

Policy Brief No. 215 – November 2025

Dual-Use Technologies in the Age of Intangibles

James W. Hinton

Key Points

- Dual-use technologies are increasingly central to global economic resilience, innovation strategies and national defence. Canada's current trajectory risks surrendering strategic and economic benefits if it does not prioritize investment in domestic companies that develop and commercialize dual-use technologies.
- Without a shift in approach, increased defence spending will disproportionately benefit foreign firms, weakening Canada's ability to build sovereign capacity.
- Structural reforms are urgently needed to prioritize Canadian innovators in defence procurement; expand the freedom to operate for domestic firms with intellectual property (IP) frameworks that retain ownership and control of key dual-use technologies; and build sovereign compute capacity and infrastructure to secure Canadian data and algorithms.
- Continued neglect of these areas will erode Canadian sovereignty and deepen economic dependence on countries that dominate dual-use technology.

Introduction

Dual-use technology refers to technology that has both civilian and military applications. These technologies are increasingly central to national security, economic resilience and technological leadership. Dual-use technologies have become increasingly important for a nation's economic growth and in a country's ability to defend itself. They are critical to fostering competitiveness, resilience and crucial national defence and security, especially in the current international high-threat geopolitical environment (Chivvis and Keating 2024).¹

Initially, dual-use technology focused on nuclear technologies that have well-known military uses (for example, nuclear warfare) and civilian uses (for example, nuclear energy). Today, dual-use technologies encompass a range of industries and technology areas including "artificial intelligence, advanced materials, nanotechnology,

¹ See https://research-and-innovation.ec.europa.eu/research-area/industrial-research-and-innovation/dual-use-technologies_en.

About the Author

James (Jim) W. Hinton is a senior fellow at CIGI, where he contributes expertise on intellectual property (IP) and innovation. He is an IP lawyer, patent agent and trademark agent with his firm Own Innovation. He is a fellow at the Balsillie School of International Affairs, building capacity on digital and technology governance. Jim is also an assistant professor at Western University with a standing appointment in the Faculty of Engineering.

cybersecurity tools, satellite technologies, biotechnologies, quantum, aerospace and drones.”²

Dual use is not simply a defence and commercial strategy; it is also a business strategy for innovative companies. Firms developing and commercializing dual-use technologies must manage two often distinct customers and value chains. While there is a benefit to having a variety of customers from both government and commercial buyers, selling to government often means long procurement cycles, and the need to have sophisticated government relations resources and meet onerous government reporting requirements.

Canada, as an open economy, is an example of a country that has overlooked the principle that national security depends on the vitality and resilience of its economy (Business Council of Canada 2024). Additionally, despite Canada’s capacity for discovery research, Canada has not been able to economically benefit from this research (Norman 2025).

This policy brief examines how dual-use technologies are being developed and prioritized globally in an intangibles-driven economy, as well as how countries are leveraging them to strengthen both national security and economic independence. It evaluates Canada’s position in its industrial activity, research capacity and gaps in IP ownership, as compared to other players in the development of dual-use technologies internationally. Drawing on these insights and key challenges, policy recommendations are proposed to enhance Canada’s role in the global dual-use innovation landscape, especially within strategic areas, including artificial intelligence (AI), quantum technologies and nuclear energy. The policy approaches discussed herein may apply equally to other nations with a sovereignty deficit, limited autonomy and barriers to commercializing dual-use technologies.

2 Ibid.

Background

In 2014, North Atlantic Treaty Organization (NATO) members agreed to commit a minimum of two percent of their GDP to defence spending within a decade. Ten years later, 23 of 32 members reached this goal. For example, the United States currently spends 3.38 percent of its GDP on defence (Blais-Savoie 2025). In June 2025, the Canadian government announced that Canada and its NATO allies have committed to a new five percent GDP defence spending target by 2035 (Brewster and Zimonjic 2025), which could cost up to \$150 billion³ annually, and \$1 trillion over a 10-year period (Brewster 2025). This increase in spending presents the opportunity to align defence investments with dual-use innovation, particularly in areas such as AI, cybersecurity, quantum technologies and aerospace (Galea and Norman 2025). In order for Canada to realize this potential, it must strategically drive its significantly larger defence budget into Canadian-headquartered firms. It is critical that the Government of Canada stops procuring core defensive capabilities fundamental to its national and economic security from foreign firms and rather focus on developing its capabilities domestically.

