ECONSTOR
Make Your Publications Visible.

A Service of

ZBW Leibniz-Informationszentrum Wirtschaft
Leibniz Information Centre for Economics

Durand, David; Briggs, Kyle

Working Paper

Intellectual property is economic and national security

CIGI Papers, No. 340

Provided in Cooperation with:
Centre for International Governance Innovation (CIGI), Waterloo, Ontario

Suggested Citation: Durand, David; Briggs, Kyle (2025) : Intellectual property is economic and national security, CIGI Papers, No. 340, Centre for International Governance Innovation (CIGI), Waterloo (Ontario)

This Version is available at:
https://hdl.handle.net/10419/337188

Standard-Nutzungsbedingungen:

Die Dokumente auf EconStor dürfen zu eigenen wissenschaftlichen Zwecken und zum Privatgebrauch gespeichert und kopiert werden.

Sie dürfen die Dokumente nicht für öffentliche oder kommerzielle Zwecke vervielfältigen, öffentlich ausstellen, öffentlich zugänglich machen, vertreiben oder anderweitig nutzen.

Sofern die Verfasser die Dokumente unter Open-Content-Lizenzen (insbesondere CC-Lizenzen) zur Verfügung gestellt haben sollten, gelten abweichend von diesen Nutzungsbedingungen die in der dort genannten Lizenz gewährten Nutzungsrechte.

Terms of use:

Documents in EconStor may be saved and copied for your personal and scholarly purposes.

You are not to copy documents for public or commercial purposes, to exhibit the documents publicly, to make them publicly available on the internet, or to distribute or otherwise use the documents in public.

If the documents have been made available under an Open Content Licence (especially Creative Commons Licences), you may exercise further usage rights as specified in the indicated licence.

