and commercial systems. These are concrete defence capabilities that require deliberate investment in sensing, data integration, secure communications, analytic capacity, and exercised response mechanisms.

Canada does not need to mirror the most escalatory capabilities being explored by others. It needs investment choices that preserve access, maintain flexibility, and support stability in a domain where miscalculation imposes shared and lasting costs. In space, security is measured not by visibility or posture, but by the ability to manage risk, sustain operations, and contribute credibly to collective defence under conditions of uncertainty.

Notes

[1] Royal Bank of Canada, *A Higher Orbit: How Canada Can Build and Finance a Bolder Space Strategy* (Toronto: RBC Thought Leadership, 2023), https://www.rbc.com/en/thought-leadership/space/a-higher-orbit-how-canada-can-build-and-finance-a-bolder-space-strategy/

[2] Pippa Norman, "Canada's Space Companies Make National-Security Pitch for Chunk of Defence Dollars," *The Globe and Mail*, November 19, 2025, updated November 20, 2025, https://www.theglobeandmail.com/business/economy/article-canadas-space-companies-make-national-security-pitch-for-chunk-of/

[3] Government of Canada, *Security, Sovereignty and Prosperity: Canada's Defence Industrial Strategy* (Ottawa: Department of National Defence, 2026).

[4] Government of Canada, *Our North, Strong and Free: A Renewed Vision for Canada's Defence* (Ottawa: Department of National Defence, April 2024), https://www.canada.ca/en/department-national-defence/corporate/reports-publications/our-north-strong-and-free-2024.html

[5] Government of Canada, *Defence Industrial Strategy*, 37–38.

[6] Government of Canada, "NORAD Modernization Project Timelines," Department of National Defence, last modified June 2022, https://www.canada.ca/en/department-national-defence/services/operations/allies-partners/norad/norad-modernization-project-timelines.html

[7] Marc Boucher, "Federal Budget Includes $182.6 Million for Sovereign Space Launch Capability," *SpaceQ*, November 4, 2025, https://spaceq.ca/federal-budget-includes-182-6-million-for-sovereign-space-launch-capability/

[8] Government of Canada, *3 Canadian Space Division*, Royal Canadian Air Force, accessed February 15, 2026, https://www.canada.ca/en/air-force/corporate/who-we-are/organizational-structure/3-canadian-space-division.html.

[9] United States Space Command, *Multinational Force Operation Olympic Defender*, accessed February 15, 20226, https://www.spacecom.mil/About/Multinational-Force-Operation-Olympic-Defender/.

[10] The White House, *Ensuring American Space Superiority* (Washington, DC: White House, December 2025), https://www.whitehouse.gov/presidential-actions/2025/12/ensuring-american-space-superiority/; State Council Information Office of the People's Republic of China, *China's Space Program: A 2021 Perspective* (Beijing: State Council Information Office, January 28, 2022), https://english.www.gov.cn/archive/whitepaper/202201/28/content_WS61f35b3dc6d09c94e48a467a.html.

[11] See for example Office of the Director of National Intelligence, *Annual Threat Assessment of the US. Intelligence Community* (Washington, DC: ODNI, 2025), sections on space and counterspace threats, https://www.dni.gov/files/ODNI/documents/assessments/ATA-2025-Unclassified-Report.pdf. North Atlantic Treaty Organization (NATO), *Strategic Concept 2022* (Madrid: NATO, June 29, 2022).

[12] Ankit Panda, "The Dangerous Fallout of Russia's Anti-Satellite Missile Test," *Carnegie Endowment for International Peace*, November 17, 2021, https://carnegieendowment.org/posts/2021/11/the-dangerous-fallout-of-russias-anti-satellite-missile-test

[13] John D. Plumb, *Statement of John D. Plumb, Assistant Secretary of Defense for Space Policy*, testimony before the Subcommittee on Strategic Forces, Committee on Armed Services, U.S. House of Representatives, May 1, 2024, https://docs.house.gov/meetings/AS/AS29/20240501/117236/HHRG-118-AS29-Wstate-PlumbJ-20240501.pdf

[14] Jessica West, "Geneva, We Have a Problem: Space Diplomacy Goes Nuclear," *Centre for International Governance Innovation* (CIGI), 2023, https://www.cigionline.org/publications/geneva-we-have-a-problem-space-diplomacy-goes-nuclear/

[15] James M. Acton, "Escalation through Entanglement: How the Vulnerability of Command-and-Control Systems Raises the Risks of an Inadvertent Nuclear War," *International Security* 43, no. 1 (Summer 2018): 56–99, https://doi.org/10.1162/isec_a_00320.

[16] Secure World Foundation, *Global Counterspace Capabilities: An Open-Source Assessment* (Washington, DC: Secure World Foundation, 2025), https://www.swfound.org/publications-and-reports/2025-global-counterspace-capabilities-report.

[17] Victoria Samson and Kathleen Brett, *Chinese Military and Intelligence Rendezvous and Proximity Operations* (Washington, DC: Secure World Foundation, fact sheet), https://www.swfound.org/publications-and-reports/chinese-military-and-intelligence-rendezvous-and-proximity-operations-fact-sheet; Victoria Samson and Kathleen Brett, *U.S. Military and Intelligence Rendezvous and Proximity Operations* (Washington, DC: Secure World Foundation, fact sheet), https://www.swfound.org/publications-and-reports/u-s-military-and-intelligence-rendezvous-and-proximity-operations-fact-sheet.

[18] Jessica West and Jordan Miller, "Clearing the Fog: The Grey Zones of Space Governance," *Centre for International Governance Innovation* (CIGI), CIGI Paper No. 287, November 30, 2023, https://www.cigionline.org/publications/clearing-the-fog-the-grey-zones-of-space-governance/Michael J. Mazarr, *Mastering the Gray Zone: Understanding a Changing Era of Conflict* (Carlisle, PA: U.S. Army War College Press, 2015), https://press.armywarcollege.edu/monographs/428/

[19] National Research Council, *Severe Space Weather Events—Understanding Societal and Economic Impacts: A Workshop Report* (Washington, DC: National Academies Press, 2008), https://www.nationalacademies.org/read/12507/chapter/1; European Space Agency, *ESA Space Environment Report* (Paris: European Space Agency, latest edition), https://www.esa.int/Space_Safety/Space_Debris/ESA_Space_Environment_Report; Anca Agachi et al., *Order in Orbit: Operationalizing an International Space Traffic Management Organization*, (RAND Corporation, Santa Monica, CA: RAND Corporation, 2025), https://www.rand.org/pubs/research_reports/RRA3463-1.html; European Space Agency, "Sounding the Alarm: ESA Introduces Space Environment Health Index," *ESA Space Safety*, https://www.esa.int/Space_Safety/Space_Debris/Sounding_the_alarm_ESA_introduces_space_environment_health_index.

[20] Almudena Azcárate Ortega, *Dual-Use and Dual-Purpose Objects*, United Nations Institute for Disarmament Research (UNIDIR), presentation by to the Open-Ended Working Group on "Reducing Space Threats through Norms, Rules and Principles of Responsible Behaviours," September 2022, https://documents.unoda.org/wp-content/uploads/2022/09/OEWG-dual-use-presentation-FINAL.pdf

[21] Laetitia Cesari, "Commercial Space Operators on the Digital Battlefield," in The *Cybersecurity and Outer Space* series, Aaron Shull, Jessica West, and Wesley Wark eds., Centre for International Governance Innovation, January 29, 2023, https://www.cigionline.org/articles/commercial-space-operators-on-the-digital-battlefield/.

[22] Cassandra Steer, "International Humanitarian Law in the 'Grey Zone' of Space and Cyber," in The *Cybersecurity and Outer Space* series, Aaron Shull, Jessica West, and Wesley Wark eds., Centre for International Governance Innovation, January 29, 2023, https://www.cigionline.org/articles/international-humanitarian-law-in-the-grey-zone-of-space-and-cyber/.

[23] Anca Agachi, *Order in Orbit: Operationalizing an International Space Traffic Management Organization*.

[24] Almudena Azcárate Ortega and Sara Erickson, *OEWG on Reducing Space Threats through Norms, Rules and Principles of Responsible Behaviours: Recap Report* (Geneva: UNIDIR, 2024), https://unidir.org/wp-content/uploads/2024/03/unidir_oewg_on_reducing_space_threats_recap_report.pdf

[25] Ibid.

[26] The Aerospace Corporation, *Resilience for Space Systems* (El Segundo, CA: The Aerospace Corporation, 2017), https://aerospace.org/sites/default/files/2018-05/Resilience%20for%20Space%20Systems.pdf.

[27] Azcárate Ortega and Erickson, *OEWG Recap Report* (2024).

[28] French Ministry of the Armed Forces, *Space Defence Strategy* (Paris: Ministère des Armées, 2019), https://cd-geneve.delegfrance.org/IMG/pdf/space_defence_strategy_2019_france.pdf; Theresa Hitchens, "European Defense Fund Invests in 'Bodyguard' Satellite Development to Counteract Orbital Threats," *Breaking Defense*, May 30, 2024, https://breakingdefense.com/2024/05/european-defense-fund-invests-in-bodyguard-satellite-development-to-counteract-orbital-threats/; U.S. Space Force, *Space Doctrine Publication 3-0: Operations* (Washington, DC: Department of the Air Force, July 19, 2023), https://www.starcom.spaceforce.mil/Portals/2/SDP%203-0%20Operations%20%2819%20July%202023%29_1.pdf.

[29] Michael J. Mazarr, *Mastering the Gray Zone;; Rajeswari Pillai Rajagopalan, Electronic and Cyber Warfare in Outer Space (*Geneva: United Nations Institute for Disarmament Research, 2019*), https://unidir.org/publication/electronic-and-cyber-warfare-in-outer-space/*

[30] James M. Acton, "Escalation through Entanglement,"; Almudena Azcárate Ortega and Sara Erickson, *OEWG on Reducing Space Threats through Norms, Rules and Principles of Responsible Behaviours.*

[31] Bruce McClintock et al., *Allied by Design: Defining a Path to Thoughtful Allied Space Power* (Santa Monica, CA: RAND Corporation, 2024), https://www.rand.org/pubs/research_reports/RRA1739-1.html

[32] Allison Goody and Ariel Shapiro, *The Growing Complexity of Space: Implications for Security and Stability*, HillStudies Publication no. 2022-10-E (Ottawa: Library of Parliament, July 26, 2022), https://lop.parl.ca/sites/PublicWebsite/default/en_CA/ResearchPublications/202210E.

[33] Sarah Erickson, "The Long Shadow of the Nuclear Age on Space Security Governance," United Nations Institute for Disarmament Research, 2023, https://unidir.org/the-long-shadow-of-the-nuclear-age-on-space-security-governance/.

SEA

Maritime Security in 2026: From Competition to Contestation

Kate E. Todd

His Majesty's Canadian Ship Regina in Alaska during Operation LATITUDE, August 2025.
Photo Credit: Combat Camera

Kate E. Todd is a maritime security specialist and fellow with several Canadian think tanks and research networks, including the Canadian Maritime Security Network, the North American and Arctic Defence and Security Network, the Canadian Global Affairs Institute, Triple Helix, and Arctic360. She also serves on the Editorial Board of the Canadian Naval Review.

In 2026, Canada finds itself in a maritime security environment undergoing a consequential shift. Strategic competition, where states pursue long-term advantages without directly challenging each other's activities, has degraded into contestation in key regions. In the Taiwan Strait, Red Sea, and Arctic, state and non-state actors are no longer just investing in maritime systems, assets, and weaponry. Now, they are using kinetic, legal, and political means to deliberately limit, disrupt, and shape the actions of others in particular maritime regions, without triggering open conflict.[1] To operate in contested maritime environments like these, Canada must have a credible and combat-ready naval force capable of defending its territory and interests at home and abroad. However, Canada's current naval posture is ill-equipped to meet this moment. Without accelerated recapitalization of its navy, Canada risks losing access, influence, and autonomy in contested waters.

Canada's naval force posture and ability to sustain operations in contested theatres is limited by fleet availability, aging platforms, and personnel shortages. The Navy's 12 Halifax-class frigates and four Victoria-class submarines are approaching the end of their service lives.[2] Also in need of replacement are Canada's eight Orca-class training vessels and 12 Kingston-class Maritime Coastal Defence Vessels, eight of which were paid off in 2025, significantly reducing the overall size of the fleet.[3] However, Canada recently commissioned six new Arctic and Offshore Patrol Ships, the last of which was delivered in 2025.[4] Although they are not intended to engage in combat, the Arctic and Offshore Patrol Ships conduct a variety of missions, including tasks formerly reserved for Maritime Coastal Defence Vessels. Despite this class's welcome addition, maintenance cycles and crewing gaps further reduce fleet availability at any given time. These structural limitations shape the extent to which Canada can respond to contestation in the maritime domain.

Canada needs to rapidly invest in its navy to protect its interests in an international context where might, increasingly, makes right.

Stability in the maritime domain is crucial for Canada, as a maritime nation whose marine economy accounts for approximately 1.8 percent of the country's gross domestic product.[5] It is also critical for the global economy, as over 80 percent of global trade is transported by sea and 99 percent of worldwide communications rely on subsea cables.[6] As Prime Minister Carney noted in his January 2026 Davos speech, a "rupture in the world order" is giving way to "a brutal reality" in which actors operate without limits.[7] As a result, Canada's sovereignty and interests now depend on the country's ability to withstand contestation in both distant choke points and closer to home in the Arctic.[8]

Contestation in Action

Contestation now characterizes several of the world's most strategically significant maritime regions, including the Taiwan Strait, Red Sea, and Arctic. In each, access, influence, and sovereignty are actively contested.

Taiwan Strait

China engages in contestation to control the Taiwan Strait and deny other actors' access to the important waterway.[9] Years of military buildup, persistent exercises, and lawfare demonstrate China's willingness to challenge legal and operational norms and claim the Strait.[10] China has built the world's largest navy and is rapidly modernizing its fleet with advanced weaponry and drone technology capable of enforcing a robust anti-access/area-denial posture around Taiwan.[11] It uses its fleet to hold frequent military drills in the region to deter and desensitize adversaries who reject its claim to the Strait.[12] China is also instrumentalizing its interpretation of the United Nations Convention on the Law of the Sea (UNCLOS) to legitimize its position that the Strait is part of China's internal waters.[13]

While these actions do not pose an existential threat to Canada, they pose significant risk to Canadian interests and assets. Canada has a strategic interest in semiconductor chips produced in Taiwan, used in advanced electronics and military equipment.[14] This makes freedom of navigation operations vital to preserving market access. The Royal Canadian Navy also deploys three ships per year to the region under Operation HORIZON.[15] These deployments are largely symbolic, signalling Canada's rejection of China's interpretation of UNCLOS, but pose a challenge for China and its stated goals. In response, China openly contests access to, and attempts to assert sovereignty over, the Strait by interfering with freedom of navigation operations, performing unsafe aerial intercepts, and nearly colliding with North Atlantic Treaty Organization vessels.[16] Taken together, China's efforts in the Taiwan Strait highlight the magnitude and multidimensional threats Canada faces operating in contested maritime environments.