Dual Use in the Age of Intangibles: IP

Dual-use technology, like all innovation, is owned, controlled and commercialized by leveraging intellectual property rights (IPRs), which include patents, industrial designs, trade secrets, copyrighted works such as software code, trademarks and contractual agreements. It is essential to understand what countries own and how they control defence technology for building a domestic dual-use industry, considering that existing IP positions will limit the freedom to operate of any new industry actors. Freedom to operate is the ability to innovate, scale and export in particular markets without being limited by the IPRs of others. Freedom to operate also includes other legal, regulatory and licensing constraints. Further, IP, including patenting, takes a significant amount of time, resources and foresight to put into position. Patents may play a key role in a company's ability to exploit its research and development (R&D) of technologies and prevent others from making, using, importing or selling patented technologies.

By way of an example of patent holdings, as shown in Table 1, the top three American defence companies each have tens of thousands of patents and patent applications globally, and

Table 1: Global Patent Holdings by Key Defence Companies

Company	Headquarters	Focus Areas	Global Patents	Canadian Patents
Lockheed Martin	United States	Aerospace, arms, defence, information security	30,112	1,612
RTX	United States	Aerospace, defence, spacecraft, aviation	67,592	2,841
Northrop Grumman	United States	Aircraft, spacecraft, cybersecurity systems, radar technologies	89,060	4,657
CAE	Canada	Defence, aerospace, aviation, military	467	120

Data source: Global Patent Databases, accessed via Questel Orbit Intelligence, September 2025.

³ All dollar figures in Canadian dollars.

thousands of patents and patent applications in Canada.⁴ For comparison, a top Canadian defence company, CAE, has just hundreds of global patents and patent applications, and just over 100 patents and patent applications in Canada, which is orders of magnitude less than the top American defence companies.⁵

Canadian Defence Firms and Freedom to Operate Challenges

Canada's defence industrial base is made up of more than 700 companies contributing more than \$12.4 billion to Canada's national economy and employing nearly 100,000 people (McKay 2024, 48). Most Canadian defence firms include small and medium-sized enterprises (SMEs) occupying lower tiers of global value chains (that is, manufacturing parts, providing specialized services or support logistics rather than producing complete defence systems themselves) (Jenkins 2013). These firms frequently depend on US or European prime defence contractors, companies that often retain control over essential IP and have the ability to limit Canadian companies' freedom to operate. Foreign-owned firms are often given major Canadian defence contracts, then restrict access across the value chain to proprietary technology. Consequently, Canadian firms often have no choice but to license key components or software under restrictive terms, significantly undermining their competitiveness and strategic autonomy (ibid.).

Researchers at 50 Canadian universities were found to have collaborated with Chinese military institutions on hundreds of advanced-technology research projects, generating knowledge for China's defence sector (Fife and Chase 2023). More than 20 Canadian universities have partnered on hundreds of patents with Huawei, a company that has ties with the Chinese state (Silcoff et al. 2018). The United States and other Five Eyes allies have also expressed concern that Canadian-developed technologies could be transferred to the Chinese military due to foreign investments from China, especially in areas such as 5G infrastructure, AI and cybersecurity (Library of Congress, Federal Research Division 2021). Further, Canada's lack of a comprehensive

cybersecurity strategy and oversight of research partnerships has resulted in vulnerability to foreign influence and technology transfer risks (ibid.).

Despite Canada's investments in research areas such as AI, quantum computing and aerospace, there is a fundamental lack of centralized coordination among departments and agencies, as well as a defence procurement system that is bureaucratic, slow and risk averse, making developing dual-use technologies an arduous process to navigate (Salt 2025). This steep trajectory discourages firms from engaging with domestic defence buyers, pushing them toward international markets where procurement is faster and more predictable (One9 2024). Canada's procurement ecosystem lacks the speed and strategic alignment curated in the United States and the United Kingdom, where innovation funding is closely tied to procurement cycles (Salt 2024). There is also a need to align Canadian research toward industry needs, in order for Canada to compete with countries prioritizing research in dual-use technologies (Lowey 2024). To their detriment, Canadian firms developing dual-use applications receive comparatively less public support at critical stages of development and commercialization.