https://creativecommons.org/licenses/by/4.0/

WWW.ECONSTOR.EU

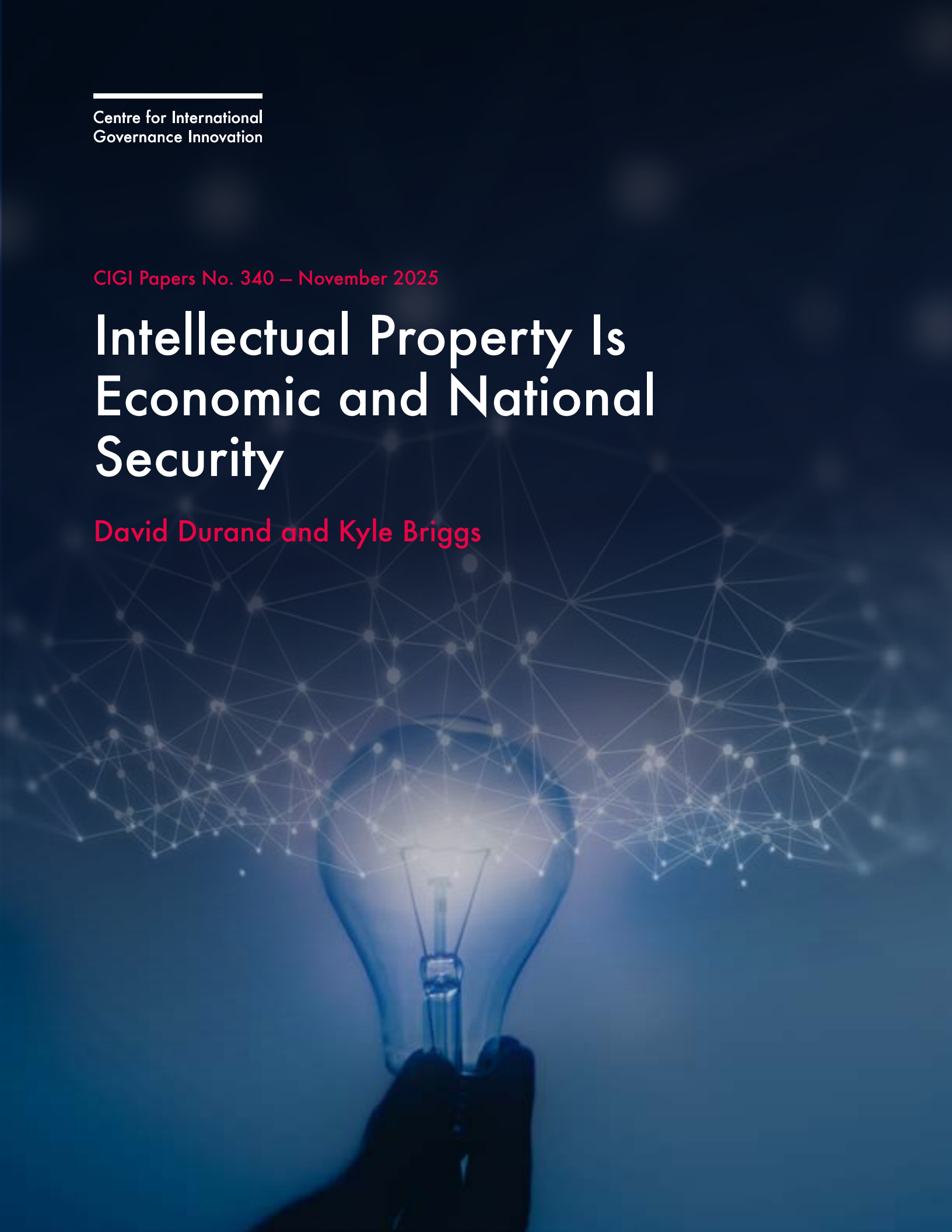
Mitglied der Leibniz-Gemeinschaft

Centre for International
Governance Innovation

CIGI Papers No. 340 — November 2025

Intellectual Property Is Economic and National Security

David Durand and Kyle Briggs



Centre for International
Governance Innovation

CIGI Papers No. 340 — November 2025

Intellectual Property Is Economic and National Security

David Durand and Kyle Briggs

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

Managing Director and General Counsel Aaron Shull
Director, Program Management Dianna English
Senior Program Manager Jenny Thiel
Program Manager Grace Wright
Publications Editor Christine Robertson
Publications Editor Susan Bubak
Graphic Designer Sami Chouhdary

Copyright © 2025 by the Centre for International Governance Innovation

The opinions expressed in this publication are those of the authors 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

Table of Contents

About the Authors

David Durand is the co-founder of MVIP Solutions, Inc. and an intellectual property (IP) lawyer and board member of FORPIQ and AIoT Canada. He is co-author of the Simple Agreement for Innovation Licensing (SAIL) framework (www.howtoSAIL.ca) and has appeared before the standing committees on finance as well as science and research on the support for the commercialization of IP. David has also contributed a chapter titled "What's the Big Idea? The Crossroads Between Investment and IP" in *Intellectual Property Management for Start-Ups* (Springer, 2023); an article on closing the gender gap in *WIPO Magazine*; and another article on national security in *The Globe and Mail*. His full biography can be found at www.daviddurand.ca.

Kyle Briggs is a physicist, a deep-tech entrepreneur and the Entrepreneur in Residence for the Faculty of Science at the University of Ottawa. He holds a Ph.D. in biophysics from the University of Ottawa and is the former CEO of Northern Nanopore Instruments, a company that operated at the interface of nanotechnology and biotechnology from 2020 to 2023 prior to its acquisition. He has won numerous awards for his research, including the CMC Douglas R. Colton Medal for his contributions in nanotechnology. Kyle is the author of *CanInnovate*, an innovation policy newsletter that seeks to shine a light on challenges to commercialization of emerging technologies and suggest practical policy changes through which they can be overcome. In service of this goal, he is also a co-author of the SAIL framework.