Red Sea

In the Red Sea, contestation takes a different form: non-state actors, notably the terrorist group known as the Houthis, use asymmetric tactics to disrupt access to one of the world's busiest maritime trade routes.[17] Approximately 11 percent of maritime trade transits the Red Sea.[18] Accordingly, the security of this corridor is vital to both global shipping and supply chain resilience. Prolonged disruptions in the region indirectly affect Canada's economic security, as well as the economic security of Canada's allies. Since 2023, the Houthis have launched dozens of missile and drone attacks on commercial ships, forcing companies to re-route around the Cape of Good Hope.[19] These attacks include the use of small high-speed uncrewed surface vessels as munitions against ships, as well as the simultaneous deployment of missiles and drones in swarm attacks to overwhelm ships' defences.[20] The use of these inexpensive and efficient technologies allows the Houthis to exert disproportionate influence over the region.

Through Operation PROSPERITY GUARDIAN and Operation ASPIDES, launched by the United States (U.S.) in 2023 and the Council of the European Union in 2024, Western allies have been able to protect shipping in this vital corridor.[21] However, Canada's contribution to these operations – only three staff officers – underscores the current limitations of its naval force posture.[22] The Royal Canadian Navy is already engaged in multiple theatres and lacks the capacity to send ships to another region for prolonged periods or fend off attacks such as coordinated drone swarms. Without additional ships, personnel, and advanced technologies, Canada will continue to face challenges in committing assets to the region. Contestation in the Red Sea illustrates how even simple systems used by non-state actors can produce outsized effects, reinforcing the need for Canada to invest in its navy and advanced technologies that are capable of countering asymmetric attacks.

Arctic

Unlike the Red Sea, contestation in the Arctic is primarily legal and political, rather than kinetic. Competing territorial claims, interpretations of international law, and political pressures challenge the sovereignty of Arctic nations, including Canada's. Without a persistent military presence, domain awareness, and the ability to sustain forces, Arctic nations may struggle to deter these challenges.

Although Russia's military buildup and China's patrols of the Northwest Passage continue to shape the security environment in the Arctic, Canada's sovereignty is now also threatened by its southern neighbour. Recent U.S. rhetoric concerning Greenland has underscored the vulnerability of Arctic states and reinforced the need for Canada to possess Arctic military capabilities.[23] As with Greenland, the U.S. has expressed concern over Canada's ability to protect against threats posed by Russia and China.[24] According to the U.S.'s 2026 National Defense Strategy, if Canada fails to do so, Washington "will stand ready to take focused, decisive action that concretely advances U.S. interests."[25] While this does not signal an imminent territorial threat, it constrains Canadian decision-making autonomy, narrowing Ottawa's ability to independently set priorities, timelines, and risk thresholds. It also highlights the need for Canada to spend more on defence to protect its sovereignty in the North.

Recent investments demonstrate Canada's commitment to maintaining a credible presence and operational readiness in the Arctic. Operation NANOOK, Canada's premier Arctic operation with annual naval deployments, is expanding in 2026 to provide nearly-persistent presence in the region, employing troops for 10 months per year.[26] In addition, the federal government has invested millions of dollars in support of expanding the Port of Churchill and accelerating the construction of the Grays Bay Road and Port project, both of which could support naval operations in the region.[27] Canada's investments in the modernization of the North American Aerospace Defence Command, including upgrades to radar systems, sensor suites, and space-based surveillance capabilities, will further bolster maritime domain awareness.[28] However, these investments must materialize rapidly to deliver capacity at the pace required by the deteriorating security environment.

Trends in Contemporary Contestation

Across these theatres, contestation is executed to different degrees, in different domains, and with different means for different ends by state and non-state actors. Importantly, technological innovation – particularly the proliferation of autonomous systems and advanced sensors – is increasing the complexity of contestation everywhere. Inexpensive munitions, drones, and networked sensors empower actors to exert influence persistently and precisely.[29] These capabilities lower the threshold for contestation, allowing states and non-state actors to test navigation rights, monitor commercial shipping, or challenge territorial claims without deploying crewed assets or risking escalation through direct confrontation. As demonstrated in the Red Sea, even simple systems operated by non-state actors can generate disproportionate effects when employed in strategic corridors.

Beyond kinetic threats, state and non-state actors are using legal and political tools to affect the maritime domain. Legal contestation is leveraged to legitimize navigation rights and sovereignty assertions through competing interpretations of UNCLOS, particularly in the Taiwan Strait and Arctic.[30] Political pressure, applied through trade policies, rhetoric, or control over critical resources, is also used to influence state behaviour and constrain decision-making.[31]

The contrast between theatres highlights the diversity of modern contestation. In the Taiwan Strait, a capable state actor is employing sustained military buildup, exercises, and coercive actions to assert control over a critical waterway, while avoiding full-scale conflict. In the Red Sea, non-state actors are using asymmetric tactics to disrupt commerce and test coalition coordination. Contrastingly, in the Arctic, sovereignty is being tested by Arctic and non-Arctic states asserting competing claims and applying political pressure.[32]

This diversity illustrates that effective maritime deterrence and defence require tailored approaches: kinetic capabilities are essential for combatting threats in strategically important choke points, while credible military presence and domain awareness are central to managing challenges in the Arctic.

Implications for Canada

Canada's current ability to operate in contested environments reflects structural constraints and the effect of long-standing choices about where defence fits among national priorities. Decades of underinvestment, slow procurement, and personnel shortages have left the Royal Canadian Navy with limited flexibility and surge capacity. This forces the Government of Canada to make hard choices about where ships can be deployed, and for how long. As a result, Canada's maritime engagements are often reactive, shaped by what the Navy can spare, rather than by a clear alignment between Canada's interests and capabilities.

What is increasingly clear is the need for urgent and continued investment in the Royal Canadian Navy, so it can operate in contested regions and protect Canada's interests and territory in increasingly complex and contentious environments. This means procuring more ships and advanced technologies, hiring and training more sailors, and investing in the infrastructure needed to support them. Canada is making headway by procuring 15 River-class destroyers, two Joint Support Ships, and up to 12 submarines, but these platforms are not enough on their own. Additional investments are needed to replace the Kingston and Orca-class to maintain and improve the Navy's abilities.[33]

Looking ahead, Canada must also begin integrating advanced technologies, including autonomous systems, into naval operations to enhance situational awareness and provide scalable response options in contested waters.[34] By deploying persistent, networked platforms, Canada can maintain a credible presence, increase domain awareness, and operate in areas where conventional forces alone may be insufficient. Strategic investments in these

technologies are critical to extending the Royal Canadian Navy's reach, improving responsiveness, and mitigating operational risk.

The Need for Accelerated and Continued Investment

In 2026, contestation, rather than competition, defines the maritime domain. From high-intensity coercion in global choke points to legal and political pressures in the Arctic, states and non-state actors are testing boundaries, shaping behaviour, and challenging sovereignty in persistent, uneven, and multidimensional ways. Confronting maritime contestation requires more than symbolic operations, like in the Taiwan Strait. It demands a credible and combatready Navy capable of sustaining operations across regions where Canada's interests and sovereignty are at risk. Without accelerated and continued investment in the Royal Canadian Navy, Canada will face growing constraints on where it can deploy, what it can defend, and how much pressure it can withstand in contested maritime spaces.

Notes

[1] Major Jon Michael King, "Contested Logistics Environment Defined," The United States Army, February 1, 2024, https://www.army.mil/article/272922/contested_logistics_environment_defined.

[2] Naval Association of Canada, "Halifax-Class Frigates," October 2024, https://www.navalassoc.ca/wp-content /uploads/2024/11/BN-Halifax.pdf; Public Services and Procurement Canada, "Government of Canada Advances to Next Step in Canadian Patrol Submarine Project Procurement," Government of Canada, August 26, 2025, https://www.canada.ca/en/public-services-procurement/news/2025/08/government-of-canada-advances-to-next-step-in-canadian-patrol-submarine-project-procurement.html.

[3] National Defence, "Royal Canadian Navy to Pay Off Kingston-class Vessels," Government of Canada, July 24, 2-25, https://www.canada.ca/en/department-national-defence/news/2025/07/royal-canadian-navy-to-pay-off-kingston-class-vessels.html; Kate Todd, "Redesigning the Royal Canadian Navy for a More Dangerous World," Canadian Global Affairs Institute, January 2025, https://www.cgai.ca/redesigning_the_royal_canadian_navy_for_a_more_dangerous_world.

[4] Public Services and Procurement Canada, "Arctic and Offshore Patrol Ships," Government of Canada, February 27, 2025, https://www.canada.ca/en/department-national-defence/services/procurement/arctic-offshore-patrol-ships.html.

Naval Association of Canada, "Arctic and Offshore Patrol Vessels," October 2024, https://www.navalassoc.ca/wp-content/uploads/2024/11/BN-AOPV.pdf, pp. 2-3.

[5] Fisheries and Oceans Canada, "Book 2, Tab A6 – Overview of the Marine Economy," Government of Canada, July 11, 2025, https://www.dfo-mpo.gc.ca/transparency-transparence/mtb-ctm/2025/2-a6-marine-economy-economie-maritime-enghtml.

[6] United Nations Conference on Trade and Development (UNCTAD), "Shipping Data: UNCTAD Releases New Seaborne Trade Statistics," April 23, 2025, https://unctad.org/news/shipping-data-unctad-releases-new-seaborne-trade-statistics; William Park, "The Deep-Sea 'Emergency Service' That Keeps the Internet Running," BBC News, October 15, 2024, https://www.bbc.com/future/article/20241014-the-deep-sea-emergency-service-that-keeps-the-internet-running.

[7] World Economic Forum. "Davos 2026: Special Address by Mark Carney, Prime Minister of Canada." January 20, 2026. Accessed January 25, 2026. https://www.weforum.org/stories/2026/01/davos-2026-special-address-by-mark-carney-prime-minister-of-canada/.

[8] World Economic Forum, "Davos 2026: Special Address."

[9] Ministry of National Defense of the People's Republic of China, "Eastern Theater Command Spokesman Speaks on the Passage of Canadian and Australian Warships through the Taiwan Strait," translated statement, Eastern Theater WeChat public account, edited by Shang Xiaomin, September 6, 2025, http://www.mod.gov.cn/gfbw/qwfb/16408161.html.

[10] Koh Ewe, "China Holds Military Drills Around Taiwan as Warning to 'Separatist Forces'," BBC News, December 29, 2025, https://www.bbc.com/news/articles/c87l7xjp235o; Hu Yuwei, Fan Wei, and Feng Fan, "Chinese Report Challenges Legality of US 'Freedom of Navigation' Operations," Global Times, August 25, 2025, https://www.globaltimes.cn/page/202508/1341650.shtml.

[11] Harper Ellis, « How Powerful is the Chinese Navy Compared to the U.S. Navy?" Defense Feeds, January 25, 2026, https://defensefeeds.com/analysis/geopolitics/how-powerful-is-the-chinese-navy/.

[12] Koh Ewe, "China Holds Military Drills Around Taiwan as Warning to 'Separatist Forces'."

[13] Jill Goldenziel, "China Claims to Own the Taiwan Strait. That's Illegal," Forbes, June 28, 2022, https://www.forbes.com/sites/jillgoldenziel/2022/06/28/china-claims-to-own-the-taiwan-strait-thats-illegal/.

[14] Karen Hui, "Taiwan, Canada, and the Global Semiconductor Race," Asia Pacific Foundation, February 10, 2025, https://www.asiapacific.ca/publication/taiwan-canada-and-global-semiconductor-race.

[15] National Defence, "Operation HORIZON," Government of Canada, November 27, 2025, https://www.canada.ca/en/department-national-defence/services/operations/military-operations/current-operations/operation-horizon.html.

[16] Mercedes Stephenson and Sean Boynton, "Canada Alarmed as Chinese Fighter Pilots 'Buzz' Canadian Planes over International Waters," Global News, June 1, 2022, https://globalnews.ca/news/8885980/canada-china-pilots-buzz-planes-asia/; Jamie Seidel, "'How Wars Start': Close Call Reveals Terrifying China Reality amid Warship Showdown," news.com.au, June 6, 2023, https://www.news.com.au/technology/innovation/military/how-wars-start-close-call-reveals-terrifying-china-reality-amid-warship-showdown/news-story/185b4e476dd481eafbb8ad3588218f70.

[17] Scott N. Romaniuk, "The Houthis and Maritime Vulnerability: Implications for 2026 – Analysis," Eurasia Review, January 5, 2026, https://www.eurasiareview.com/05012026-the-houthis-and-maritime-vulnerability-implications-for-2026-analysis/.

[18] European Parliament, "Recent Threats in the Red Sea," 2024, https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/760390/EPRS_BRI(2024)760390_EN.pdf, p. 2.

[19] BBC News, "Who are the Houthis and why is the US targeting them," March 25, 2025, https://www.bbc.com/news/world-middle-east-67614911.

[20] Robert Martyn, "Robotic Kraken: Trends in Uncrewed Maritime Systems," Kingston Consortium on International Security, January 22, 2025, https://www.thekcis.org/publications/insights/insight-5-3.

[21] Concepts, Interoperability and Capability Branch, "CIMIC Contribution to Operations in the Bad-al-Mandeb and the Red Sea, Civil-Military Cooperation Centre of Excellence, 2024, https://www.cimic-coe.org/wp-content/uploads/2025/01/factsheet-operation-prosperity-guardian-aspides.pdf, p. 4.

[22] National Defence, "Canada to Participate in United States-led Operation PROSPERITY GUARDIAN," Government of Canada, December 19, 2023, https://www.canada.ca/en/department-national-defence/news/2023/12/canada-to-participate-in-united-states-led-operation-prosperity-guardian.html.

[23] Paula Newton, "How Canada is Positioning Itself on Greenland Knowing it Could Be Next," CNN, January 20, 2026, https://www.cnn.com/2026/01/20/americas/canada-greenland-trump-analysis-latam-intl.

[24] Katherine Doyle, Carol E. Lee, Courtney Kube and Kristen Welker, "Trump's Latest Western Hemisphere Fixation: Canada," NBC News, January 18, 2026, https://www.nbcnews.com/politics/white-house/trumps-latest-western-hemisphere-fixation-canada-rcna254552.

[25] Department of War, "2026 National Defense Strategy," United States of America, January 23, 2026, https://media.defense.gov/2026/Jan/23/2003864773/-1/-1/0/2026-NATIONAL-DEFENSE-STRATEGY.PDF p. 3.

[26] Murray Brewster, "Canada's Military Plans to be in the Arctic 'on a Near Permanent Basis' says Commander," CBC News, May 15, 2025, https://ici.radio-canada.ca/rci/en/news/2165304/canadas-military-plans-to-be-in-the-arctic-on-a-near-permanent-basis-says-commander.

