Securing Canada's Future: Cybersecurity, Prosperity and Sovereignty

Thomas Gries, Sarah Hamm and Sierra Van Tent

Issue

Amid growing geopolitical uncertainty and economic challenges, the need for a robust cybersecurity ecosystem has become a strategic imperative for governments around the world. For Canada, strengthening institutional capacity in intelligence and cybersecurity is critical to protect national security while collaborating with international partners. This policy brief examines key issues and opportunities in the cybersecurity domain, which address global security challenges facing Canadian prosperity imperatives and its allies.

Background

Geopolitical Challenges

Multi-use Necessities

Canada requires further investment in dual-use technology and infrastructure — those that serve both military and civilian purposes. These investments ensure a commitment to national security and the promotion of Canadian prosperity. This need was recognized by the Trudeau government, which pledged CDN$218 million over the next two decades to invest in Arctic multi-use infrastructure (Doward 2024). Moreover, the federal government's defence policy has committed to contributing to the North Atlantic Treaty Organization (NATO) Innovation Fund, which aims to promote start-ups in their pursuit of dual-use technologies such as artificial intelligence (AI), quantum computing and energy (Department of National Defence 2024, 21-22).

The importance of these technologies and infrastructure is particularly evident in the Arctic territories. Former Defence Minister Bill Blair has emphasized the necessity to invest in projects such as deep-water ports, fibre and satellite communications, and medical treatment facilities to help build prosperity while defending Canada's north, highlighting the need for such investment (Global Affairs Canada [GAC] 2024).

Trump Tensions

The second Trump administration has embraced transactional diplomacy, treating friend and foe alike while focusing solely on what each party can offer the United States. This is evident in the mineral deal which granted the United States access to Ukraine's rare earth metals and other precious resources such as oil and copper, deepening US interests in Ukrainian continued sovereignty (Kottasova and Butenko 2025). This signals a US shift away from traditional alliance interactions toward quid-pro-quo geopolitical dealings and is undoubtedly why Prime Minister Mark Carney listed "establishing a new economic and security relationship with the United States" as his mandate's number one priority (Carney 2025).

Despite being a US neighbour and NATO member, Canada is not exempt from such geopolitical dealings and must demonstrate its strategic value. Despite a CDN$38.6 billion dollar commitment to help modernize NORAD (North American Aerospace Defense Command) and protect NATO's Arctic flank (Government of Canada 2024, 18), as well as a CDN$4.6 billion pledge to technology development (Ciuriak and Carbonneau 2024), Canada still only contributed an estimated 1.37 percent of GDP to defence in 2024 (Burke 2025). President Trump has repeatedly referenced this lack of defence contributions, even saying, "They rely on our military… They've got to pay for that. It's very unfair" (Crawley 2025). This suggests the United States can no longer be relied upon as Canada's security guarantor and that Canada must improve its worth as an ally.

Need for Cybersecurity

The Carney government's mandate has prioritized strengthening the Canadian Armed Forces and acknowledged "the transformative" nature of AI technologies (Carney 2025). This is in-line with the 2024-2025 Canadian budget, which included increased investment in AI through its Canadian Sovereign AI Compute Strategy. This program allocates CDN$2 billion to Canadian researchers and AI companies, with CDN$700 million intended to increase Canadian AI capabilities (Innovation, Science and Economic Development Canada 2025). This investment is significant, as AI has many potential defence applications. Logistics, satellite imagery and information processing can all benefit through AI implementation, reducing costs and freeing up personnel (Araya 2024).

However, with increased AI adoption come certain challenges. Current AI systems remain vulnerable to cyberwarfare through methods such as jamming and spoofing (Payne 2024, 100). Additionally, the widespread availability of AI tools enhances the capabilities of non-state actors, allowing them to "target and automate, at scale, disinformation and influence campaigns, malicious cyber operations, espionage, and foreign interference activities" (Department of National Defence 2024, 9). This could have consequences for Canada, which is increasingly reliant on digital infrastructure for banking, health services, communications, energy and defence (Klein and Hossain 2020, 11). As such, without sufficient attention to, and investment in, Canadian cybersecurity, Canada's critical infrastructure and its investments in AI research and development could be severely undermined.