Acronyms and Abbreviations

AI	artificial intelligence
AIDA	Artificial Intelligence and Data Act
CSIS	Canadian Security Intelligence Service
DND	Department of National Defence
FDI	foreign direct investment
IA	intellectual assets
ICA	Investment Canada Act
IFRS	International Financial Reporting Standards
IP	intellectual property
ISED	Innovation, Science and Economic Development Canada
M&A	mergers and acquisitions
NATO	North Atlantic Treaty Organization
NSERC	Natural Sciences and Engineering Research Council of Canada
OECD	Organisation for Economic Co-operation and Development
OSINT	open-source intelligence
R&D	research and development
SAIL	Simple Agreement for Innovation Licensing
SWOT	strengths, weaknesses, opportunities and threats

Executive Summary

This paper explores the economic security implications of Canada's management of intellectual assets (IA) and intellectual property (IP) and makes the argument that sound management of IA/IP is a requirement for economic and national security. It reviews the concepts of economic warfare and economic security, describing how attacks on IP, through both legal and illegal means, can be used to undermine economic security and sovereignty. Vulnerabilities in Canada's IP regime arising from fragmented policy frameworks are highlighted, with a focus on the implications for data and IP relating to emerging technologies, including those with dual-use potential.

The paper concludes with a set of five key recommendations for policy reform aimed at securing Canada's IA/IP. First, establish an open-source intelligence (OSINT) agency to identify innovation areas of strategic priority for research, IP security and defensive publication and to directly inform and support the rest of the recommendations. Second, take specific measures necessary to secure the outputs of Canadian research. Third, reform foreign investment controls and actively subsidize acquisition of foreign technologies of strategic interest. Fourth, invest in sovereign cloud compute and storage, including quantum computing. And fifth, harmonize key legal frameworks at the federal level, including trade secret legislation and post-secondary IP governance.

Introduction

Many of Canada's crown jewels, from its natural resources to the intangible outputs of its world-class research institutions, are vulnerable to acquisition and exploitation by foreign interests using both front- and backdoor techniques.

While Canada has the raw potential to be an economic powerhouse, its approach to managing its myriad advantages leaves much to be desired. Where tangible assets are concerned, the implications are relatively easy to understand. Much of Canadian forestry is controlled by Malaysia (Dubinsky and Thompson 2023). Canada's mining industry is increasingly controlled by Australia (McGee 2023) and, to an increasing degree, China, despite a crackdown on foreign investment in Canadian critical minerals (Lorinc and Platt 2024). In addition, about one-fifth of the world's uranium is mined in Canada but is backed with significant foreign investment (World Nuclear Association 2025). Meanwhile, our agricultural potential remains largely untapped despite our ability, in principle, to project food power (Ashton 2025).

Much less obvious, but no less impactful, are the implications of Canada's poor management of IA, IP and data.[1] Control over these assets is often lost through entirely legal means (Azzi et al. 2025) and may even be reinforced by Canada's approach to technology and economic development. Globalization, fragmentation and disconnection of supply chains provide new avenues for attacks on Canadian sovereignty, which, while they remain below the threshold that would provoke an armed response, represent an evolution of warfare predicated on the idea of "winning without fighting" (Garbers 2025b).

Achieving economic security in the rapidly evolving geopolitical landscape requires a cohesive and security-focused national strategy with respect to IA/IP. These assets are not only key to strengthening Canada's competitive advantage in a global economy but also to promoting economic growth, prosperity, security and sovereignty (Edler et al. 2023; Business Council of Canada 2023). Canada's approach to governance of its IA, particularly where foreign direct investment (FDI) is concerned (Matthews and Rice 2022), has left us vulnerable to economic warfare (Garbers 2025b, 2025c), and other countries are taking advantage (Wong Leung, Robin and Cave 2024). While China is the most obvious and salient threat (Bell 2025), Canada's IA management practices leave potential value on the table even with respect to allies.

As Canada's alliances evolve in response to the "United States' unanticipated and jarring approach to resetting its relations with allies and adversaries alike" (Garbers 2025b), Canada's contribution to the North Atlantic Treaty Organization (NATO) and the

1 A detailed introduction to IA and IP is provided in Appendix 1 to this paper.

Five Eyes alliance[2] must change. The value of IA/IP and data is not limited to their economic potential. Following recent recognition of the importance of emerging technologies to defence and security (Baldwin 2024; Araya and Mavinkurve 2022), IA and IP are also key intelligence assets that could rank among Canada's most valuable contributions to the global allied intelligence and defence community. Canada's very productive research infrastructure and highly educated talent should be positioned as cornerstones of its contribution to global security. Instead, Canada's IA/IP assets are underutilized, misunderstood and leaking.