[27] Canada Infrastructure Bank, "Grays Bay Road and Port," n.d., https://cib-bic.ca/en/projects/trade-and-transport/grays-bay-road-and-port-project-2/; Prime Minister of Canada, "Joint Statement by Prime Minister Mark Carney and Premier Wab Kinew on Federal-Provincial Collaboration Regarding Port of Churchill Plus," November 16, 2025, https://www.pm.gc.ca/en/news/statements/2025/11/16/joint-statement-prime-minister-mark-carney-and-premier-wab-kinew.

[28] National Defence, "NORAD Modernization Project Timelines," Government of Canada, November 22, 2024, https://www.canada.ca/en/department-national-defence/services/operations/allies-partners/norad/norad-modernization-project-timelines.html.

[29] Robert Martyn, "Robotic Kraken," Guido L. Torres and Austin Gray, "Sailing Through the Spyglass: The Strategic Advantages of Blue OSINT, Ubiquitous Sensor Networks, and Deception," Atlantic Council, August 8, 2024, https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/sailing-through-the-spyglass-the-strategic-advantages-of-blue-osint-ubiquitous-sensor-networks-and-deception/.

[30] Jill Goldenziel, "China Claims to Own the Taiwan Strait. That's Illegal;" Jan Jakub Solski, "The US Arctic Gambit: Testing the Limits of UNCLOS," The Arctic Institute, January 16, 2024, https://www.thearcticinstitute.org/us-arctic-gambit-testing-limits-unclos/.

[31] Elena Chachko and Abraham Newman, "Building Norms of Economic Coercion," Journal of International Economic Law 28, no. 3 (September 2025): 542–59, https://doi.org/10.1093/jiel/jgaf035.

[32] Luke Coffey, "Arctic Region Becoming Increasingly Contested," Hudson Institute, December 5, 2025, https://www.hudson.org/foreign-policy/arctic-region-becoming-increasingly-contested-luke-coffey.

[33] National Defence, "Royal Canadian Navy to Pay Off Kingston-class Vessels;" Public Services and Procurement Canada, "Government of Canada Advances to Next Step in Canadian Patrol Submarine Project Procurement;" Public Services and Procurement Canada, "Large Vessel Shipbuilding Projects," Government of Canada, November 3, 2025, https://www.canada.ca/en/public-services-procurement/services/acquisitions/defence-marine/national-shipbuilding-strategy/projects/large-vessels.html; Kate Todd, "Redesigning the Royal Canadian Navy for a More Dangerous World."

[34] Kate Todd, "Lessons for Canada: Comparing Maritime Autonomous Systems Adoption Across the Five Eyes," Canadian Global Affairs Institute," September 2025, https://www.cgai.ca/lessons_for_canada_comparing_maritime_autonomous_systems_adoption_across_the_five_eyes; Guido L. Torres and Austin Gray, "Sailing Through the Spyglass."

AIR

Explaining Integrated Air and Missile Defence for Canada

Nicholas Glesby

Royal Canadian Air Force CF-188 Alpha Hornet from 425 Tactical Fighter Squadron.
Photo Credit: Combat Camera

Nicholas Glesby is a Ph.D. Student in the School for the Study of Canada at Trent University, Administrator of the MINDS-funded North American and Arctic Defence and Security Network (NAADSN), and Student Fellow at the Centre for Defence and Security Studies at the University of Manitoba.

Renewed great power competition, increased attention to the circumpolar Arctic, and Russia's war in Ukraine have forced Canada to rethink both how to defend itself and its role to play in continental defence. Today, North America faces a complex threat environment, where the Arctic Ocean serves as the fastest avenue of approach, with threats travelling through the region to strike southern Canada or the United States (US).[1] Russia and China have successfully fielded delivery systems that can target any location on the continent – including long-range cruise missiles, hypersonics, and sea-launched and intercontinental ballistic missiles that can be fitted with conventional or nuclear warheads. Iran and North Korea remain long-term concerns. The threat environment thus requires next-generation integrated air and missile defence (IAMD) to protect critical civilian and defence infrastructure that adversaries can target anywhere on the North American continent. Canada has now removed existing restrictions on IAMD, and the same functional logic that drove North American Aerospace Defense Command's (NORAD) binational integration applies given proximity of Canadian and American infrastructure along the border that benefits both nations, such as the St. Lawrence Seaway.[2] Owing to a combination of factors, Canada will still need to pursue national IAMD given the complex threat environment, regardless of participation in the United States' Golden Dome initiative.[3]

This analysis examines what the Golden Dome would entail, Canadian considerations for participation, the current state of IAMD policy, and NORAD modernization commitments. Weighing the advantages and disadvantages of Canada participating in the Golden Dome, the paper recommends that Canada should become a full partner – given the complexity of the North American threat environment, the need to achieve national IAMD, and the imperative to fully contribute to continental defence.

The Golden Dome for America

US Presidential Executive Order (PEO) 14186 of January 2025 seeks to build an "Iron Dome for America", now referred to as "Golden Dome". The PEO outlines "the threat from next-generation strategic weapons has become more intense and complex with the development by peer and near-peer adversaries of next-generation delivery systems and their own homeland integrated air and missile defense capabilities."[4] US President Trump has made IAMD a priority for US homeland defence through Golden Dome, with an ambitious target of full operational deployment by 2028. IAMD is necessary throughout the continuum of competition, crisis, and conflict. It is conducted with a 360-degree approach using systems based in the sea, land, air and space to track, target, and defeat air and missile threats, emanating from all strategic directions, and coming from both state and non-state actors.[5]

The PEO further acknowledges that "the world is in a new age in terms of the variety, speed and accuracy of air and missile threats that demand air and missile defence."[6] The Golden Dome would amalgamate layered sensor and interceptor capabilities such as (but not limited to) radar stations, ground and sea-based missile batteries, and fighter jets into an overarching ecosystem from seabed to space at a scale and scope not seen globally. This would enable the United States to deter, detect, and defeat air-breathing and aerospace threats.[7] However, there is no singular "exquisite" system that can be built nor bought to achieve perfect coverage and accuracy.[8] Former NORAD/US Northern Command (USNORTHCOM) Commander Glen VanHerck (2020-2023) states that "a one-size-fits-all solution is not the answer," instead preferring the combination of new and existing systems.[9]

Building on his predecessor's assessment, NORAD/USNORTHCOM Commander Gregory Guillot (2024-Present) envisions the Golden Dome as three parallel systems: First, a domain-awareness dome integrating stove-piped, national sensors across domains to deliver real-time information into a single common operating picture; second, an ICBM dome to detect, track, and defeat emerging systems; and third, a cruise-missile and air threat dome at low altitudes for remotely piloted systems (RPAS), aircraft, and

low-flying cruise missiles. Guillot emphasized that "the three nodes must be resilient, interconnected, and tailored to defeat specific threats," and reflect "the complex strategic environment and the reality of a homeland at risk."[10] The reason for the three domes, as opposed to one exquisite system described by Trump, is that no defeat system can manage the different vectors and speeds of the various types of missiles.

Canadian Considerations for Integrated Air and Missile Defence

Canada already partially contributes to the domain-awareness and air-threat domes Guillot proposes through NORAD, but does not participate in the ICBM dome due to past policy restrictions on ballistic missile defence (BMD).[11] Since 1957, Canada and the United States have jointly defended the approaches to North America through NORAD. NORAD is North America's first line of defence, responsible for aerospace warning and control and maritime warning of Canada and the continental US. Following years of warning that North America was "no longer a sanctuary" amidst shifting global military and political dynamics,[12] Canada pledged a generational investment in 2022 to defend Canada, contribute to continental defence, and help modernize the command.[13]

Canada has gradually shifted its position on participating in missile defence. The 2022 NORAD modernization commitments invest in all-domain IAMD research, development, and innovation.[14] In addition, Canada's current defence policy, 2024's *Our North, Strong and Free*, states that modern missiles "threaten to overwhelm [Canada's] existing air defence systems and impose new challenges on our ability to support allies and partners around the world."[15] In October 2025, Canadian Chief Air and Space Force Development Major General J.D. Smyth stated that Canada has worked towards participating in Golden Dome by committing to dozens of NORAD modernization commitments. These include new radars, satellites, maritime sensors, aircraft, and command-and-control systems.[16] In October 2025, Minister of National Defence David McGuinty also recognized that Canada "needs to be able to detect what's coming at us," saying that "[Canada] may have three-and-a-half or four minutes to be able to respond to the kind of capabilities that we're seeing now that are out there – that a number of states possess."[17] The geostrategic context has now forced Canada to consider full participation in IAMD.

Canada has been "invited" by Trump to join Golden Dome for $61 billion USD, nearly a third of the approximated $175 billion cost.[18] Ottawa is weighing its next steps and has facilitated conversations by ending its "no" decision of 2005 to not participate in BMD. Notably, on 16 July 2025, Minister McGuinty "confirmed that the Government has removed all restrictions on air and missile defence of Canada (…) to better deter and defend against threats to our country's sovereignty, population, and critical infrastructure."[19] This announcement still requires further details on what it means for Canada to participate in either BMD or Golden Dome, but is a positive step towards doing so.

Prime Minister Mark Carney has said that participating in Golden Dome is "[…] something that we are looking at and something that has been discussed at a high level."[20]

If Canada participates, that choice will be motivated by the same logic that has long driven the binational defence relationship; North American security is indivisible and Canada will not permit its territory to be used by adversaries to threaten or attack the US.[21]

This thinking continues to steer Canada's approach to continental defence.[22] As a partner in defending North America, Canada contributes domain awareness of the northern avenues of approach through the North Warning System (NWS) which is a product of 1970s technology and "was not designed to detect modern weapons and delivery systems, such as long-range cruise and hypersonic missiles."[23] To solve the issue of inadequate domain awareness coverage, Canada's NORAD modernization commitments invest in an Arctic Over-the-Horizon Radar (A-OTHR) system, future Polar-OTHR (P-OTHR)/ North Watch system, satellites, and ground and maritime sensors outlined in the NORAD modernization commitments to detect missile launches sooner, providing greater time for early-warning.[24] Domain awareness assists senior leaders by providing more time and space for decision-making options to respond with, and therefore is NORAD's priority.

IAMD requires coordination of air and missile defence assets across all domains into a system-of-systems with a single chain-of-command.[25] Yet, NORAD already participates in IAMD, but its role ends with tracking and warning when it comes to ICBMs.[26] NORAD's aerospace warning detects and tracks aerospace threats to North America, including global missile warning, as NORAD has a global area of operations for warning purposes. Defeating ballistic missiles rests with USNORTHCOM through the US Ground Based Midcourse Defense (GMD) system for now.[27] As Canada opted out of participating in BMD in 2005, Canadians assigned to NORAD assist by warning on incoming ballistic missiles. As a result, USNORTHCOM manages the defeat decision and has no mandate or requirement to protect Canada.[28] Canada's "no" to BMD means NORAD's aerospace control is currently limited to defeating aircraft, cruise missiles, and RPAS. Given that all restrictions have been lifted, talks can begin about Canada's participation in any of the Golden Dome mission sets and whether the defeat mechanism would be folded into NORAD.[29]

The 2025 US National Security Strategy is focused on hemispheric defence which requires allies to prioritize greater burden-sharing.[30] Indeed, Canada is making sustained and novel investments to defend the continent through NORAD modernization and is increasingly recognizing the need for IAMD to protect vital infrastructure. As the Canada-US relationship is at a historic nadir, further continental defence integration within Golden Dome is a challenging discussion politically, financially, technologically, and operationally. However, the same functional logic that dictated the need for joint air defence of North America should guide Canada-US cooperation on IAMD. After all, a missile attack on any northern US city or infrastructure will likely devastate Canadian sites as well given propinquity.

Advantages and Disadvantages of Canadian Participation in Golden Dome

Opponents propose Golden Dome undermines strategic stability and weakens international norms.[31] However,

given the complex threat environment, opting out of Golden Dome would weaken Canada's reputation and marginalize NORAD.

There are three major considerations should Canada choose not to participate. First, defending critical civilian and military infrastructure is necessary regardless of participation. These sites are identified and prioritized through critical and defended asset lists (CAL/DAL), which, in Canada, are the responsibility of National Defence and Public Safety. Given adversaries' ability to target any site in North America, defending critical infrastructure is paramount.[32] Examples of critical civilian infrastructure include ports, electrical grids, and rail links; defence infrastructure includes ammunition depots and bases.[33] Defending CAL/DAL will require merging numerous national organizations and systems responsible for specific missions, and integrating detection and defeat systems across domains.[34] This is a challenging command and control task, made more difficult by the proximity of US CAL/DAL to Canadian sites. Andrea Charron suggests Canada will need its own point defence systems, linked with Golden Dome, to protect CAL/DAL far away from the border regardless of participation in order to protect national assets.[35] Integrating IAMD with the US binationally would therefore create additional options for Canada to respond to a wide array of threats, especially important as much of the CAL/DAL along the border benefits both countries.[36]

Second, participation in Golden Dome could benefit Canadian interests in non-defence and security areas of the broader bilateral relationship. The Canada-US relationship is at a historic nadir, brought upon by Trump's threats of annexation and economic coercion through punishing tariffs. Disagreements in one area of the bilateral relationship are now spilling into others given Trump's maximalist negotiating tactics. Carney recognizes this balancing act when negotiating with the current White House, as his speech in Davos declared that "if we're not at the table, we're on the menu."[37] Now is a precipitous time for conversations on IAMD with the upcoming review of the Canada-United States-Mexico Agreement (CUSMA) on free trade, although Canada's decision to lift IAMD restrictions this past July shows commitment to deeper collaboration to defend the continent.

Third, Canada risks marginalizing its "knowledge of, access to, and influence over US thinking and plans for continental defence" by not participating.[38] Declining commitment of resources and capabilities to Golden Dome means that the United States could push Canadian interests to the wayside, with what

James Fergusson warns as the "implicit re-nationalization of North American defence, contrary to Canadian strategic interests."[39] Doing so may also increase pressures on US rhetoric around Greenland, although the 1951 US-Danish Defense Agreement allows the US to place infrastructure such as sensors and interceptors supporting Golden Dome in the territory.[40] A Canadian "no" to Golden Dome defies the functional logic that the defence of the continent is indivisible. Canadian officials have referred to both a "continental shield" and a "Canadian shield", but further definition of how these concepts fit into Canadian and North American defence is needed.[41]

Conclusion

Canada is a committed partner in the defence of North America, evidenced through NORAD modernization commitments and progress made thus far. Projects must continue apace. As adversaries possess the capability to strike anywhere on the continent, Golden Dome faces complications across political and operational spectrums, combined with an eager and costly timeline. Clear policy guidance from Washington about the resources and capabilities Canada is expected to contribute to Golden Dome would aid Ottawa's long-term planning, with the Canada-United States Permanent Joint Board on Defence (PJBD) serving as a potential forum for these sensitive discussions.[42] Should Canada not participate, national critical infrastructure will still need to be protected, the US may violate Canadian airspace with ground-based interceptors at will, domain awareness data siloed, and Canadian interests could be dismissed in favour of US re-nationalization of continental defence.[43] The functional logic which drove Canada and the US to integrate defences and create NORAD applies to IAMD.[44] Already partially involved in IAMD through NORAD's mission suites, Canada can and should participate in Golden Dome to defend critical infrastructure, maximize available response options across domains, and send a clear message of resolve to defend North America.