Dual Use in the Age of Intangibles: Data

In a modern economy, data is a crucial asset for both commercial and defence capabilities. Data is the foundation for the development of AI, automation and digital services, leading to productivity, innovation and economic competitiveness (Ciuriak 2025). Countries that control vast, high-quality data sets gain a significant advantage in dual-use technologies. Economically, access to proprietary data sets accelerates innovation, controls global value chains and determines which countries will lead technological development.

Digital sovereignty defines Canada's ability to ensure that its data and proprietary algorithms, whether commercial, personal or defence-related, are governed solely by Canadian law. As it currently stands, even if data and algorithms are stored on servers physically located in Canada, Canada

⁴ See <https://people.defensenews.com/top-100/>.

⁵ See <https://canadiandefencereview.com/top-defence-companies-ranking/2025-top-100-defence-companies/>.

may not have jurisdiction over these assets, as this is determined by corporate ownership and legal control rather than by geography. This undermines national sovereignty and creates vulnerabilities, especially within sensitive sectors such as health, defence and AI. At least 25 percent of Canada's domestic internet traffic is unnecessarily routed through the United States, where it loses Canadian control and protection and may be subject to US surveillance and other forms of interference, leaving Canada's digital infrastructure vulnerable to US companies (Organizations and Individuals Concerned about Canada's Digital Sovereignty 2025). Additionally, under the US Clarifying Lawful Overseas Use of Data Act (the CLOUD Act), American authorities have the right to demand access to data from US-based technology firms, regardless of whether the data was stored physically within Canada, and without approval from Canadian authorities (Galea and Norman 2025). For example, a Microsoft representative described how US law supersedes foreign law when it comes to data requests: "If the United States were to issue a legal request to Microsoft...Microsoft would comply regardless of French or EU law" (Rudolph 2025).

Countries that lack control over their own data and algorithms ultimately lose the productivity, innovation and security benefits that would have otherwise resulted from such developments, including dual-use technologies (Ciuriak 2020). Dual-use technologies rely heavily on secure, sovereign data environments. Without sovereign compute infrastructure, Canadian companies may rely on foreign-owned cloud services when hosting data within Canada, exposing them to risks such as IP theft, foreign surveillance and loss of legal control (Office of the Privacy Commissioner of Canada 2020). Additionally, without sovereign compute infrastructure, government agencies are unable to guarantee privacy for citizens or security in defence operations (Treasury Board of Canada Secretariat 2018). Canada will continue to fall behind in AI, biotech and quantum innovation as data becomes restricted due to the lack of sovereignty and parallel risk of cyberattacks (Public Safety Canada 2025). Without Canadian-owned and -controlled digital infrastructure, including sovereign cloud compute services, Canada will not be able to guarantee the safe use, access or protection of data and algorithms necessary for the development and commercialization of dual-use technologies.

Global Leaders: Europe and South Korea

Enhanced dual-use research within the European Union has led to significantly enhanced GDP, as the development of dual-use technologies results in cross-sectoral cooperation, innovation, investment and industrial growth (European Commission, Directorate-General for Research and Innovation 2025). Through the cooperation between defence and civilian research initiatives, EU member states are then able to establish high-value markets and attract international collaborations that provide substantial benefits to national and regional economies (ibid.). The progression of dual-use research in the European Union has been closely linked to enhancements in overall national productivity, as it fosters higher value markets and attracts international collaborations (ibid.).

South Korean defence companies have recently been set to surpass 100 trillion won (\$98.7 billion) in combined orders (Jung and Kim 2025). At the same time, the Korean Intellectual Property Office has been elevated to the status of a Ministry of Intellectual Property, establishing a government-wide innovation framework and increasing national competitiveness and global leadership in critical technologies such as AI (ibid.). Such investments and collaborative changes supported by the government aim to position Korea as a global leader in its development of technology and culture (Suh 2025). Other nations should look to these global leaders to inform their own strategies to develop and commercialize dual-use technology.