To address this, the nexus between IA/IP, data and emerging technologies must be better understood by businesses and policy makers alike. In this paper, the authors review the concept of economic warfare, provide an overview of the ways in which Canada's approach to IA/IP management leads to lost potential for value creation and weakened national and economic security, and make recommendations toward securing and building on Canada's competitive advantage in a global economy. The authors emphasize the importance of public sector data literacy and OSINT, highlighting examples where key policy insights of national and economic security relevance can be gleaned through careful analysis of public information.

What Is Economic Warfare?

The notion of warfare has evolved to include the idea of subthreshold conflict (NATO 2022, 2023; Ministry of Defence 2021); grey-zone conflict (Gizewski and Teeple 2023; Qasrawi et al. 2023); and hybrid warfare (Costigan and Hennessy 2024). These terms are used to refer to actions taken by state actors that do not meet the threshold at which they would spark a kinetic response, but which seek to achieve broadly similar objectives, particularly in the context of asymmetric conflict (QinetiQ 2020; Nelson 2022). While these concepts lack consistent definitions in international law (Gizewski and Teeple 2023; Mačák, Dias and Kasper 2025), examples of subthreshold conflict include:

- cyber and information warfare (Hakala and Melnychuk 2021);
- lawfare (Qiao and Wang 2015);
- use of narrative and public communication as a tool to "change or maintain the attitudes and behaviours of key target audiences" (NATO 2023; Waldman 2023);
- information confrontation tactics (Eggen 2024);
- disinformation and social media manipulation (Serrato and Wallis 2020; Strick 2020; Thomas 2020; Thomas, Zhang and Currey 2020);
- election interference (Hogue 2025); and
- other tactics intended to undermine state capabilities or influence perceptions and policy (Policy Exchange 2020).

Work by Hugh Segal and Ann Fitz-Gerald (2021) at the Centre for International Governance Innovation (CIGI) provides an overview of the constantly changing threat landscape. In the current highly dynamic geopolitical context, and in light of trade interdependence brought about by globalization, economic warfare as a class of subthreshold conflict is of particular concern to small, open economies such as Canada's (Ciuriak 2022; Mulder 2022).

In considering what constitutes economic warfare, it is possible to draw from more developed literature on cyber warfare. For example, a recently published NATO handbook on establishing international positions on cyber warfare (Mačák, Dias and Kasper 2025) can be readily adapted to economic warfare, whereas a series of policy briefs by Raquel Garbers (2025b, 2025c) provides a detailed discussion of economic warfare and proves useful in the Canadian context. In this latter work, economic warfare refers to the deliberate use of economic tools by one state to weaken, destabilize or coerce another without crossing the threshold that would trigger kinetic conflict. This tactic could be intended to reduce an opposing state's political and military power and capacity to respond to threats; hinder its ability to operate and compete in critical emerging technological spheres; compel it to change its policies; deny it access to critical resources; hinder its engagement in normal economic relations; or render it vulnerable

2 The Five Eyes is an intelligence network composed of Australia, Canada, New Zealand, the United Kingdom and the United States.

to other unilateral actions (Førland 1993; Oermann and Wolff 2022, chapter 5). Its tools can include trade embargoes, sanctions and tariffs (Ciuriak 2025); export, acquisition or exfiltration of IA/IP assets (Business Council of Canada 2023; Garbers 2025b); measures that restrict trade, investment or financial flows; or limitation of access to critical resources (Baskaran and Schwartz 2025).

Economic warfare must be carefully distinguished from economic statecraft, which shares many of the same tools and is ubiquitous in international relations, even between allies (Garbers 2025a). Economic warfare is distinguished from routine statecraft by three main criteria: it involves the use of non-routine tactics, including IP theft, extortion, bribery and currency manipulation; it is always embedded in a broader set of hostile acts, very often disinformation campaigns designed to sway public perception of the events in question; and, at its most extreme level, it weaponizes all aspects of society, seeking to take advantage of individuals, organizations and legal structures to achieve a broad set of subthreshold goals (Garbers 2025b, 2025c, 2025d).