The author would like to thank Dr. Andrea Charron and CDA Institute for their expert advice and feedback.

Notes

[1] P. Whitney Lackenbauer, "Threats Through To, and In the Arctic: A Framework for Analysis," *North American and Arctic Defence and Security Network*, 23 March 2021, https://www.naadsn.ca/wp-content/uploads/2021/03/Lackenbauer_Threats-Through-To-and-In-the-Arctic.pdf.

[2] For more on the functional logic which drove Canada and the United States to integrate air defences, see: Andrea Charron and James Fergusson, *NORAD: In Perpetuity and Beyond*, (Montreal/Kingston: McGill-Queen's University Press, 2022), 13, 16; Andrea Charron, "Golden Dome and Canada: The "New" Age of Integrated Air and Missile Defence," *CDA Institute*, 25 August 2025, https://cdainstitute.ca/golden-dome-and-canada-the-new-age-of-integrated-air-and-missile-defence/.

[3] Charron, "Golden Dome and Canada: The "New" Age of Integrated Air and Missile Defence."

[4] "The Iron Dome for America," *The White House*, 27 January 2025, https://www.whitehouse.gov/presidential-actions/2025/01/the-iron-dome-for-america/; It has been suggested that US military planners are deeply concerned about the implications of Russia's use of hypersonics, and "ground-hugging" cruise missiles and drones during their invasion of Ukraine. For more, see: Murray Brewster, "The Golden Dome is where Canada's F-35 debate and Trump's Greenland threat meet," *CBC News*, 31 January 2026, https://www.cbc.ca/news/politics/f35-greenland-canada-missile-defence-9.7069059.

[5] "NATO Integrated Air and Missile Defence," *North Atlantic Treaty Organization*, 13 February 2025, https://www.nato.int/en/what-we-do/deterrence-and-defence/nato-integrated-air-and-missile-defence.

[6] See Andrea Charron's parliamentary testimony: Canada, Parliament, House of Commons, Standing Committee on National Defence (NDDN), *Evidence*, 1st session, 25th Parliament, Number 011, 9 October 2025, https://www.ourcommons.ca/documentviewer/en/45-1/NDDN/meeting-11/evidence.

[7] Brewster, "The Golden Dome is where Canada's F-35 debate and Trump's Greenland threat meet": The Office of Golden Dome for America in the Pentagon has proposed architecture including "four integrated layers – one satellite-based and three land-based with a notional 11 short-range missile batteries positioned across the continental United States, Alaska, and Hawaii." See: Mike Stone, "Pentagon to get first official briefing on Golden Dome missile shield architecture," *Reuters*, 17 September 2025, https://www.reuters.com/business/aerospace-defense/pentagon-get-first-official-briefing-golden-dome-missile-shield-architecture-2025-09-17/; "

[8] Charron, "Golden Dome and Canada: The "New" Age of Integrated Air and Missile Defence."

[9] Glen VanHerck and Pete Fesler, "'Iron Dome' for America: A Fresh Look at Homeland Defense," *National* interest, 17 February 2025, https://nationalinterest.org/feature/iron-dome-for-america-a-fresh-look-at-homeland-defense.

[10] Gregory M. Guillot, "Statement of General Gregory M. Guillot, United States Air Force, Commander, United States Northern Command and North American Aerospace Defense Command," *House Armed Services Committee – Strategic Forces*, 9 April 2025, 12-14, https://www.congress.gov/119/meeting/house/118115/witnesses/HHRG-119-AS29-Wstate-GuillotG-20250409.pdf.

[11] Charron, "Golden Dome and Canada: The "New" Age of Integrated Air and Missile Defence"; For the seminal work on Canada and BMD, see: James Fergusson, *Canada and Ballistic Missile Defence, 1954-2009: Dējā Vu All Over Again*, (Vancouver: UBC Press, 2010).

[12] Terrence J. O'Shaughnessy, "Statement of General Terrence J. O'Shaughnessy, United States Air Force Commander, United States Northern Command, and North American Aerospace Defence Command," *Senate Armed Services Committee*, 26 February 2019, 2, https://www.armed-services.senate.gov/imo/media/doc/OShaughnessy_02-26-19.pdf.

[13] Department of National Defence, "Minister Anand announces continental defence modernization to protect Canadians," *Government of Canada*, 20 June 2022, https://www.canada.ca/en/department-national-defence/news/2022/06/minister-anand-announces-continental-defence-modernization-to-protect-canadians.html; Canada has made progress on NORAD modernization commitments, such as renewing Forward Operating Locations (FOLs), Arctic Over-the-Horizon Radar (A-OTHR), and the first F-35 aircraft are set to be delivered later this year.

[14] Department of National Defence. "NORAD modernization project timelines." *Government of Canada*, last modified 22 November 2024. https://www.canada.ca/en/department-national-defence/services/operations/allies-partners/norad/norad-modernization-project-timelines.html.

[15] Department of National Defence, *Our North, Strong and Free: A Renewed Vision for Canada's Defence*, (Ottawa: His Majesty the King Right of Canada as represented by the Minister of National Defence, 2024), 13, https://www.canada.ca/content/dam/dnd-mdn/documents/corporate/reports-publications/2024/north-strong-free-2024-v2.pdf.

[16] Gavin John, "Canada has been working for years to prepare for Golden Dome, Air Force general says," *The Globe and Mail*, 9 October 2025, https://www.theglobeandmail.com/canada/article-canada-prepare-golden-dome-air-force-general/.

[17] Steven Chase, "McGuinty defends Canada's Golden Dome collaboration with U.S., citing potential threats," *The Globe and Mail*, 8 October 2025, https://www.theglobeandmail.com/canada/article-trump-golden-dome-missile-defence-system-canada/.

[18] Three years is an ambitious timeline. Andrea Charron suggests that "this will not be a one and done system but rather will be built over the time with mainly 'off the shelf' options (systems already tested and operational)." For more, see: Charron, "Golden Dome and Canada: The "New" Age of Integrated Air and Missile Defence."

[19] "Minister McGuinty visits NORAD."

[20] Nadine Yousif, "Carney says Canada in talks to join Trump's Golden Dome defence system," *BBC News*, 21 May 2025, https://www.bbc.com/news/articles/cy4ee9jmk17o.

[21] The origin of the Canada-US defence relationship is The Ogdensburg Agreement of 18 August 1940, a one-page press release creating the binational Canada-United States Permanent Joint Board on Defence (PJBD) to coordinate the defence of North America during the Second World War. For an explanation of the functional logic which drove Canada and the US to integrate defences, see: Charron and Fergusson, *NORAD: In Perpetuity and Beyond*, 13-16.

[22] Michel Fortmann and David G. Haglund, "Canada and the Issue of Homeland Security: Does the 'Kingston Dispensation' still hold?" Canadian Military Journal 3, no. 1, (Spring 2002): 17-23.

[23] Department of National Defence, "North American Aerospace Defense Command (NORAD) Backgrounder," *Government of Canada*, 22 June 2022, https://www.canada.ca/en/department-national-defence/news/2022/06/north-american-aerospace-defense-command-norad.html.

[24] "NORAD modernization project timelines."

[25] See Charron's testimony to NDDN, 9 October 2025, https://openparliament.ca/committees/national-defence/45-1/11/andrea-charron-1/; James Fergusson, "The Canadian Ballistic Missile Dilemma," *Canadian Global Affairs Institute*, April 2025, https://www.cgai.ca/th_pp_canadian_ballistic_missile_dilemma.

[26] Charron and Fergusson, *NORAD: In Perpetuity and Beyond*, 124.

[27] Charron, "Golden Dome and Canada: The "New" Age of Integrated Air and Missile Defence."

[28] Andrea Charron and James Fergusson, "From NORAD to NOR[A]D: The Future Evolution of North American Defence Co-Operation," *Canadian Global Affairs Institute*, May 2018, https://www.cgai.ca/from_norad_to_nor_a_d_the_future_evolution_of_north_american_defence_co_operation.

[29] NORAD's warning missions also fits within the Pentagon's goal of achieving Joint All Domain Command and Control for global detection of approaching threats to ensure sufficient early warning to protect North America. For more, see: "Joint All-Domain Command and Control: Background and Issues for Congress." *Congressional Research Service*, 12 August 2021, https://www.congress.gov/crs_external_products/R/PDF/R46725/R46725.7.pdf.

[30] Government of the United States, *National Security Strategy of the United States of America*, (Washington, D.C.: The White House, 2025), https://www.whitehouse.gov/wp-content/uploads/2025/12/2025-National-Security-Strategy.pdf.

[31] Jessica West and Kathryn Barrett, "Golden Dome Explained: Ambition, Reality, Risk," *Project Ploughshares*, 15 July 2025, https://ploughshares.ca/golden-dome-explained-ambition-reality-risk/.

[32] Charron, "Golden Dome and Canada: The "New" Age of Integrated Air and Missile Defence."

[33] NATO, "Resilience, civil preparedness and Article 3," *North Atlantic Treaty Organization*, 13 November 2024, https://www.nato.int/en/what-we-do/deterrence-and-defence/resilience-civil-preparedness-and-article-3; Charron, "Golden Dome and Canada: The "New" Age of Integrated Air and Missile Defence"; Fergusson, "The Canadian Ballistic Missile Dilemma."

[34] Charron, "Golden Dome and Canada: The "New" Age of Integrated Air and Missile Defence."

[35] *Our North, Strong and Free* committed Canada "to invest in integrated air and missile defence capabilities alongside NATO allies to continue to protect Canadians at home and abroad." See: *Our North, Strong and Free*, 13.

[36] See Andrea Charron and Scott Clancy in: Chris Lambie, "Opting out of F-35 purchase would be 'three ways from Sunday stupid,' says retired major general," *National Post*, 28 January 2026, https://nationalpost.com/news/canada/what-is-norad-why-this-security-agreement-allows-u-s-fighter-jets-to-patrol-canadian-airspace#:~:text=Canada%20opting%20out%20of%20the,Article%20content.

[37] Prime Minister Carney's 20 January 2026 speech in Davos may "be remembered as one of the most profound, courageous, and important speeches by a Canadian political leader on the international stage." For additional analysis and a transcript of the prime minister's remarks, see: P. Whitney Lackenbauer, Andrea Charron, Peter Kikkert, Suzanne Lalonde, Kari Roberts, Jackson Walling and Rory Jakubec, "'Values-Based Realism,' Middle Powers, and a New World Order: Prime Minister Carney's Davos Speech," *North American and Arctic Defence and Security Network*, 21 January 2026, https://www.naadsn.ca/wp-content/uploads/2026/01/26jan21-Values-Based-Realism-Carney-NAADSN-QI.pdf.

[38] Fergusson, *Canada and Ballistic Missile Defence, 1954-2009*, 122.

[39] Fergusson, "The Canadian Ballistic Missile Dilemma."

[40] Troy Bouffard, Steven Phillips, James Morton, and Cameron Carlson, "The Strategic Importance of Greenland: The Role of Tactical Missile and Air Defense in the Arctic," *Small Wars Journal*, 13 October 2025, https://smallwarsjournal.com/2025/10/13/greenland-missile-defense-strategy/.

[41] P. Whitney Lackenbauer, "NORAD Modernization, Golden Dome, and/or 'Canadian Shield'? Canada Needs its Own Narrative," *North American and Arctic Defence and Security* Network, 9 October 2025, https://www.naadsn.ca/wp-content/uploads/2025/10/25oct9-NORADmod-NDDN-lackenbauer-QI.pdf.

[42] Andrea Charron, Nicholas Glesby, Laura Conrad, and Channah Greenfield, "The Permanent Joint Board on Defence (PJBD): How Permanent and Joint? Celebrating 80 Years of Cooperation," *Centre for Defence and Security Studies*, 25 February 2020, https://umanitoba.ca/arts/sites/arts/files/2022-07/The-Permanent-Joint-Board-on-Defence-final-workshop-report_2020.pdf; The PJBD's last meeting in October 2024 resulted in the first-ever readout of the discussions held. It has a legacy of providing binational advice directly to political leaders on how to resolve difficult issues in the relationship. See: Department of National Defence, "The 242nd Meeting of the Permanent Joint Board on Defense," *Government of Canada*, 14 November 2024, https://www.canada.ca/en/department-national-defence/news/2024/11/the-242nd-meeting-of-the-permanent-joint-board-on-defense.html.

[43] Charron, "Golden Dome and Canada: The "New" Age of Integrated Air and Missile Defence"; Fergusson, "The Canadian Ballistic Missile Dilemma."

[44] Charron and Fergusson, *NORAD: In Perpetuity and Beyond*.

LAND

Lessons from the Russia-Ukraine War: Adaptation, Resilience, and Implications for Modern Militaries

Howard G. Coombs

Operation REASSURANCE: enhanced Forward Presence (eFP).
Photo Credit: Combat Camera

Dr. Howard G. Coombs is an Associate Professor of History at the Royal Military College of Canada and Associate Director of Defence Outreach at the Centre for International and Defence Policy at Queen's University. Coombs has over four decades of service in the regular and reserve forces. His research interests include Canadian professional military education and Canadian military operations and training. His most recent publication was the co-edited volume *The Northern Flank - The Arctic: Implications for SOF*, published by the Canadian Special Operations Forces Command in 2025.

Introduction

From December 8-12, 2025, a Lessons Learned team from the Ukrainian National Defence University traveled to Canada, delivering briefings in Toronto, Kingston, and Ottawa to highlight lessons learned for Canadians during the ongoing Russia-Ukraine War. What became quickly apparent is that modern war is best understood as competition between adaptive systems rather than a duel between fixed orders of battle. In Ukraine's experience, every advantage quickly becomes temporary. A new drone design triggers changes in electronic warfare; a revised artillery method drives camouflage and dispersion; deeper mining, new sensors, or different force packaging counter a successful tactical pattern. The decisive edge, therefore, comes not from perfection but from the capacity to evolve faster than an opponent while preserving legitimacy and public support.

This perspective reshapes what "readiness" means. Traditional assumptions that doctrine, training pipelines, and procurement cycles can operate at peacetime tempo are ill-suited to a war in which relevant lessons may emerge and change within weeks. Ukrainian presenters described learning as a closed loop: frontline observation, rapid validation, dissemination through professional education channels, and field implementation, followed by further refinement. *The loop is as important as the individual innovation.*

For partner militaries, such as Canada's, the implication is systemic. Adaptive capacity depends on institutions that can absorb stress without fragmenting: clear command intent, empowered junior leaders, resilient logistics, and public trust. It also depends on disciplined experimentation, where change is introduced, measured, and updated rather than celebrated and forgotten. In high-intensity war, "adaptation" is not a supporting effort. It is the core function that converts hardship into advantage.