Canada's Current Innovation Ecosystem: Challenges and Opportunities

Cybersecurity in Canada functions within a broader "innovation ecosystem," composed of four interdependent pillars. The first pillar is material sourcing and processing, which involves the extraction and refinement of critical minerals and rare earth elements used to manufacture the hardware components that support cybersecurity technologies. The second pillar is software development, which is supported by Canada's strong education system, a growing pool of expertise and a strong start-up culture. The third pillar is globalization, where Canadian cybersecurity firms face challenges to scaling to globally competitive "unicorn" status due to domestic constraints. The fourth pillar is commercialization and value creation, which is currently limited by an underdeveloped intellectual property (IP) infrastructure and procurement process supporting the protection of IP.

Material Sourcing and Processing

Canada's current innovation ecosystem begins with the sourcing and extraction of critical minerals used for cybersecurity hardware components. There are numerous critical minerals, including lithium, graphite, cobalt, nickel, copper and other rare earth elements. Critical minerals and rare earth elements are integral to the production of semiconductors, batteries and other technologies (Natural Resources Canada 2022). Canada is resource-rich in these minerals and elements, harbouring some of the largest known reserves and resources (measured and indicated) of rare earths in the world, estimated at over 15.2 million tonnes of rare earth oxide in 2023 (ibid.). This abundance places Canada in a strategically advantageous position to support not only domestic technological needs, but also to contribute to global supply chains. Despite this advantage, Canada's capacity to process these materials and manufacture them into finished cybersecurity hardware remains underdeveloped. Currently, Canada imports a vast amount of this hardware, the mainstay of which is from China (Observatory of Economic Complexity 2023). This dependence stems from domestic barriers, including long approval processes on mining and a tax structure that disincentivizes the development of processing facilities (Bruvels et al. 2025). As a result, raw materials extracted in Canada are exported for processing and returned as finished products, thereby missing opportunities for economic and technological value capture within Canadian borders.

Overreliance on foreign supply chains, especially those tied to China is increasingly viewed as a vulnerability. As Prime Minister Carney has noted in his mandate letter, "the global trading system is currently undergoing the biggest transformation since the fall of the Berlin Wall" (Carney 2025). In the context of shifting global geopolitics, particularly the accelerated China containment strategy pursued by the Trump administration in the United States, Canada is facing renewed pressure to reassess its role within North American security and trade. Canada will, therefore, be expected to foster a regional environment that is less accommodating to Chinese influence, particularly in sectors related to national security and technological sovereignty.

As cybersecurity becomes increasingly intertwined with national defence and economic competitiveness, the need to localize supply chains for hardware components becomes more urgent. This includes investing in the infrastructure and innovation required to refine, process and manufacture hardware domestically. The future of Canada's cybersecurity hardware supply chain will depend on its ability to utilize natural resources while reducing dependencies on foreign actors.

Software Development

Alongside its resource wealth, Canada boasts top-tier universities and produces highly skilled graduates in software development and related disciplines. However, a significant portion of this intellectual capital is migrating out of Canada (*The Brock News* 2018). Canadian universities, largely funded by public money, conduct research, but foreign companies often acquire the resulting IP and commercialize it outside the country. As a result, Canada loses out on potential royalties, job creation, tax revenue and global competitiveness. Thus, while the education system produces quality outputs, Canada's current innovation ecosystem is not conducive to retaining talent and capitalizing on homegrown research.

Globalization

As the global economy has transitioned from tangible goods to intangibles, Canada has failed to adapt. Public procurement accounts for approximately 14.6% of Canada's GDP; however, the government's preference for large incumbent, and often foreign, firms, undermine domestic technology companies and weakens Canada's innovation ecosystem (Carbonneau and Kamat 2024, 4,13). The Organisation for Economic Co-operation and Development recently ranked Canada last out of 38 countries in per capita economic growth and predicted it would be the "worst-performing advanced economy over 2020 to 2030" (Veldheuis and Palacios 2023).