The distinction between economic warfare and economic statecraft may not reflect the potential for harm. For example, the extent of the harm inflicted by the recently imposed tariffs and volatile economic policies of the United States is evidence of the potential consequences of economic dependence, and IP and data lost to allied nations are no less lost as drivers of domestic value creation. For the purposes of this work, whether any particular economic action or policy constitutes an act of economic warfare is of secondary importance to identifying that which must be done to mitigate its potential impact, given that the actions that Canada must take to address our economic security vulnerabilities are largely independent of this distinction.

What Is Economic Security?

Title 6 of US Code § 474 defines economic security as "the condition of having secure and resilient domestic production capacity, combined with reliable access to the global resources necessary to maintain an acceptable standard of living and to protect core national values."[3] Other authors draw from a Japanese literature review to distill the concept of "economic security" to "the protection of essential values, such as national survival, sovereign independence, and economic prosperity, from threats, including the disruption of critical commodity supplies, the outflow of advanced technologies, and overreliance on other countries" (Yuzue and Sekiyama 2025, 1), further suggesting that "regulatory measures should be limited to what is indispensable and reasonable for eliminating or deterring threats to national survival, sovereign independence, and economic prosperity" (ibid., 6).

Globalization and the fragmentation of supply chains, as well as the rise of transnational cloud computing (Qiu, Yu and Oreglia 2024; Zheng 2021), have created exploitable economic interdependencies. To mitigate these risks, nation-states are beginning to refocus on economic independence, with numerous authors pointing to a decline in tendencies toward further globalization (Butollo et al. 2024; Chen and Evers 2023; Gopinath et al. 2024; Paul 2023) and increased calls for domestic data storage, compute and cloud infrastructure (Kushwaha, Roguski and Watson 2020) in the name of sovereignty (Vatanparast 2021; Clement 2018). It is worth noting explicitly that this latter trend in the West is primarily driven by a pullback from dependence on American big tech, especially following recent revelations that American data laws trump those of any other sovereign nation when data is held by American companies (Senat Français 2025). The volatility of recent American trade policy has highlighted that the dangers of economic dependence are not limited to harms inflicted by historically adversarial states.

As part of a report in a CIGI series, Dan Ciuriak and Patricia Goff (2021) undertook an exploration of the topic of economic security that points to a tension

3 *Homeland Security Critical Domain Research and Development*, 6 USC § 474 (2021), tit 6.

between economic security and economic efficiency via globalization through which an externally dependent state can be economically influenced or subordinated. This subordination could manifest as "(a) limited ownership of valuable intangible assets (e.g., valuable data, intellectual property, and artificial intelligence assets) and (b) excessive specialization in less rewarding upstream functions (e.g., supply or production of raw materials and intermediate goods or services) in global value chains with foreign anchor firms" (Morgan 2024).

Of particular interest to this work is the exfiltration, denial or destruction of economic drivers such as IA/IP through both legal and illegal means[4] (Corneau-Tremblay 2022; Business Council of Canada 2023; Durand and Shull 2023; Zhao et al. 2020), as well as the offensive use of IP registration or defensive publications to limit access to critical emerging technologies (Gupta et al. 2025). The potential for harm inflicted through trade interdependence and IP loss is proportional to the degree to which IP can flow between economies, which is to say that even the approach taken to IA sharing with allies has the potential to be a strong driver for value loss through perfectly legitimate means. This is especially true of research and emerging technologies, since the adoption of emerging technology is being framed as a cornerstone of the Western response to grey-zone threats (Bellochio 2023; QinetiQ 2020; Ministry of Defence 2021; Business Council of Canada 2023; Garbers 2025b; Qasrawi et al. 2023; Araya and Mavinkurve 2022). Protecting IA/IP is of economic and national security interest.

Why Are IA/IP Assets So Important to Our Economic and National Security?