Information warfare as a permanent front

Ukrainians stress that Russia's information war did not begin in February 2022. It was a long-running campaign to shape narratives, normalize aggression, and erode confidence in institutions. Social media and messaging platforms enable propaganda at scale, rapid impersonation of local voices, and micro-targeting of existing grievances. The delegation highlighted a particularly corrosive practice: hostile actors embedding themselves in routine community networks – local chat groups used for schools, neighbourhoods, and municipal life – well before major operations. Those spaces were then exploited to observe social dynamics, test narratives, and, when the invasion began, solicit information and spread panic.

Several practical lessons follow. Information defence must be treated as a continuous national security function, not an improvised wartime activity. The goal is not only to rebut but also to prevent, through societal "immunity": critical thinking, media literacy, and an understanding of how manipulation works. In crisis, coordination is decisive; fragmented messaging creates openings that adversaries exploit. Finally, information operations targeting Ukraine were aimed at partners, seeking to delay support and, therefore, fracture cohesion. Countermeasures must be coordinated across allies and at home.

Strategic evolution and the logic of attrition

The war's strategic evolution is a story of failed assumptions, constraints, and adaptation. Russia's initial attempt to force rapid political collapse through a swift advance on Kyiv relied on poor intelligence, unrealistic political expectations, and an underestimation of Ukrainian cohesion. When a quick victory failed, Russia shifted toward a protracted approach: territorial consolidation, mobilization, and attrition designed to exhaust manpower, infrastructure, and will.

Ukraine's strategy also evolved. In 2022, total defence aimed to blunt the invasion, preserve the state, and deny Russia decisive gains. Once state survival was secured, Ukraine pursued counteroffensives to regain initiative and liberate territory. The presenters were frank about the structural challenges of prolonged high-intensity conflict: casualties accumulate, trained personnel are finite, and key munitions and air defence often depend on external supply.

The central lesson for partners is that modern war becomes a multi-domain contest of endurance – moral, physical, economic, and informational – where the advantage goes to the system that can regenerate and adapt longer.

Russia's operational and tactical adaptation

Russian adaptation seems to have been uneven but consequential. At the operational level, there have been efforts to improve coordination through revised command arrangements and joint groupings, as well as adjustments to logistics structures and training pipelines. These changes did not produce seamless joint integration, but they reduced early friction and enabled sustained pressure across multiple axes.

At the tactical level, there has been a shift from massed formations to smaller, more survivable maneuver elements with limited daily objectives. These groups probe, infiltrate, and steadily shape the battlefield while presenting a more challenging target set in environments where defenders cannot afford to expend scarce fires on every contact. Ukrainians highlight the enduring centrality of artillery, increasingly paired with drones for observation and correction. Engineering support has become a defining feature of the ground fight: deep fortification lines, extensive mining, and layered defensive zones designed to channel movement and punish concentration.

The overarching point is that an adversary does not need to innovate elegantly to become more dangerous. Adapting to constraints can produce effective methods that exploit the defender's shortages, mainly when those shortages include munitions, air defence coverage, and trained personnel. For NATO planners, the lesson is to assume a learning opponent. Early enemy failure is not reassurance; it may be the beginning of a more resilient and more lethal approach to attritional warfare.

Ukraine's operational adaptation and learning architecture

Ukraine's battlefield adaptations were repeatedly linked to institutional learning rather than improvisation alone. Command arrangements were adjusted to improve control and responsiveness across expanding frontages. Authority and initiative increasingly moved downward, both because modern sensors punish centralized signatures and because electronic warfare and strikes can sever communications at critical moments. The ability of small units to act with intent and then re-synchronize when communications return was presented as essential.

Equally important was the mechanism that moved lessons from the front into the force. Ukrainian instructors rotate through operational zones, observe current enemy tactics and friendly methods, and then return to update training. This is portrayed as a practical answer to the "innovation gap" between training institutions and battlefield reality. The war also forced the decentralization of training infrastructure: fixed sites were vulnerable and often targeted, requiring dispersed locations, concealment, and austere delivery methods.

The Armed Forces of Ukraine believe that this learning architecture constitutes combat power. It reduces the time between discovery and field change, allowing the force to keep pace in the adaptation battle. It also helps create coherence. Rapid change without dissemination leads to fragmentation; rapid change with shared learning creates a force that can evolve while still operating as a single system.

NCO development and training under fire

Professional military development, particularly the role of non-commissioned officers, was presented as a decisive institutional lesson. Ukraine began the war with an NCO culture still shaped by Soviet-era patterns, where NCO authority and education were limited compared to many NATO models. Reforms after 2014 sought to professionalize the NCO corps and extend leadership roles upward. Still, the full-scale invasion disrupted training capacity and created an immediate demand for squad-level leaders.

In response, Ukrainian trainers prioritized essentials. Leadership curricula were shortened and refocused on survivability, decision-making, and small-unit leadership. Instructors often shifted between teaching and combat rotations, returning with current lessons and credibility. International training opportunities provided by partners helped generate scale but introduced friction when partner procedures differed. The delegation described a solution based on standardization and liaison: sending Ukrainian programs abroad, coordinating with training centers, and embedding instructors who could ensure alignment with national methods.

A particularly telling feature was the speed of horizontal knowledge sharing. When new weapons arrived in multiple variants, NCO networks helped spread "how-to" information quickly through videos, pocket guides, and simple digital distribution. The broader lesson for Canada and NATO is that high-intensity conflict demands empowered junior leaders, especially when communications degrade. NCO authority, education, and career systems must be built before a crisis, not assembled during it.

Air warfare, air defence, and the drone ecosystem

Air and drone warfare were among the most transformative themes. Ukraine's early dispersion and concealment of air defence and aviation assets helped prevent Russia from achieving uncontested air superiority. As losses mounted and air defences remained dense, Russia reduced close-in tactical aviation. It leaned on standoff strike: cruise missiles, guided aerial bombs delivered from outside the most dangerous zones, and sustained drone campaigns against military targets and critical infrastructure.

Drones are now ubiquitous tools for reconnaissance, targeting, strike, and psychological effects. Their rapid evolution has been a characteristic of this war. These changes have included improved navigation, resistance to jamming, better sensors, mass production, and tighter integration with artillery and electronic warfare. Ukrainians emphasize that the economics of defence are decisive. It is not sustainable to defeat cheap drones only with expensive missiles. Ukraine has therefore pursued a layered defence that combines high-end systems for priority threats with mobile fire teams, electronic warfare, passive protection, and low-cost interceptors. For partner militaries, such as Canada, the implication is that they treat air defence and counter-UAS as a single ecosystem that must be trained and sustained for long-duration pressure, rather than episodic attacks.

Logistics, sustainment, and unmanned support

Logistics was framed as a contested domain in which survivability is now as important as capacity. Efforts are ongoing to align logistics concepts with NATO-like structures, including standardized supply classes and an increased use of digital tools for tracking and management. Precision strikes and surveillance have forced dispersion, concealment, and the use of hardened or underground infrastructure for storage and accommodation. Large, predictable depots and routes are liabilities; sustainment must be modular, mobile, and deceptive.

Unmanned systems are increasingly used for sustainment tasks, not just combat. The delegation described experimentation with ground robotic platforms to move supplies forward, support demining, conduct casualty evacuation, and reduce exposure along dangerous routes. These systems do not remove risk, but they change the risk calculus by substituting machines for personnel in the most exposed segments of the logistics chain. The broader lesson is that sustainment is now inseparable from counter-reconnaissance. If the enemy can see, it can strike; therefore, logistics must be designed to operate under constant observation and intermittent disruption.

For Canada and NATO, this suggests that logistics modernization must include low-signature distribution, digital resilience, and the integration of unmanned tools as routine enablers of endurance rather than exotic add-ons.

National resilience, mobilization, and territorial defence

The Armed Forces of Ukraine link national resilience to battlefield effectiveness. Resilience was described as the ability of individuals, institutions, and society to resist shocks and adapt to change. Stressors included persistent strikes on infrastructure, shortages in air defence coverage, electronic warfare that degrades navigation and communications, and the psychological fatigue of prolonged mobilization and disinformation.

Against this, the operational value of civic identity, social cohesion, and volunteerism is critical. Volunteer networks provide equipment, solving problems faster than formal processes, and sustaining morale and legitimacy. Mobilization reforms were described as moving toward greater transparency and digitization to improve force generation and preserve

public trust. Territorial defence forces also illustrate how resilience must be organized: early volunteers conducting local security tasks had to evolve into formations capable of operating in a precision-strike, drone-saturated environment. The lesson for partners is concrete: reserve and territorial forces need modern tools, integration into command structures, and sustained training.

A thought-provoking aspect for Canadians, as we discuss civil aspects of military preparedness, is that whole-of-society defence also depends on civil readiness – tactical medicine, basic drone literacy, emergency response, and information resilience – all built before a crisis.

Personnel recovery and reintegration

Personnel recovery and reintegration are perceived as both a moral obligation and a practical contributor to endurance. Ukrainians describe adopting NATO-informed recovery concepts but adapting them to a battlefield where air recovery is often unfeasible. In an environment saturated with air defences, drones, and strikes, recovery operations frequently become land-based, tactical-level efforts that depend on rapid action and local initiative. Drones are increasingly used to support recovery, to locate isolated personnel, and, in some cases, to influence adversary behaviour and facilitate surrender or capture.

Reintegration was emphasized as distinct from general rehabilitation. Returnees bring knowledge and perspectives that can strengthen the force as instructors, advisors, and sources of critical information on adversary practices. Reintegration processes, when properly designed, can help preserve hard-won experience in a force under strain, support mental and physical recovery and reduce stigma. It has also been noted that the risks of captivity and isolation extend beyond traditional categories; in a drone-observed environment, units can experience "isolation events" even while still within friendly territory. This reality pushes survival and conduct-after-capture preparation into broader training rather than limiting it to niche communities.

For partners, the implication is to plan for personnel recovery as part of force design, not as a specialized afterthought, especially in prolonged attritional war.

Implications for Canada and NATO partners

This points to several actionable implications for Canada and NATO partners preparing for high-intensity warfare.

Accelerate institutional tempo: Standardization, interoperability, contracting, and sustainment processes determine whether capabilities arrive in time to matter. Peacetime systems should be designed to operate under wartime urgency by enabling rapid fielding, iterative upgrades, and repairable designs that can be modified as the enemy adapts.

Build an economically sustainable counter-drone and air defence posture: High-end systems must be prioritized for the most dangerous threats, while layered defences absorb mass attacks through guns, mobile teams, electronic warfare, passive protection, and low-cost intercept solutions. Counter-UAS training should be embedded at every echelon, with exercises that assume constant surveillance and intermittent communications.

Strengthening mission command through professional education: When communications degrade and units disperse, junior leaders become the decisive node. That requires empowered NCOs and junior officers trained to act in accordance with intent, regain coherence after disruption, and quickly integrate new tools.

Institutionalize information defence: Standing capabilities should combine public education, rapid analysis, coordinated messaging, and partnerships with local authorities and civil society, with special attention paid to community-level digital spaces.

Modernize reserves and civil preparedness: Reserves need modern sensors, drone and counter-drone skills, and integration into command structures. Civil competence in tactical medicine and emergency response increases the speed and effectiveness of mobilization. Partnerships remain enabling when they are interoperable, sustained, and supported by maintenance and training capacity.

Conclusion

The Russia-Ukraine War underscores that the decisive advantages in modern war are systemic and cumulative. Adaptation is not a one-time leap; it is a continuous capability rooted in learning institutions that can capture lessons, validate them, and push change into the field at speed. Resilience is not separate from combat power; it is the condition that allows regeneration and legitimacy during prolonged attrition.

For Canada and its allies, the warning is clear. Future wars will compress decision time, punish centralized signatures, and reward forces that can operate in dispersed formations under constant observation, with contested logistics and degraded communications. Preparing for that environment requires more than acquiring new equipment. It requires building a national and military "learning engine" that links operations, education, procurement, and industry, and that can be surged when crises begin. It also requires treating citizens, infrastructure, and information space as part of the battlespace rather than as a distant rear area. This concept is known as "total defence," and it encapsulates the requirements of twenty-first-century conflict.[1]

Ukraine's experience, paid for at immense cost, offers a practical model: adapt faster, stay coherent, and endure.

Notes

[1] For more information on the total defence concept, see Joakim Berndtsson, Irina Goldenberg, and Stéfanie von Hlatky, eds., Total Defence Forces in the 21st Century (Montreal and Kingston: McGill-Queen's University Press, 2023).

BELOW THE THRESHOLD

Threats to Canada Below the Threshold of Warfare

Dani Belo

Critical infrastructure: high voltage electric tower.
Photo Credit: Getty Images

Dr. Dani Belo is an Assistant Professor and Director of International Relations and Security Studies at Webster University in St Louis, USA. He is also a Fellow at the Canadian Global Affairs Institute in Ottawa, Canada. His research and publications focus on gray zone conflict, hybrid threats, global governance, ethnic conflicts, and transatlantic security relations.

Introduction

In 2026, Canada faces a security environment that differs sharply from the post-Cold War period. Competition among states now unfolds largely below the threshold of armed conflict. Coercion is exercised through cyber operations, foreign interference, economic pressure, proxy actors, and legal or diplomatic obstruction. These activities rely on ambiguity and deniability. Together, they define what is commonly described as gray zone conflict.

For Canada, this shift creates distinct vulnerabilities. Canada is an open society with high levels of political trust and economic integration. These strengths also create exposure. Gray zone tactics target social cohesion, institutional confidence, and economic interdependence rather than military forces. As a result, the costs of competition are often political and societal rather than immediately physical.

Canada must also operate in a more fragmented allied environment. Transatlantic and Indo-Pacific partners continue to share broad strategic concerns. These include deterring Russia, managing China's global reach, and protecting critical infrastructure. However, allies increasingly differ in their approaches to risk, escalation, and burden sharing. Cooperation and competition now coexist, even among like-minded states.

The analysis below focuses on Canada's position in this environment through three lenses. First, it identifies the most serious gray zone dangers facing Canada, with emphasis on societal fragmentation, cyber intrusion, and economic coercion. Second, it situates these threats within the structural condition of competitive multilateralism, where institutions remain important but are often used for strategic competition rather than cooperation. Third, it assesses the role of middle powers, arguing that states like Canada retain agency but must integrate political, economic, and security tools more effectively. The discussion concludes by outlining strategic priorities for Canada in the gray zone. These priorities emphasize resilience as a form of deterrence. They also stress the need for institutional adaptation across government and selective investment in middle-power coalitions.

Key Gray Zone Dangers Facing Canada

The first threat is societal fragmentation, driven by foreign interference and information manipulation. It represents the most serious gray zone vulnerability.

Foreign actors rarely create divisions within Canadian society. Instead, they amplify existing political, regional, cultural, and identity-based tensions through disinformation, selective amplification, and intimidation.