One of the most significant barriers is the inability of start-ups to access investment or the mentorship required to expand. This challenge is exacerbated by Canada's comparatively small venture capital market, particularly in capital-intensive sectors such as cybersecurity, quantum technologies and AI (Tran and Kwok 2022). Combined with a broader culture of risk aversion, this forces firms to seek US-based funding, which often comes with conditions that require relocation of operations, talent and IP abroad, draining Canadian innovations of long-term domestic value (Prescott 2024). In this context, Canada functions as an innovation donor in the global knowledge economy, surrendering its strategic advantage at a time when geopolitical influence increasingly hinges on technological leadership (Fitz-Gerald and Padalko 2025).

Commercialization and Value Added

Canada's weak commercialization infrastructure further compounds this challenge. An underdeveloped IP infrastructure means that many start-ups struggle to secure the legal and financial support required to protect their inventions. Many are discouraged by the high costs, lengthy processes and unclear returns on investment (Gallini and Hollis 2019). This often leads to a failure to secure ownership over key technologies, making firms more vulnerable to foreign acquisition or IP theft, and limiting opportunities for economic benefit and national technological sovereignty.

Furthermore, Canadian public procurement processes are often too arduous for smaller businesses. Without the government acting as an early adopter, something that has played a key role in scaling innovation in the United States and the United Kingdom, Canadian start-ups struggle to secure the early revenue and validation needed to attract private sector investment. An underdeveloped IP and procurement process therefore presents problems in scaling up, which undermines Canada's ability to provide the value-added goods that can compete successfully in the global marketplace.

While Canada possesses many of the right ingredients in the innovation ecosystem — an abundance of critical minerals, strong post-secondary institutions and deep multilateral partnerships — it lacks the procurement strategy and scale-up support necessary to retain IP, grow Canadian firms and compete globally in emerging sectors such as cybersecurity.

Canada loses economic and strategic advantages by not building its own cybersecurity supply chain and, therefore, strengthening its innovation ecosystem should be the strategic objective to help Canada produce hard capability in a way which will support prosperity, sovereignty and security.

Recommendations

Exploration of the development of mineral refining within Canada. While beyond the scope of this project, the strengthening of Canada's innovation system with the promotion of mineral refinement within Canadian borders is encouraged. Canada should commission a study on the mineral refinement processes in allied global producers such as Australia with lithium, and the United States with rare earth metals. It should examine the practices of leading producers in Latin America, such as Chile, which produced 4,400 metric tons of lithium in 2023 (Williams 2025). This can develop Canadian human capacity in the area of mineral production and refinement in a way that promotes good practices globally. Readily available, domestically produced critical minerals can promote the production of cybersecurity hardware within Canada. Finally, domestically produced hardware reduces reliance on foreign states and can allow Canada to export hardware to allied nations.

Establish expert committees. Canada should re-establish expert committees as structured channels to advise the government on how IP, data and knowledge assets are the driver of modern economies. Experts should include representatives from academia, industry, public institutions and innovation sectors with experience in technology, cybersecurity, IP law and commercialization. Canada once had strong expert advisory committees (for example, the Science, Technology and Innovation Council), but these were disbanded in 2015, creating a gap between policy makers, universities, think tanks and technical experts from industries. Expert committees would be dedicated to longitudinal research, which falls outside the immediate mandate of policy makers, similar to the models used in the United States and the United Kingdom. Expert committees would liaise with federal funding agencies to act as a centre of expertise and training, specifically to review and direct funding priorities, align research and development with industrial strategy, and support commercialization of public research.

Establish IP attachés. Canada should improve its cybersecurity innovation through strengthening its IP protection and enforcement. Trade agreements between countries are brokered bilaterally or multilaterally with each country maintaining its own IP laws. Therefore, Canada should consider the development of roles for IP attachés in embassies. IP attachés could be similar to those used by the US Patent and Trademark Office (USPTO) or the United Kingdom's Intellectual Property Office (IPO). The attachés can be hired based on their knowledge of international property law. With the rise of AI and increased digitization will come increased regulatory frameworks regarding governing data, data sharing, and how data and computing equipment is used. Attachés in embassies can strengthen Canadian IP negotiating capability on the ground. Protected IP will encourage cybersecurity innovation, which can be shared with allies, improving Canada's value as a defence partner, in line with Prime Minister Carney's mandate of a defence policy that "fulfills our responsibilities to our allies, and helps build our economy" (Carney 2025). The attaché program could be completely self-funded by mirroring the IPO or the USPTO, which are not funded by taxpayers but instead through patent and trademark fees. (Eurofound 2022; US Patent and Trademark Office 2024).