Articulation of the relationship between IP and national security is relatively new (Durand and Shull 2023; Halbert 2016). A recent report by the US Center for Strategic & International Studies argues that "decades of globalization have exposed critical vulnerabilities in the U.S. economy, as dependence on foreign competitors for essential goods and the offshoring of manufacturing have weakened industrial capacity, eroded economic resilience, and threatened national security" (Gupta et al. 2025, vi), and that a "strong and predictable system of IP rights" (ibid.) is a cornerstone of achieving national security by creating a stable foundation from which to enable innovation and technological leadership. In a similar vein, Ciuriak and Goff (2021, 1) highlights the "nexus of national security, economic security and economic prosperity," while a report by the Business Council of Canada (2023, 4) argues that "economic security is national security" and that "Canada should follow the path of many of its closest allies by integrating economic security considerations into a national security strategy" (ibid., 3), pointing to numerous cases of economic harm caused by incidents of IP theft and loss.

Building on these foundations, the authors provide a set of recommendations to assist businesses and policy makers to determine which technologies represent economic security concerns, on the one hand, and valuable opportunities for investment in Canadian economic security, on the other. The authors balance their recommendations against Canada's need to expand into foreign markets, attract choice FDI, and secure value and supply chains through security-conscious export. This approach must be supported by an ability to undertake frequent threat assessments to detect and identify emerging threats, scrutinize known risks and evaluate potential responses, particularly through strategic and tactical use of IA.

To achieve these objectives, we must first be able to determine whether an IP asset falls under a "matter of national concern" and/or "national security," which generally remains a subjective and

4 House of Commons, *The Security of Research Partnerships between Canadian Universities, Research Institutions and Entities Connected to the People's Republic of China*, Report of the Standing Committee on Science and Research (May 2024) (Chair: Lloyd Longfield) [*Security of Research Partnerships*], online: <www.ourcommons.ca/DocumentViewer/en/44-1/SRSR/report-10/>.

nebulous qualification in Canadian law. Common elements hinge on what is "injurious to Canada" under the Guidelines on the National Security Review of Investments[5] under the Investment Canada Act (ICA),[6] but Canada's last national security strategy was issued in 2004 (Privy Council Office 2004) and is badly in need of comprehensive review and modernization (Shull and Wark 2021).

These issues are further complexified by the challenge of ascribing value and importance to a given IA/IP asset early in its development, which the authors do not suggest is actionable. Rather, it is important to ensure that a strengths, weaknesses, opportunities and threats (SWOT) analysis has been performed at the level of emerging technology sectors, given the (necessarily) fluid concept of national security.

The authors also suggest that there is a pressing need to harmonize the various laws, frameworks, guidelines and directives under federal jurisdiction for any of them to be practically useful. This security-informed approach to IP should be one of the key inputs into decisions relating to which technologies Canada should prioritize in support of economic security and how to effectively and efficiently deliver this support considering the risks involved.

There are a few places from which inspiration can be drawn in support of starting this critical analysis. The teachings of the Supreme Court of Canada with respect to the national concern test are useful (Doblanko 2021). They require one to assess whether the issue:

- → is of "sufficient concern to Canada as a whole";
- → invites "a common-sense inquiry into the national importance of the proposed matter";
- → has a "singleness, distinctiveness and indivisibility that clearly distinguishes it from matters of provincial concern"; and
- → has a "scale of impact on provincial jurisdiction [that] is reconcilable with the fundamental distribution of legislative power under the Constitution" (ibid.).

Canada's vulnerable patchwork approach to conceptions of trade secret and national security legislation is set forth in Table 1. It is noteworthy that the definitions used in many of these concepts themselves contain undefined subordinate terms ("economic value," "Canada's economic interests" and so on) that leave the scope broad but vague, while others are quite narrow in scope (relating, for example, only to munitions).

It is also important to bear in mind the constitutional distribution of legislative powers (federal versus provincial competency) in relation to the second criteria above ("singleness, distinctiveness and indivisibility"). To effectively address the issues of national security raised in this paper, these powers would need to be centralized into a form of regularly updated technological inquiry conducted at the federal level. Inspiration can be drawn, for example, from the US Emerging Technology Technical Advisory Committee and Australia's List of Critical Technologies in the National Interest. Adapting these approaches to Canada, a dedicated committee (in addition to Canada's Sensitive Technology List[7]) could advise on matters involving the identification of emerging technologies and research and development (R&D) activities that may be of national and economic security interest and/or dual-use potential; the prioritization of new and existing controls to determine which are of greatest consequence to national security; the potential impact of dual-use export control requirements on research activities; and the threat to national security posed by the unauthorized export of technologies.