Policy Recommendations

If Canada aims to invest significantly in defence technology, upwards of \$1 trillion over a decade, this funding must prioritize the growth of a Canadian defence industry, especially within strategic areas, including AI, quantum technologies and nuclear energy. However, not addressing the IP positions of incumbent players will force domestic companies into lower value positions, without the freedom to operate that is needed to scale and grow internationally. Thus, Canada must not only invest in procurement reform as well as R&D funding but

also in enabling domestic firms to generate, protect and commercialize intangible assets including IP and data. Strengthening data governance and maintaining sovereignty over sensitive technology are also critical to ensuring that dual-use innovation results in lasting economic and security for Canadians. Improving Canadian economic prosperity and security will mean building, capitalizing and scaling small Canadian firms into global Canadian-headquartered companies.

Policy action needs to recognize that dual-use technologies in the age of intangible assets require updated policy levers across at least three fronts: building a domestic defence industry; managing freedom to operate; and providing sovereign data and computing capacity.

Build a Globally Competitive Domestic Defence Industry

- Canada has historically over-relied on foreign firms to procure defence technology. Instead, Canada should prioritize procuring the vast majority of defence technologies from Canadian-headquartered firms. Further, since Canada's current defence industry is made up of many SMEs, procurement strategies must be tailored to meet the needs of these small and medium-sized companies, placing Canadian firms as prime contractors, so that Canadian firms can control the defence and civilian value chains.
- Since dual-use business strategies will be new to many Canadian firms, Canada must invest heavily in resources (for example, training programs and funding) that support the growth of Canadian dual-use technology companies.

Manage Freedom to Operate

- Since Canadian firms do not generate IP, namely patents, at the same rate as their global peers, Canadian firms will need to be resourced to fortify their IP position. Further, terms in government procurement must ensure the retention of IP and data assets within Canadian companies developing dual-use technologies.
- Canadian firms, with their small and fragmented IP positions, have limited freedom to operate because of the outsized existing patent position of incumbent defence players. The freedom to operate of Canadian dual-use companies must be increased using tools such as

state-supported defence-focused patent collectives (building on models based on, for example, the US Department of Defense IP policies and Canada's Innovation Asset Collective).

- Canada must discontinue its role as a source of technology for foreign military and military-linked firms. Canadian research institutions must be incentivized to support R&D within Canadian dual-use firms on IP transfer terms that directly benefit Canada.

Data and Compute Sovereignty

- Canada must end its reliance on foreign-controlled compute infrastructure. Canada must build domestic sovereign compute infrastructure that can support the security of data and algorithms for sensitive defence applications, especially for compute-heavy technologies such as AI.
- Since Canadian firms do not have access to a deep well of data as compared to global peers, Canada must protect and avail data sets within dual-use sectors to Canadian firms. Curated access to proprietary data is critical to enabling innovation in AI, defence systems and autonomous technologies.

Conclusion

Canada has a critical window of opportunity to enhance its abilities domestically as it commits to a higher level of defence spending. However, if this spending is not strategically implemented, Canada will remain dependent on foreign suppliers, further eroding its sovereignty and limiting its economic growth. Canada can look to global leaders such as the United States, the European Union and South Korea in how to build its defence capabilities. By properly aligning defence procurement, increasing freedom to operate and improving data sovereignty, Canada can capture the long-term security, defence and economic benefits of dual-use technologies.

Acknowledgement

The author would like to thank Anna Shin for research and contributions to the policy brief.