This threat has been noted in Canadian Government documents such as the final report of the Public Inquiry into Foreign Interference 2025. It concluded that foreign interference constitutes a persistent and evolving threat to Canada's democratic institutions, extending beyond elections to include information manipulation and pressure on communities.[1]

Public Safety Canada has similarly warned that foreign interference increasingly targets diaspora communities through harassment, coercion, and disinformation. These activities can suppress political participation and weaken trust in public institutions.[2] Canadian intelligence reporting further links polarization and misinformation to a broader threat environment, noting that social fragmentation creates permissive conditions for hostile state activity and extremist mobilization.[3] In gray zone terms, societal fragmentation constrains policy choices by reducing consensus and undermining the legitimacy of sustained security commitments.

A second major danger is persistent cyber intrusion and pressure on critical infrastructure. The primary risk is not short-term disruption but long-term access and leverage. State-aligned cyber actors routinely target Canadian government systems, critical infrastructure operators, academic institutions, and private-sector innovation ecosystems. The National Cyber Threat Assessment 2025–2026 warns that hostile cyber activity against Canadian interests is ongoing and is expected to intensify as cyber tools become cheaper and more scalable.[4]

Ransomware illustrates this threat clearly. Although often financially motivated, ransomware attacks can generate strategic effects when they disrupt essential services or impose repeated recovery costs. The Cyber Centre's Ransomware Threat Outlook 2025–2027 assesses ransomware as a persistent national security concern, noting that automation and artificial intelligence are accelerating attack frequency and lowering barriers to entry.[5] In gray zone conflict, these cyber activities create uncertainty, strain governance capacity, and provide adversaries with leverage without clear attribution.

The third danger is economic coercion through strategic dependency. Canada's integration into global trade and investment networks increases efficiency but also creates exposure to coercive pressure. States can apply influence through tariffs, import restrictions, regulatory actions, or informal market barriers. These measures aim to shape Canadian policy behaviour without resorting to force.

China's use of trade pressure against Canada provides a clear example. In 2024 and 2025, Chinese authorities pursued trade investigations and retaliatory measures affecting Canadian agricultural exports, including canola-related products, in the context of broader bilateral disputes. Reporting by Reuters documents how such actions function as instruments of geopolitical signaling rather than purely commercial regulation.[6] Canadian government briefing materials explicitly describe these practices as economic coercion designed to exploit sectoral dependence and generate domestic political pressure.[7]

In turn, such dependencies can limit policy autonomy and complicate coordination with allies facing uneven exposure to retaliation.[8] To complicate matters, even in threat domains where allies have historically had clear overlapping strategic interests, reliance on traditional allies must be examined with greater scrutiny.

Competitive Multilateralism as a Structural Condition

The concept of competitive multilateralism, articulated by Dani Belo and David Carment, has become an accurate descriptor of the international system by 2026. States continue to operate within multilateral institutions. However, they increasingly treat these forums as arenas of competition rather than cooperation.[9]

This trend was evident throughout 2025 within NATO. Allies broadly agreed on the need to deter Russia following its continued war against Ukraine, but they diverged on escalation thresholds, defence spending timelines, and the scope and duration of military support to Kyiv.[10] Some allies prioritized forward military deployments and rapid reinforcement. Others focused on rebuilding domestic defence-industrial capacity or emphasized diplomatic engagement to manage escalation risks. These differences complicated collective signalling and weakened the clarity of deterrence messaging, even as formal alliance cohesion was maintained.[11]

Canada experienced competitive multilateralism directly in economic and technological domains. Allied states increasingly pursued national supply-chain strategies for critical minerals, semiconductors, and advanced manufacturing. While these initiatives often overlapped rhetorically, they did not fully align in practice.[12] Canada's own critical minerals strategy emphasized national security and economic resilience, but coordination with allies remained uneven, reflecting differing industrial priorities and risk tolerances.[13] Cooperation and competition thus coexisted, even among close partners.

Competitive multilateralism also blurred behavioural distinctions between allies and adversaries. Economic security measures such as export controls, investment screening, and trade restrictions increasingly affected friendly states as well as strategic rivals.[14] The expansion of geo-economic tools reinforced what Henry Farrell and Abraham Newman describe as "weaponized interdependence," in which states exploit network centrality and market access to pursue strategic advantage.[15] For Canada, this environment demands strategic realism. Multilateral engagement remains essential, but it no longer guarantees shared outcomes or predictable cooperation.

The Strategic Role of Middle Powers

Middle powers like Canada occupy a critical position in gray zone competition. They lack the unilateral power of great states but possess sufficient economic, diplomatic, and institutional capacity to shape outcomes collectively. In pursuit of strategic goals, their influence depends on coordination and strategic clarity.[16]

Ad-hoc coalitions of middle powers can also be an escape for nations facing economic pressure from great powers. In 2025, Canada experienced economic pressure from the United States, illustrating how gray zone dynamics can operate even within close alliances. Several U.S. trade measures were instituted. These were framed around domestic industrial policy, supply-chain security, and national economic resilience and had indirect constraining effects on Canadian policy space. They included the continued use of Buy America provisions, targeted trade remedies, and ongoing uncertainty around steel and aluminum measures first introduced under Section 232 authorities.[17] While these actions were directed at Canada, Ottawa was not designated as an adversary. However, the measures created adjustment pressures for Canadian exporters in sectors such as metals, energy, and advanced manufacturing.[18] This episode highlights how economic statecraft can blur the line between cooperation and coercion among allies, reinforcing the need for Canada to manage economic vulnerability without undermining broader bilateral and alliance relationships.

In pursuit of trade, political, and security partnership diversification, Canada may leverage its historical strength which lies in coalition-building and norm promotion. These remain valuable assets. However, norms alone do not deter gray zone coercion. Middle powers must also demonstrate the ability to impose costs and deny benefits. However, even with such potential, significant collective action challenges remain.

In 2025, middle power coordination remained uneven across regions. In Europe, states pursued joint initiatives focused on cyber resilience, energy security, and protection of critical infrastructure, often within NATO and EU frameworks.[19] In contrast, Indo-Pacific middle powers concentrated on maritime domain awareness, supply-chain resilience, and minilateral security arrangements such as the Quad, reflecting more immediate concerns over maritime coercion and economic vulnerability.[20] Despite shared interests, cross-regional coordination between European and Indo-Pacific middle powers remained limited, reinforcing fragmented approaches to gray zone challenges.

Canada is well positioned to help bridge these gaps. Its deep transatlantic ties and expanding Indo-Pacific engagement provide structural access to both regional security conversations. However, this connector requires prioritization and internal coherence. Economic policy must align with security objectives, particularly as critical minerals, advanced manufacturing, and technology standards become instruments of strategic competition.[21] Canada's own critical minerals strategy explicitly links economic resilience to alliance coordination, underscoring that industrial policy cannot be separated from security planning.

The Road Ahead: Canada's Strategy for the Gray Zone

Several priorities emerge from this analysis. First, resilience should become a core deterrence strategy. Cybersecurity, supply chain robustness, and information integrity reduce vulnerability. They also signal resolve by limiting the effectiveness of coercive tactics. As gray zone conflict increasingly defines the contemporary security environment, traditional deterrence frameworks alone are insufficient to address persistent, low-level coercion. Deterrence through resilience refers to a strategy that seeks to discourage adversarial action by reducing a target state's vulnerability to coercion rather than by threatening punishment or denial through force.

Instead of relying on retaliation (deterrence by punishment) or on the ability to physically block or defeat an attack (deterrence by denial), deterrence through resilience focuses on ensuring that disruptive actions fail to produce meaningful strategic, political, or societal effects. It emphasizes the capacity of institutions, societies, and critical systems to absorb shocks, adapt under pressure, and recover quickly from interference. This approach is particularly distinct in that it does not require

clear attribution, escalation dominance, or rapid response, all of which are often absent or risky in contemporary competition.

Deterrence through resilience is especially effective in gray zone conflict, where adversaries deliberately operate below the threshold of armed attacks. In such contexts, punishment-based deterrence is difficult to apply and denial is often incomplete. However, resilience directly undermines the logic of gray zone coercion by denying adversaries the political leverage, social fragmentation, or institutional paralysis they seek to create. By making societies harder to manipulate and systems harder to disrupt, resilience shifts the cost-benefit calculus of gray zone operations, reducing their strategic utility. The adoption of such a strategic deterrence posture can enable the necessary collaboration among government institutions.

Second, Canada must mainstream gray zone analysis across government, treating unconventional threats as a standing condition of international competition rather than as episodic or sector-specific problems. Gray zone dynamics should inform defence planning, where persistent cyber operations, information warfare, and proxy activity must be integrated into force development, readiness, and deterrence concepts alongside conventional threats. They should also shape trade and economic policy, as supply chains, investment flows, and market access are increasingly used as instruments of coercion rather than neutral economic exchanges. Similarly, diplomatic engagement must be recalibrated to reflect the reality that cooperation and competition now occur simultaneously, often within the same institutional settings. Achieving this shift requires institutional adaptation, including cross-departmental coordination mechanisms, shared threat assessments, and integrated policy planning that bridges security, economic, and diplomatic domains. Without such structural changes, gray zone threats risk being addressed in isolation, leaving Canada reactive rather than anticipatory and undermining its ability to deter and manage sustained low-level coercion.

Third, Canada should invest in middle power coalitions focused specifically on gray zone challenges. Even though strategic fragmentation has become a prominent feature of international affairs, such coalitions can supplement NATO and other alliances when they fail. Smaller multilateral formats can move faster and address gaps that large institutions struggle to fill. However, in cases where cooperation does not serve Ottawa's interests, Canada must adapt to competitive multilateralism. Engagement should be strategic and selective. Institutions remain valuable, but they are no longer neutral arenas. Canada must enter them with clear objectives and realistic expectations.

Notes

[1] Marie-Josée Hogue, *Public Inquiry into Foreign Interference in Federal Electoral Processes and Democratic Institutions: Final Report* (Ottawa: Government of Canada, January 28, 2025), https://publications.gc.ca/site/eng/9.946443/publication.html

[2] Public Safety Canada, "Foreign Interference: Overview of Hostile Activities," Government of Canada, 2025, https://www.publicsafety.gc.ca/cnt/trnsprnc/brfng-mtrls/prlmntry-bndrs/20250226-1/17-en.aspx

[3] Canadian Security Intelligence Service, *CSIS Public Report 2024* (Ottawa: Government of Canada, 2024), https://www.canada.ca/en/security-intelligence-service/corporate/publications/csis-public-report-2024.html

[4] Canadian Centre for Cyber Security, *National Cyber Threat Assessment 2025–2026* (Ottawa: Communications Security Establishment, October 30, 2024), https://www.cyber.gc.ca/en/guidance/national-cyber-threat-assessment-2025-2026

[5] See three sources: Canadian Centre for Cyber Security, *Ransomware Threat Outlook 2025–2027* (Ottawa: Communications Security Establishment, December 2024), https://www.canada.ca/en/communications-security/news/2025/12/cyber-centre-releases-ransomware-threat-outlook-2025-to-2027.html.

and Canadian Security Intelligence Service, *CSIS Public Report 2024* (Ottawa: Government of Canada, 2024), https://www.canada.ca/en/security-intelligence-service/corporate/publications/csis-public-report-2024.html and Canadian Centre for Cyber Security, *National Cyber Threat Assessment 2025–2026* (Ottawa: Communications Security Establishment, October 30, 2024), https://www.cyber.gc.ca/en/guidance/national-cyber-threat-assessment-2025-2026.

[6] Reuters, "China Slaps Temporary Duties on Canadian Canola," *Reuters*, 2025, https://www.reuters.com/markets/commodities/china-sets-temporary-anti-dumping-duty-canadian-canola-2025-08-12/

[7] Global Affairs Canada, *Minister of International Trade: Briefing Book* (Ottawa: Government of Canada, 2025), https://international.canada.ca/en/global-affairs/corporate/transparency/briefing-documents/briefing-books/2025-03-international-trade

[8] Global Affairs Canada, *Minister of International Trade: Briefing Book* (Ottawa: Government of Canada, 2025), https://international.canada.ca/en/global-affairs/corporate/transparency/briefing-documents/briefing-books/2025-03-international-trade

[9] Dani Belo and David Carment, "Unilateralism and Competitive Multilateralism in Gray-Zone Conflict: A Comparison of Russia and the United States," *Wild Blue Yonder Journal* (Air University), August 3, 2020, https://www.airuniversity.af.edu/Wild-Blue-Yonder/Articles/Article-Display/Article/2292990/unilateralism-and-competitive-multilateralism-in-gray-zone-conflict-a-compariso/

[10] Henrik Larsen, "Toward a Europeanised NATO," International Centre for Defence and Security (ICDS), 2025, http://www.jstor.org/stable/resrep71144 and NATO, *NATO Strategic Concept and Defence Planning Update* (Brussels: North Atlantic Treaty Organization, 2024), https://www.nato.int/en/what-we-do/introduction-to-nato/nato-defence-planning-process

[11] Heidi Hardt, "NATO after the Invasion of Ukraine: How the Shock Changed Alliance Cohesion," *International Affairs* (online first, 2024), https://link.springer.com/article/10.1057/s41311-024-00629-x

[12] Organisation for Economic Co-operation and Development (OECD), *Global Value Chains: Risks, Resilience and Rebalancing* (Paris: OECD Publishing, 2023), https://www.oecd.org/trade/global-value-chains/

[13] Global Affairs Canada, *Canada's Critical Minerals Strategy: From Security to Supply Chains* (Ottawa: Government of Canada, 2024), https://www.canada.ca/en/campaign/critical-minerals-in-canada/canadian-critical-minerals-strategy.html

[14] Daniel W. Drezner, Henry Farrell, and Abraham L. Newman, eds., *The Uses and Abuses of Weaponized Interdependence* (Washington, DC: Brookings Institution Press, 2021), https://www.brookings.edu/books/the-uses-and-abuses-of-weaponized-interdependence/

[15] Henry Farrell and Abraham L. Newman, "Weaponized Interdependence: How Global Economic Networks Shape State Coercion," *International Security* 44, no. 1 (2019): 42–79, https://www.mitpressjournals.org/doi/10.1162/isec_a_00351

[16] Dani Belo, "Middle Power Foreign Policy in an Era of Gray Zone Conflict: Addressing the Challenges for Canada," in *Canada and Great Power Competition: Canada Among Nations 2021*, ed. David Carment, Laura Macdonald, and Jeremy Paltiel (Cham: Springer International Publishing, 2022), 277–96, https://link.springer.com/chapter/10.1007/978-3-031-04368-0_13 and Alexander M. Hynd, "Repositioning Middle Powers in International Hierarchies of Status and Order," *International Relations* (2025), https://journals.sagepub.com/doi/10.1177/00471178251319723 and Buğra Süsler and Chris Alden, "Brokering Peace: Emerging Middle Powers, Agency and Mediation," *Global Policy* 15, no. S1 (2024): 65–77, https://onlinelibrary.wiley.com/doi/10.1111/1758-5899.70100

[17] United States Trade Representative, *2024 Trade Policy Agenda and 2023 Annual Report* (Washington, DC, 2024), https://ustr.gov/sites/default/files/The%20Presidents%202024%20Trade%20Policy%20Agenda%20and%202023%20Annual%20Report.pdf and Congressional Research Service, *Build America Buy America* (Washington, DC, 2024), https://www.commerce.gov/oam/build-america-buy-america

[18] BBC, "From Surge in Patriotism to Fewer US Trips – Trump's Impact on Canada," *BBC*, 2025, https://www.bbc.com/news/articles/crmlvym2e3eo

[19] NATO, *NATO Strategic Concept and Defence Planning Update 2024* and European Commission, *European Economic Security Strategy* (Brussels, 2023), https://research-and-innovation.ec.europa.eu/strategy/strategy-research-and-innovation/europe-world/international-cooperation/strategic-autonomy-and-european-economic-and-research-security_en

[20] Department of Defence Australia, *National Defence Strategy 2024* (Canberra: Australian Government, 2024), https://www.defence.gov.au/about/strategic-planning/2024-national-defence-strategy-2024-integrated-investment-program

[21] OECD, 2023 and Global Affairs Canada, 2024.