Protect and project Canadian competencies via science diplomacy streams. Canada should establish itself as a global leader in cybersecurity and technology regulation — embedded in a trusted and predictable legal and democratic system through science diplomacy streams led by GAC. Canada has produced world-leading scientists, particularly in transformative areas such as AI and data science, thus placing it in a strong position to lead on science diplomacy. Completed through the development of Canadian-led capacity-building programs to strengthen digital governance and cyber resilience in partner countries, thereby promoting data sovereignty more broadly. The federal government can project Canadian expertise abroad by embedding cybersecurity training and regulatory support into diplomacy efforts while promoting responsible, rights-based digital norms that reflect Canadian values and encourage global cyber stability.

About the Authors

Thomas Gries is a student in the University of Waterloo's Master of Arts in Global Governance program, based at the Balsillie School of International Affairs.

Sarah Hamm is a student in Wilfrid Laurier University's Master of International Public Policy program, based at the Balsillie School of International Affairs.

Sierra Van Tent is a student in Wilfrid Laurier University's Master of International Public Policy program, based at the Balsillie School of International Affairs.

Acknowledgements

The authors would like to sincerely thank Professor Ann Fitz-Gerald for her guidance and mentorship throughout the course of the fellowship program.

Works Cited

Araya, Daniel. 2024. "Leveraging AI for the Canadian Armed Forces." CDA Institute, expert series. https://cdainstitute.ca/leveraging-ai-for-the-canadian-armed-forces/.

Bruvels, Alex, Micah Zierer-Clyke, Cory Kent, Joshua Chad and Andrew Striling. 2025. "Ontario mining: Rocky industry challenges and opportunities." McMillan. https://mcmillan.ca/insights/ontario-mining-rocky-industry-challenges-and-opportunities/#:~:text=Our%20mining%20sector%20faces%20critical, which%20we%20steadfastly%20remain%20committed.&text=%5B9%5D%20Ibid.,Financial%20Statements%20%7C%20Solaris%20Resources%20Inc.

Burke, Ashley. 2025. "Defence minister accelerates 2% NATO spending timeline to 2027 amid pressure from Trump." CBC. www.cbc.ca/news/politics/defence- spending-two-percent-defence-spending-target-1.7440870.

Carbonneau, Laurent, and Abu Kamat. 2024. *Buying Ideas: Procuring Public Sector Innovation in Canada*. Council of Canadian Innovators. https://www.canadianinnovators.org/content/buying-ideas-procuring-public-sector-innovation-in-canada

Carney, Mark. 2025. "Mandate letter." Office of the Prime Minister. May 21. www.Pm. gc.ca /en/mandate-letters/2025/05/21/mandate-letter.

Ciuriak, Dan and Laurent Carbonneau. 2024. "Canada needs to use government procurement to boost innovation." *The Globe and Mail*. October 6. https://www.theglobeandmail.com/business/commentary/article-canada-needs-to-use-government-procurement-to-boost-innovation/.

Crawley, Mike. 2025. "Trump has threatened Canada in all sorts of ways. What does he really want?" CBC Radio Canada International. https://ici.radio-canada.ca/ rci/en/news/2131634/ trump-has -threatened-canada-in-all-sorts-of- ways-what-does- he-really-want.

Department of National Defence. 2024. *Our North, Strong and Free: A Renewed Vision for Canada's Defence*. Government of Canada. June 6. www.canada.ca/content/dam /dnd-mdn/ documents/ corporate/reports-publications/2024/north-strong-free-2024-v2.pdf.

Doward, Kira Wronska. 2024. "Examining the Canadian government's future approach to Arctic defence." *Nunavut News*. October 15. www.nunavutnews.com/home/examining-the-canadian-governments-future-approach-to-arctic-defence-7552142.