Works Cited

- Blais-Savoie, Fabrice. 2025. "A Dual-Use Solution to a Dual Problem: Canada's Innovation and Defence Spending." Network for Strategic Analysis. April 16. <https://ras-nsa.ca/a-dual-use-solution-to-a-dual-problem-canadas-innovation-and-defence-spending/>.
- Brewster, Murray. 2025. "NATO's 5% benchmark would cost Canada \$150B a year, Carney says." CBC News, June 24. www.cbc.ca/news/politics/nato-leaders-summit-1.7568938.
- Brewster, Murray and Peter Zimonjic. 2025. "Canada promises to spend 5% of GDP on defence by 2035 in pact with NATO leaders." CBC News, June 25. www.cbc.ca/news/politics/canada-agrees-five-percent-gdp-defence-spending-1.7570191.
- Business Council of Canada. 2024. *Security & Prosperity: The Economic Case for a Defence Industrial Base Strategy*. November 25. Ottawa, ON: Business Council of Canada. www.thebusinesscouncil.ca/report/security-and-prosperity/.
- Chivvis, Christopher S. and Jack Keating. 2024. "Cooperation Between China, Iran, North Korea, and Russia: Current and Potential Future Threats to America." Carnegie Endowment for International Peace, October 8. <https://carnegieendowment.org/research/2024/10/cooperation-between-china-iran-north-korea-and-russia-current-and-potential-future-threats-to-america?lang=en>.
- Ciuriak, Dan. 2020. *Economic Rents and the Contours of Conflict in the Data-driven Economy*. CIGI Paper No. 245. Waterloo, ON: CIGI. www.cigionline.org/publications/economic-rents-and-contours-conflict-data-driven-economy/.
- . 2025. *Enterprise Value and the Value of Data*. CIGI Paper No. 327. Waterloo, ON: CIGI. www.cigionline.org/publications/enterprise-value-and-the-value-of-data/.
- European Commission, Directorate-General for Research and Innovation. 2025. *Unlocking the potential of dual-use research and innovation*. Luxembourg: Publications Office of the European Union. <https://data.europa.eu/doi/10.2777/5771805>.
- Fife, Robert and Steven Chase. 2023. "Canadian universities conducting joint research with Chinese military scientists." *The Globe and Mail*, January 30. www.theglobeandmail.com/politics/article-chinese-military-scientists-canadian-universities/.
- Galea, Irene and Pippa Norman. 2025. "How Carney's historic defence spending could change the economy," July 22, in *The Decibel*, 22:03. www.theglobeandmail.com/podcasts/the-decibel/article-how-carneys-historic-defence-spending-could-change-the-economy/.
- Jenkins, Tom. 2013. *Canada First: Leveraging Defence Procurement Through Key Industrial Capabilities*. Report of the Special Adviser to the Minister of Public Works and Government Services. February. Ottawa, ON: Government of Canada. https://publications.gc.ca/collections/collection_2013/tpsgc-pwgsc/P4-52-2013-eng.pdf.
- Jung, Han-kook and Seo-young Kim. 2025. "S. Korean defense giants set to surpass 100 trillion won in combined orders." *The Chosun Daily*, May 6. www.chosun.com/english/industry-en/2025/05/06/QEWK537NZNCZHCKMFPUWMBA7HU/.
- Library of Congress, Federal Research Division. 2021. *Crossed Wires: China's Investments in the Canadian Technology Sector*. August 31. Washington, DC: Library of Congress, Federal Research Division. www.loc.gov/static/services/federal-research-division/our-federal-research/documents/CrossedWires_ChinasInvestmentsInTheCanadianTechnologySector.pdf.
- Lowe, Mark. 2024. "Canada is failing to capitalize on its technological potential: patents and productivity." *Research Money*, June 5. <https://researchmoneyinc.com/article/canada-is-failing-to-capitalize-on-its-technological-potential-patents-and-productivity>.
- McKay, John. 2024. *A Time for Change: Reforming Defence Procurement in Canada*. Report of the Standing Committee on National Defence. June. Ottawa, ON: House of Commons. www.ourcommons.ca/Content/Committee/441/NDDN/Reports/RP13203590/nddnrp12/nddnrp12-e.pdf.
- Norman, Pippa. 2025. "Hundreds of Canadian companies making 'dual use' products useful for defence, survey finds." *The Globe and Mail*, August 25. www.theglobeandmail.com/business/article-canadian-companies-dual-use-products-defence/.
- Office of the Privacy Commissioner of Canada. 2020. "Appendix 3: Cross-border Data Flows and Transfers for Processing — Jurisdictional Analysis." September 28. www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2021/tbdf_app3/.
- One9. 2024. "Briefing Note: Investing Strategically for Canada's National Security." May 24. www.one9.ca/originals/investing-strategically-for-canadas-national-security.
- Organizations and Individuals Concerned about Canada's Digital Sovereignty. 2025. "Open Letter: Standing on Guard for Canada's Digital Sovereignty." Letter to the Prime Minister of Canada. September 2. www.documentcloud.org/documents/26080445-open-letter-to-prime-minister-mark-carney.
- Public Safety Canada. 2025. *Canada's National Cyber Security Strategy: Securing Canada's Digital Future*. Ottawa, ON: Government of Canada. www.publicsafety.gc.ca/cnt/rsrscs/pblctns/ntnl-cbr-scrtrt-2025/index-en.aspx.
- Rudolph, Alexander. 2025. "Microsoft Admits: US Law Supersedes Canadian Sovereignty." *Canadian Cyber in Context*, Substack, July 21. www.cyberincontext.ca/p/microsoft-admits-us-law-supersedes.
- Salt, Alexander. 2024. "Canada and the Interoperability Challenge." Canadian Global Affairs Institute. October. www.cgai.ca/canada_and_the_interoperability_challenge.
- . 2025. "Venture Capital Financing and Canadian Defence." Canadian Global Affairs Institute. June. www.cgai.ca/pp_venture_capital_financing_and_canadian_defence.