CYBER

A Strategic Outlook on Cyber for Canada: Where Capabilities Are Heading and Why It Matters

Kristen Csenkey

Members of CAF Cyber Command, review notes ahead of Exercize LOCKED SHIELDS 25 in Seoul, South Korea.
Photo Credit: Combat Camera

Dr. Kristen Csenkey is a Social Sciences and Humanities Research Council (SSHRC) postdoctoral fellow at the Brian Mulroney Institute of Government, St. Francis Xavier University and an Associate Fellow with the Centre for Military, Security and Strategic Studies at the University of Calgary. She studies global cyber governance, technology interdependence, and the geopolitics of emerging and disruptive digital technologies, with a focus on quantum computing and sensing and their domain-specific applications and implications. Follow her work at: kristencsenkey.com.

Introduction

The world of yesterday has changed – as Marcus Aurelius long anticipated it would when he wrote: "All things are changing; and thou thyself art in continuous mutation and in a manner in continuous construction, and the whole universe too".[1] International stability, trust among old allies, and relationships with new partners are being tested. New challenges lie ahead in an increasingly unpredictable and volatile threat environment, including those within the cyber domain. Canada must confront the evolving threat environment head-on, including the impact of emerging and disruptive technologies, to address present and future challenges.

These challenges are recognized within Canadian defence leadership. The Chief of the Defence Staff, General Jennie Carignan, has stated: "The world is in a state of transition, and the same is true for the Canadian Forces. Outcomes are not guaranteed. We must be comfortable with being uncomfortable."[2]

To maintain an advantage in the cyber domain, Canada must address artificial intelligence (AI)-enabled transformations and quantum computing's cryptographic challenges – technologies that will reshape the defence landscape in the coming years.

This paper provides a focused examination of the emerging and established defence and security challenges Canada faces in the cyber domain. In what follows, two technologies and their consequences as two related areas of strategic concern are explored, drawing on Canada's current posture and real-world examples to situate what the defence community may face in 2026. The analysis examines current threats and their impact on the construction of the defence landscape, focusing on defining issue areas of geopolitical tension and sovereignty considerations.

Overview of the Threat Landscape

In 2026, Canada must navigate changes in two related issue areas that will impact trust and relationships within the cyber domain: geopolitical tension and sovereignty considerations. Together, these represent key strategic pressures Canada faces as the global order continues to shift.

First, geopolitical tensions have affected how the motivations behind cyberattacks and the gravity of their impact are perceived. In a 2025 survey by Accenture and the World Economic Forum,[3] respondents identified geopolitically-motivated cyberattacks as the leading factor influencing their risk mitigation strategies. The release of the United States National Security Strategy[4] and National Defense Strategy[5] have raised concerns about how Canada can maintain its interests and what future cooperation with the United States may look like.[6] These developments have the potential to test trust between partners on addressing threats and areas of strategic concern where trust is essential.

Recent Pew Research Center surveys highlight the stakes of strained trust with traditional allies, specifically the United States.[7] In their recent study, the United States was identified both as the greatest threat and as the greatest ally to Canada[8] and other countries,[9] representing a significant change since 2019,[10] as the proportion of Canadians naming the United States as their country's greatest threat has almost tripled. New polling results have revealed a shift in Canadians' positive perceptions of China in 2025, reaching a 39% favourable opinion, with positive opinions of the United States falling below those of China.[11] This shift in perception will affect trusted partnerships going forward, including within NATO.

As conflict continues in hybrid forms across multiple domains, including cyber, fundamental questions about reliable partners and trust will persist. For example, the 2025 NATO Science and Technology Strategy[12] emphasises cooperation among member states to strengthen their science and technology ecosystems and to ensure that they can meet present and future security challenges.

Second, sovereignty – closely linked to the first issue area – remains an issue of concern. Over the past year, Canada has had to reassess its defence and economic posture amid geopolitical tensions, demands from allies,[13] and trade disputes.[14] These pressures affect activities and operations in the cyber domain by shaping choices in technology dependencies related to cyber capabilities.[15] For example, the procurement of domestic technological tools through the newly released Defence Industrial Strategy's "Build–Partner–Buy" framework[16] seeks to support and streamline the acquisition of strategic assets and pivots the focus to Canadian-made solutions. Protecting autonomy and carefully managing overreliance on foreign technology providers continues to be viewed as essential for Canada to demonstrate resilience in the face of threats and maintain domestic capabilities.[17]

The establishment of the Bureau of Research, Engineering and Advanced Leadership in Innovation and Science (BOREALIS)[18] in 2025 was touted as a way for Canada to develop domestic solutions related to cyber and emerging technologies, including AI and quantum computing, for the Canadian Armed Forces and the Communications Security Establishment specifically. The appointment of Canada's first Minister of Artificial Intelligence and Digital Innovation[19] further demonstrates the government's recognition of the importance of domestic capabilities for self-reliance. More broadly, this highlights the global trend of strained trust amid uncertainty. The focus on further developing and supporting trusted-networks of domestic suppliers applies not only to activities in cyberspace and integrating the capabilities of digital technologies, but also to sustaining confidence between partners in times of geopolitical tensions, preserving interoperability, and balancing it with national autonomy.

The emergence of new technological tools as cyber capabilities has the potential to transform the speed and scale of operations, security, and vulnerabilities. Technologies, such as AI and quantum computing, when wielded by strategic actors, have the potential to enhance, challenge, and contest activities in the cyber domain. As cyberspace grows increasingly intertwined with geopolitics and sovereignty concerns, including via motivations and perceptions of cyber operations, these capabilities will only become more consequential in the years ahead. For instance, quantum technologies and their potential capabilities are increasingly viewed as strategic assets in many sectors, including defence and national security.[20] The intersection of these technologies within the cyber domain is not merely a technical issue, but a strategic concern for Canada that will shape the defence landscape in the coming years.

To sum up, the politics and security of cyberspace is a prominent concern for Canada in 2026. The number of cyberattacks is rising globally due to the interconnection of people, services, and digital technologies. Threat actors[21] persist in attempting to destabilize Canada and its allies through cyber operations that fall below the threshold of armed conflict. The motivations for engaging in malicious cyber activities remain largely unchanged although the perceptions of operations may be varied, and ransomware continues to be a primary threat for Canada[22] and allies, such as the European Union.[23] Threat assessments and outlooks[24] released by the Communications Security Establishment make these points clear.

Against this background, this strategic outlook provides insights into two emerging areas of concern for Canada, as discussed in the next section.

Strategic Areas of Concern

Geopolitical tensions and sovereignty considerations will continue to influence capability and resiliency gaps in the cyber domain. AI-enabled transformations are of particular concern for Canada in 2026 because they have the potential to make cyber operations more efficient and potentially more effective. This may lead to more frequent cyberattacks, new adversarial tools that may broaden the attack surface, and greater impact across both defensive and offensive operations. AI and quantum capabilities vary in their readiness and accessibility, but both require sustained attention from the defence community. Although practical quantum computers powerful enough to break existing cryptography do not yet exist, their arrival will pose a serious threat to the confidentiality and integrity of sensitive information. Coordination to address the threat posed by actors with access to this technology will require collaboration at multiple levels.

1. AI-Enabled Transformations in the Cyber Domain

AI tools enable malicious actors to employ more targeted, low-cost, and scalable tactics. As AI progresses in development and deployment, these tools could operate more autonomously, amplifying the scale and sophistication of attacks. Attack tools and technologies are becoming cheaper, lowering barriers to entry, making them more accessible and harder to attribute, which allows less sophisticated actors to engage in malicious activities. This could result in a larger number of actors and greater unpredictability in the cyber environment.

Although AI-enabled cyber operations are not yet widespread, they are becoming more efficient and common among state and non-state threat actors.[25] The examples presented in this section demonstrate that Canada's adversaries and criminal networks are becoming increasingly sophisticated in their use of AI technologies for offensive and disruptive purposes.

AI tools will continue to shape vulnerabilities and enable new capabilities in the cyber domain. These tools include generative AI, agentic AI, and large language models (LLMs), which have the potential to enable transformation across two main dimensions of the cyber domain in the year ahead.

First, AI tools can exploit capabilities in existing vectors and introduce new vulnerabilities. A recent survey found that 87% of respondents identified AI-related vulnerabilities as the fastest-growing cyber risk over the past year.[26] The use of LLMs by threat actors to exploit weaknesses can enable new information operations capabilities, particularly for content generation and targeted research. For example, individuals associated with the global cybercrime network Storm-2139 exploited vulnerabilities in Azure to generate thousands of abusive AI-created synthetic content items, including deepfakes and misogynistic, violent, and hateful material.[27]

In several cases, People's Republic of China (PRC)-linked threat actors, posing as cybersecurity researchers and students in capture-the-flag competitions, were reported to have engaged with Gemini to illicitly access blocked information for phishing activities.[28] Similar cyber operations were also identified by Anthropic which found malicious actors used Claude to gather data by posing as an employee of a cybersecurity company and execute a cyberattack as part of an espionage campaign.[29]

Threat actors can use LLMs to gather information on potential targets, script tasks, and extract data. Over twenty government-backed threat actors linked to the PRC were reported to have used Gemini for reconnaissance and vulnerability research.[30] While providers such as Google,[31] Microsoft,[32] and OpenAI[33] work to secure their AI agents against malicious use, the misuse of AI tools by threat actors will continue to change and challenge activities in the cyber domain.

Second, these technologies have the potential to amplify cyber operations and activities through automated exploitation. LLMs have been shown to be capable of carrying out ransomware attacks across the full attack lifecycle, from initial system compromise to messaging victims, as demonstrated by a New York University research team's creation and study of PromptLock.[34] AI agents,[35] both individually[36] and in teams,[37] have demonstrated the ability to autonomously identify previously unknown (zero-day) vulnerabilities.

While AI can be leveraged to increase productivity, it can be weaponized to optimise malicious activities– including to create and enhance media for misinformation, disinformation, and influence campaigns. AI-generated and enhanced audio, video, and memes can be used by malicious actors to undermine the integrity of individuals and organisations, mislead populations, and spread harmful narratives, among other objectives.[38] Such AI-generated content has the potential to erode trust within society and between trusted partners, and to influence human behaviour.[39]

» What Lies Ahead?

Leveraging AI capabilities while addressing associated vulnerabilities will be essential to achieving strategic objectives in the cyber domain and keeping Canadians safe. Canada can do this by viewing AI-enabled cyber capabilities as both a 'sword and shield'.[40]

AI tools can be weaponized by threat actors to cause harm, but the technology can also be used as a strategic asset to strengthen defence.[41] These tools can support defensive cyber capabilities– for example by assisting in the detection of threats and attacks, helping threat intelligence teams analyze large volumes of data, and identifying and addressing vulnerabilities. This framing of AI will allow Canada to ensure that domestic cyber capabilities keep pace with present and future threats.

2. Quantum-Driven Cryptographic Uncertainty

Quantum computers are an emerging technology that harnesses the principles of quantum mechanics to enhance computational capabilities, including to break algorithms that are widely used to keep data and communications secure. Although a quantum computer capable of performing these operations remains many years away,[42] computational power in the field continues to grow. Quantum computers not only pose a technological issue, but also a cybersecurity one, because of their anticipated capability as a way for attackers to compromise current cryptographic systems.

Future[43] quantum computers will be capable of breaking existing encryption and authentication methods that are currently considered safe. While waiting for this development, adversaries, competitors, criminal organizations, and other threat actors are gathering information through "harvest now, decrypt later" attack models. The consequences of this strategy extend beyond defence as it can impact society across multiple sectors. Trust in defence, financial, and health systems depends on the ability to protect confidential data from unauthorized and malicious access.

Cryptography ensures confidentiality and is used to control and authenticate access to sensitive and confidential data. Cryptographic systems protect a wide range of information, including sensitive and confidential data held in government, financial, and health records, among other areas. Data are converted into an unreadable encrypted format so that only authorized users with the right keys can access them. At present, actors attempting to break encryption in order to obtain information may rely on classical computing and supercomputers. This approach is time consuming, resource intensive, and difficult to scale.

Quantum-driven uncertainty stems from the fear that quantum computers could undermine the cryptographic methods[44] that keep data safe, becoming a cybersecurity risk to the digital infrastructure that protects national security data and private personal information.[45] Uncertainty remains around when this will occur, which actors will develop the capability, which systems will be exposed, and whether the current cryptographic infrastructure can be updated in time to remain secure. This is referred to as the quantum threat, and states have already begun preparing for it.[46]

Post-quantum cryptography (PQC) refers to algorithms designed to replace vulnerable cryptographic standards and is considered a reliable way to prepare for the threat posed by the future quantum computing capabilities. The US National Institute of Standards and Technology (NIST) has led efforts to standardize PQC algorithms,[47] and countries including Canada[48] and the United Kingdom[49] have released guidance and roadmaps to raise awareness of the threat and guide the transition to secure cryptographic systems.

Migration plans to PQC algorithms exist, but their associated security guarantees will not be realised overnight. Additionally, migration plans, roadmaps, and progress reporting are focused on government-wide security.[50] Although guidance exists,[51] the next step is ensuring that these plans are followed across critical sectors, like health and finance.

» What Lies Ahead?

Access to practical quantum computers – existing and future – remains prohibitive to some actors. The cost depends on factors such as the type of quantum computer, required expertise, and vendor support, though access could also be granted through states or large companies willing to share their resources[52] – information about current capabilities, however, remains limited.[53] What is concerning is that once confidential data is decrypted, it can be exploited for malicious purposes. Passwords, military plans, intelligence, personnel health files, and other secrets could be exposed – ultimately putting lives at risk.

This threat is therefore not only a technological and cybersecurity issue, but an organizational, financial, and broader societal one.