Eurofound. 2022. "Intellectual Property Attaché Network, Measure GB-2011-1/2667 (Measures in United Kingdom)." EU PolicyWatch. https://static.eurofound.europa.eu /covid19db/cases/GB-2011-1_2667.html.

Fitz-Gerald, Ann and Padalko, Halyna. 2025. "Canada's Opportunity to Redefine Its Defence, and Its Value to Allies". Centre for International Governance Innovation. https://www.cigionline.org/articles/canadians-are-ready-to-strengthen-national-defence/

GAC. 2024. *ENGLISH — Launch of Canada's Arctic Foreign Policy* [YouTube Video]. www.youtube.com/live/L2BdNjEJhaw.

Gallini, Nancy and Hollis, Aidan. 2019. "To Sell or scale up: Canada's patent Strategy in a knowledge economy". Institute for Research on Public Policy. https://irpp.org/research-studies/to-sell-or-scale-up-canadas-patent-strategy-in-a-knowledge-economy/

Government of Canada. 2024. “Canada’s Arctic foreign policy.” GAC. www.international.gc.ca/gac-amc/publications/transparency-transparence/arctic-arctique/arctic-policy-politique-arctique.aspx?lang=eng.

Innovation Science and Economic Development Canada. 2025. “Canadian sovereign AI compute strategy.” Government of Canada. https://ised-isde.canada.ca/site/ised/en/canadian-sovereign-ai-compute-strategy.

Klein, Joelle and Kamrul, Hossain. 2020. “Conceptualising human-centric cyber security in the Arctic in light of digitalisation and climate change.” *Arctic Review on Law and Politics* 11: 1–18. https://doi.org/ 10.23865/arctic.v11.1936.

Kottasova, Ivana and Victoria, Butenko. 2025. “Here’s what’s in Trump’s Ukraine minerals deal and how it affects the war.” CNN, May 1. https://edition.cnn.com/2025/05/01/world/ what-we-know-about-trumps-ukraine-mineral-deal-intl.

Natural Resources Canada. 2022. “The Canadian Critical Minerals Strategy.” Government of Canada. https://www.canada.ca/content/dam/nrcan-rncan/site/critical-minerals /Critical-minerals-strategyDec09.pdf,

Observatory of Economic Complexity. 2023. “Computers in Canada trade.” https://oec.world/en/ profile /bilateral-product/computers/reporter/can.

Payne, Kenneth. 2024. *Bright Prospects, Big Challenges: Defence AI in the United Kingdom.* In T. Schütz, H. Borchert and J. Verbovsky (Eds.), *The Very Long Game:* 85–106. Springer. https://doi.org/10.100 7/978-3-031-58649-1.

Prescott, Jimmy. 2024. “Canada’s Tech Industry: Trends and Global Competitiveness.” Beltway Grid Policy Centre. https://beltwaygrid.org/canadas- tech-industry-trends-and-global-competitiveness/.

The Brock News. 2018. “Brain Drain: Study shows many science and tech grads heading to U.S. for work.” Brock University. https://brocku.ca/ brock-news/2018/05/brain-drain-study-shows-many-science-and-tech-grads-heading-to-u-s-for-work/.

Tran, Stephanie and Tiffany, Kwok. 2022. “Scaling Cyber: Advancing Canada’s Cybersecurity Startups.” Cybersecure Policy Exchange, Toronto Metropolitan University. https:// dais.c a/wp- content /uploads/2023/11/ScalingCyber.pdf.

US Patent and Trademark Office. 2024. “Budget and financial information.” US Department of Commerce. www.uspto.gov/about-us/performance-and- planning/budget-and-financial-information.

Veldhuis, Niels and Milagros, Palacios. 2023. “Cabinet shuffle won’t improve Canada’s weak economic performance” Fraser Institute. https://www.fraserinstitute.org/commentary/cabinet-shuffle-wont-improve-canadas-weak-economic-performance

Williams, Georgia. 2025. “Top 9 Lithium-producing Countries.” Investing News Network. March 5. https://investing news.com/daily/resource-investing/battery-metals-investing/lithium-investing/lithium-production-by-country/.