Silcoff, Sean, Robert Fife, Steven Chase and Christine Dobby. 2018. "How Canadian money and research are helping China become a global telecom superpower." *The Globe and Mail*, May 26. www.theglobeandmail.com/canada/article-how-canadian-money-and-research-are-helping-china-become-a-global/.

Suh, Tae Jun. 2025. "KIPO to become Ministry of Intellectual Property in Korea." LinkedIn. www.linkedin.com/posts/tae-jun-suh-badaco_kipo-activity-7364847386839416832-ZrTj/.

Treasury Board of Canada Secretariat. 2018. "Government of Canada Cloud Adoption Strategy: 2018 update." Government of Canada. www.canada.ca/en/government/system/digital-government/digital-government-innovations/cloud-services/government-canada-cloud-adoption-strategy.html.

About CIGI

The Centre for International Governance Innovation (CIGI) is an independent, non-partisan think tank whose peer-reviewed research and trusted analysis influence policy makers to innovate. Our global network of multidisciplinary researchers and strategic partnerships provide policy solutions for the digital era with one goal: to improve people's lives everywhere. Headquartered in Waterloo, Canada, CIGI has received support from the Government of Canada, the Government of Ontario and founder Jim Balsillie.

À propos du CIGI

Le Centre pour l'innovation dans la gouvernance internationale (CIGI) est un groupe de réflexion indépendant et non partisan dont les recherches évaluées par des pairs et les analyses fiables incitent les décideurs à innover. Grâce à son réseau mondial de chercheurs pluridisciplinaires et de partenariats stratégiques, le CIGI offre des solutions politiques adaptées à l'ère numérique dans le seul but d'améliorer la vie des gens du monde entier. Le CIGI, dont le siège se trouve à Waterloo, au Canada, bénéficie du soutien du gouvernement du Canada, du gouvernement de l'Ontario et de son fondateur, Jim Balsillie.

Credits

Research Director, Transformative Technologies **Tracey Forrest**
Director, Program Management **Dianna English**
Program Manager **Reanne Cayenne**
Program Manager **Grace Wright**
Manager, Publications **Jennifer Goyder**
Graphic Designer **Abhilasha Dewan**

Copyright © 2025 by the Centre for International Governance Innovation

The opinions expressed in this publication are those of the author and do not necessarily reflect the views of the Centre for International Governance Innovation or its Board of Directors.

For publications enquiries, please contact publications@cigionline.org.



The text of this work is licensed under CC BY 4.0. To view a copy of this licence, visit <http://creativecommons.org/licenses/by/4.0/>.

For reuse or distribution, please include this copyright notice. This work may contain content (including but not limited to graphics, charts and photographs) used or reproduced under licence or with permission from third parties. Permission to reproduce this content must be obtained from third parties directly.

Centre for International Governance Innovation and CIGI are registered trademarks.

67 Erb Street West
Waterloo, ON, Canada N2L 6C2
www.cigionline.org