Cyber capacity and updates to information technology systems must be enhanced through PQC deployments and standardisation plans developed with partner states and product and service providers. Not all systems may be vulnerable to quantum-enabled attacks, but defending against the threat will require collaboration at multiple levels– it is a long-term process, not a one-time fix. A coordinated approach among allies has been proposed to promote secure post-quantum solutions.[54] Such efforts would enable PQC at scale, allowing allied states to defend against "harvest now, and decrypt later" schemes. While implementation plans exist, their success depends on consistent adoption, testing, and on-going evaluation across sectors. A challenge facing such coordination efforts in 2026 is the geopolitical friction surrounding technology-based collaboration and the increasingly insular nature of these efforts.

The transition to PQC adoption is expected to protect confidential information from the threat posed by future quantum computers. Yet it is the current activities of malicious actors using "harvest now, decrypt later" attack schemes that are driving present responses to protect data. The threat posed by quantum computers – through actors who may gain access to them – will also shift perceptions of trust and stability in the international system. As sovereign technological systems increasingly become the goal and necessity for states including Canada, a new risk emerges: a quantum divide between those who will have access to these capabilities and can enhance their cyber capacity, and those who will be unable to protect against them. Geopolitical fragmentation makes it difficult to imagine a collective response for a quantum-safe world, as power imbalances and diverging interests become defining features of the defence environment.

Conclusion

The technologies discussed here will impact cyber capabilities and capacity; however, they do not operate in isolation. While autonomous AI systems are often described as capable of executing cyber operations independently, they still require human intervention. Human operators must make key decisions, including selecting relevant targets, directing reconnaissance, and developing the attack framework within which the tool operates. Detection and defence likewise require human judgment. Although these technologies increase the speed and scale of operations, they remain dependent on human operators to determine objectives and actions.

Notes

[1] Marcus Aurelius, The Meditations of Marcus Aurelius translated by George Long.

[2] House of Commons Standing Committee on National Defence, Number 115, 1st session, 44th parliament, September 26, 2024. https://www.ourcommons.ca/DocumentViewer/en/44-1/NDDN/meeting-115/evidence

[3] Giulia Moschetta, Ellie Winslow, Willem Buys, and Kilian Hayat, "Global Cybersecurity Outlook 2026: Insight Report," World Economic Forum, January 2026. https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2026.pdf

[4] The White House, National Security Strategy of the United States of America, November 2025. https://www.whitehouse.gov/wp-content/uploads/2025/12/2025-National-Security-Strategy.pdf

[5] Department of War, 2026 National Defense Strategy. January 23, 2026. https://media.defense.gov/2026/Jan/23/2003864773/-1/-1/0/2026-NATIONAL-DEFENSE-STRATEGY.PDF

[6] Marc Lanteigne, "Negative Sum Game: The 2025 US National Security Strategy and Implications for Canada," North American and Arctic Defence and Security Network, December 14, 2025. https://www.naadsn.ca/wp-content/uploads/2025/12/25dec-Negative-Sum-Game-US-NSS-Quick-Impact-Lanteigne.pdf ; Canadian Naval Review, "Broadsides Discussion Forum: The 2026 US Defense Strategy Document." January 28, 2026.

https://www.navalreview.ca/2026/01/the-2026-us-defense-strategy-document/

[7] Pew Research Center, "People in Many Countries Consider the U.S. an Important Ally; Others See It as a Top Threat," Pew Research Center, July 8, 2025. https://www.pewresearch.org/global/2025/07/08/people-in-many-countries-consider-the-u-s-an-important-ally-others-see-it-as-a-top-threat/

[8] ibid.

[9] Mexico follows a similar pattern in the 2025 survey.

[10] Pew Research Center, "U.S. an Important Ally."

[11] Mario Canseco, "Canadians Maintain Favourable Ratings for Italy, Japan and UK," Research Co., February 12, 2026. https://researchco.ca/2026/02/12/countries-feb2026/

[12] NATO, NATO Science & Technology Strategy, June 2025. https://www.nato.int/content/dam/nato/webready/documents/sto/STO-strategy-2025.pdf

[13] For example, Troy Bouffard, P. Whitney Lackenbaue, and Andrea Charron, "The "Iron Dome" and Implications for the Nort," North American and Arctic Defence and Security Network, February 28, 2025. https://www.naadsn.ca/wp-content/uploads/2025/02/25feb28_Iron_Dome_Implications_Arctic-NAADSN-QI-TB-PWL-AC.pdf

[14] For example, Prime Minister of Canada, "Prime Minister Carney forges new strategic partnership with the People's Republic of China focused on energy, agri-food, and trade," Government of Canada, January 16, 2026. https://www.pm.gc.ca/en/news/news-releases/2026/01/16/prime-minister-carney-forges-new-strategic-partnership-peoples

[15] Milena Rodban, "Political Risk and the Geopolitics of Cybersecurity." In The Routledge Handbook of Political Risk, eds. Julian Campisi, Johannes Leitner, Hannes Meissner, and Cecilia Emma Sottilotta (Routledge, 2025). https://www.taylorfrancis.com/chapters/edit/10.4324/9781003456117-15/political-risk-geopolitics-cybersecurity-milena-rodban

[16] National Defence, Canada's Defence Industrial Strategy, Government of Canada. February 17, 2026.

https://www.canada.ca/en/department-national-defence/corporate/reports-publications/industrial-strategy/security-sovereignty-prosperity.html

[17] Natasha Tusikov. "Canada must ensure its digital sovereignty in the face of U.S. threats," Policy Options, May 8, 2025. https://policyoptions.irpp.org/2025/05/digital-sovereignty/ ;Andrew Clement, "Time for Canada to strengthen its digital sovereignty." The Hill Times. March 5, 2025. https://www.hilltimes.com/story/2025/03/05/time-for-canada-to-strengthen-its-digital-sovereignty/452864/

[18] National Defence. "Bureau of Research, Engineering and Advanced Leadership in Innovation and Science (BOREALIS)." Government of Canada, February 19, 2026. https://www.canada.ca/en/department-national-defence/programs/borealis.html

[19] Government of Canada. "The Honourable Evan Solomon." October 8, 2025. https://www.canada.ca/en/government/ministers/evan-solomon.html

[20] Dongyoun Cho, Mauritz Kop, and Min-Ha Lee. "Strategic Governance of Quantum Supply Chains: A Criticality-Based Framework for Risk, Resilience, and Data-Driven Foresight," preprint, In Review, November 11, 2025, https://doi.org/10.21203/rs.3.rs-8062873/v1.

[21] This includes states such as China, Iran, and Russia, North Korea, as well as non-state actors. Generally, threat actors are individuals or groups with malicious intent that aim to exploit weaknesses in information systems and/or its operators to gain broader access. See: Communications Security Establishment. "An Introduction to the Cyber Threat Environment." Canadian Centre for Cyber Security, October 28, 2022. https://www.cyber.gc.ca/en/guidance/introduction-cyber-threat-environment.

[22] Communications Security Establishment. "Ransomware Threat Outlook 2025-2027." Canadian Centre for Cyber Security, January 28, 2026.

https://www.cyber.gc.ca/en/guidance/ransomware-threat-outlook-2025-2027; Communications Security Establishment. "National Cyber Threat Assessment 2025-2026." Canadian Centre for Cyber Security, October 30, 2024 https://www.cyber.gc.ca/en/guidance/national-cyber-threat-assessment-2025-2026

[23] European Union Agency for Cybersecurity. "ENISA Threat Landscape 2025." October 1, 2025. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025

[24] Communications Security Establishment, "Threat Assessment 2025-2026"; Communications Security Establishment, "Ransomware Threat Outlook 2025-2027."

[25] Microsoft. "Microsoft Digital Defense Report 2025", 2025. https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/msc/documents/presentations/CSR/Microsoft-Digital-Defense-Report-2025.pdf#page=1

[26] Moschetta et al., "Global Cybersecurity Outlook 2026".

[27] Microsoft, "Digital Defense Report 2025"; Steven Masada, "Disrupting a global cybercrime network abusing generative AI," Microsoft On the Issues, February 27, 2025. https://blogs.microsoft.com/on-the-issues/2025/02/27/disrupting-cybercrime-abusing-gen-ai/

[28] Google Threat Intelligence Group, "GTIG AI Threat Tracker: Advances in Threat Actor Usage of AI Tools," Google Cloud, November 5, 2025. https://cloud.google.com/blog/topics/threat-intelligence/threat-actor-usage-of-ai-tools

[29] Anthropic. "Disrupting the first reported AI-orchestrated cyber espionage campaign: Full report." Anthropic, November 17, 2025. https://assets.anthropic.com/m/ec212e6566a0d47/original/Disrupting-the-first-reported-AI-orchestrated-cyber-espionage-campaign.pdf. Also attributed to PRC-back or associated actors.

[30] Based on a 2025 report released by the Google Threat Intelligence Group, "Adversarial Misuse of Generative AI," Google Cloud, January 29, 2025. https://cloud.google.com/blog/topics/threat-intelligence/adversarial-misuse-generative-ai

[31] Google DeepMind Security and Privacy Research Team, "Advancing Gemini's security safeguards," Google DeepMind, May 20, 2025. https://deepmind.google/blog/advancing-geminis-security-safeguards/

[32] Brad Smith, "Combating abusive AI-generated content: a comprehensive approach," Microsoft On the Issues, February 13, 2024.https://blogs.microsoft.com/on-the-issues/2024/02/13/generative-ai-content-abuse-online-safety/

[33] OpenAI, "Disrupting malicious uses of AI by state-affiliated threat actors," OpenAI, February 14, 2024. https://openai.com/index/disrupting-malicious-uses-of-ai-by-state-affiliated-threat-actors/

[34] Md Raz et al., "Ransomware 3.0: Self-Composing and LLM-Orchestrated," arXiv:2508.20444, preprint, arXiv, August 28, 2025, https://doi.org/10.48550/arXiv.2508.20444. Formerly, known as Ransomware 3.0.

[35] A task-specific expert agent using (GPT-4). Fang, Richard, Rohan Bindu, Akul Gupta, Qiusi Zhan, and Daniel Kang. "LLM Agents Can Autonomously Hack Websites." arXiv:2402.06664. Preprint, arXiv, February 16, 2024. https://doi.org/10.48550/arXiv.2402.06664.

[36] Fang et al., "LLM Agents."

[37] Specifically, it was an open-source vulnerabilities in a controlled test environment. Fang et al., "LLM Agents."

[38] Canadian Centre for Cyber Security, "Cyber Threats to Canada's Democratic Process: 2025 Update," 2025. https://www.cyber.gc.ca/en/guidance/cyber-threats-canadas-democratic-process-2025-update#fn1; Microsoft Threat Intelligence. "Same targets, new playbooks: East Asia threat actors employ unique methods." Microsoft, April 2024. https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/microsoft-brand/documents/MTAC-East-Asia-Report.pdf

[39]Sobolev, Anton. "The Last Call for Authenticity: AI Reshaping Voice Fraud Landscape." Journal of Cyber Policy, December 9, 2025, 1–21. https://doi.org/10.1080/23738871.2025.2597191; Kuźnicka-Błaszkowska, Dominika, and Nadiya Kostyuk. "Emerging Need to Regulate Deepfakes in International Law: The Russo–Ukrainian War as an Example." Journal of Cybersecurity 11, no. 1 (2025): tyaf008. https://doi.org/10.1093/cybsec/tyaf008.

[40] Ilkin Javadov. "The AI Arms Race: Navigating the Dual Edged Sword in Cybersecurity." RSAC Conference. September 19, 2025. https://www.rsaconference.com/library/blog/the-ai-arms-race-navigating-the-dual-edged-sword-in-cybersecurity

[41] Ibrar, Werisha, Danish Mahmood, Ahmad Sami Al-Shamayleh, Ghufran Ahmed, Salman Z. Alharthi, and Adnan Akhunzada. "Generative AI: A Double-Edged Sword in the Cyber Threat Landscape." Artificial Intelligence Review 58, no. 9 (2025): 285. https://doi.org/10.1007/s10462-025-11285-9.

[42] Michele Mosca and Marco Piani. "Quantum Threat Timeline Report 2024. Global Risk Institute, December 6, 2024. https://globalriskinstitute.org/publication/2024-quantum-threat-timeline-report/

[43] Cryptographically-relevant and also scalable for wider use.

[44] Specifically, public-key.

[45] Called by some: "Q-Day". See: Freyer, Oscar, Max Ostermann, Timo Minssen, and Stephen Gilbert. "Quantum Cryptography and Data Protection for Medical Devices before and after They Meet Q-Day." Npj Digital Medicine 8, no. 1 (2025): 620. https://doi.org/10.1038/s41746-025-02082-3.

[46] Csenkey, Kristen, and Nina Bindel. "Post-Quantum Cryptographic Assemblages and the Governance of the Quantum Threat." Journal of Cybersecurity 9, no. 1 (2023): tyad001. https://doi.org/10.1093/cybsec/tyad001.

[47] National Institute of Standards and Technology. "Post-Quantum Cryptography PQC." U.S. Department of Commerce. December 17, 2025. https://csrc.nist.gov/Projects/post-quantum-cryptography ; National Institute of Standards and Technology. "NIST Releases First 3 Finalized Post-Quantum Encryption Standards." U.S. Department of Commerce. August 13, 2024. https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards

[48] Communications Security Establishment. "Roadmap for the migration to post-quantum cryptography for the Government of Canada (ITSM.40.001)." Canadian Centre for Cyber Security. June 2025. https://www.cyber.gc.ca/en/guidance/roadmap-migration-post-quantum-cryptography-government-canada-itsm40001

[49] National Cyber Security Centre. "Timelines for migration to post-quantum cryptography." March 20, 2025. https://www.ncsc.gov.uk/guidance/pqc-migration-timelines ; National Cyber Security Centre. "NCSC Annual Review 2025." October 14, 2025. https://www.ncsc.gov.uk/collection/ncsc-annual-review-2025/chapter-03-keeping-pace-with-evolving-technology/migrating-to-post-quantum-cryptography

[50] Communications Security Establishment, "Roadmap".

[51] Communications Security Establishment. "Preparing your organization for the quantum threat to cryptography (ITSAP.00.017)." Canadian Centre for Cyber Security. February 2025. https://www.cyber.gc.ca/en/guidance/preparing-your-organization-quantum-threat-cryptography-itsap00017

[52] James Dargan, "What Is The Price Of A Quantum Computer in 2025?" The Quantum, Insider, September 19, 2025. https://thequantuminsider.com/2023/04/10/price-of-a-quantum-computer/

[53] David Lague, "U.S. and China race to shield secrets from quantum computers," Reuters, February 13, 2023. https://www.reuters.com/investigates/special-report/us-china-tech-quantum/

[54] Mauritz Kop, "A Bletchley Park for the Quantum Age," War on the Rocks, November 6, 2025. https://warontherocks.com/2025/11/a-bletchley-park-for-the-quantum-age/