Even the concept of "dual use" lacks a unified definition as it relates to the identification of technologies of concern (Williams-Jones, Olivier and Smith 2014; Department of National Defence [DND] 2022). For the purposes of this paper, "dual use" refers to any technology that has the potential to be used for both civilian and military applications, irrespective of whether such a use case exists or is obvious at present. Where emerging technology is concerned, it is often the case that all applications or potential societal impacts of a new technology are not only not predictable when they are created

5 See https://ised-isde.canada.ca/site/investment-canada-act/en/investment-canada-act/guidelines/guidelines-national-security-review-investments

6 *Investment Canada Act*, RSC 1985, c 28 (1st Supp); EC, *Regulation (EU) 2021/821 of the European Parliament and of the Council of 20 May 2021 setting up a Union regime for the control of exports, brokering, technical assistance, transit and transfer of dual-use items*, [2021] OJ, L 206 [*Regulation (EU) 2021/821*].

7 See www.canada.ca/en/services/defence/nationalsecurity/sensitive-technology-list.html.

Table 1: Examples of Legislation that Address IP

Concept	Relevant Legislation	Operational Definition
Criminal Code of Canada: trade secret enforcement	Section 391 of the Criminal Code of Canada, RSC 1985, c C-46: → *Mens rea*: deceit or fraud. → *Actus rea*: "obtains a trade secret" or "communicates or makes available a trade secret." → Requires that the highest standard of proof "beyond a reasonable doubt" be met for conviction.	Section 391(1): "Everyone commits an offence who, by deceit, falsehood or other fraudulent means, knowingly obtains a *trade secret* or communicates or makes available a trade secret" (emphasis in original). Section 391(5): "For the purpose of this section, *trade secret* means any information that (a) is not generally known in the trade or business that uses or may use that information; (b) has economic value from not being generally known; and (c) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy" (emphasis in original).
Foreign interference and use of a trade secret for the benefit of a foreign economic entity	Section 19 of the Foreign Interference and Security of Information Act, RSC 1985, c O-5. Criteria: → Needs to be for the benefit of, or in association with, a foreign economic entity; → fraud *and* "without colour of right and to the detriment of Canada's economic interests, international relations or national defence or national security"; and → requires the communication of a trade secret to the foregoing, or the procurement, retention, alteration or destruction of a trade secret.	Section 19(1): "Every person commits an offence who, at the direction of, for the benefit of or in association with a foreign economic entity, fraudulently and without colour of right and *to the detriment of Canada's economic interests*, international relations or national defence or *national security* (a) communicates a trade secret to another person, group or organization; or (b) obtains, retains, alters or destroys a trade secret" (emphasis added by authors). Section 19(4): "For the purpose of this section, *trade secret* means any information, including a formula, pattern, compilation, program, method, technique, process, negotiation position or strategy or any information contained or embodied in a product, device or mechanism that (a) is or may be used in a trade or business; (b) is not generally known in that trade or business; (c) has economic value from not being generally known; and (d) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy" (emphasis in original).
Access to Information and Privacy requests	Sections 18.1, 18.2, 20(1), 27, 35(2) and 36.3 of the Access to Information Act, RSC 1985, c A-1 refer to the non-disclosure of trade secrets in the context of access to information requests.	Some guidance as to what constitutes trade secrets and the assessment thereof can be found in chapters 11.11 and 11.14 of the *Access to Information Manual* (Treasury Board of Canada Secretariat 1993), which further states that certain information such as research data may not be considered a trade secret and needs to be decided on a case-by-case basis.

Concept	Relevant Legislation	Operational Definition
Province of Quebec (civil law)	Article 1472 of the Civil Code of Québec, CQLR c CCQ-1991, states that "a person may free himself from his liability for injury caused to another as a result of the disclosure of a trade secret by proving that considerations of general interest prevailed over keeping the secret and, particularly, that its disclosure was justified for reasons of public health or safety." Article 1612 of the CCQ states that "the loss sustained by the owner of a trade secret includes the investment expenses incurred for its acquisition, perfection and use; the profit of which he is deprived may be compensated for through payment of royalties."	These are the only two references to trade secrets in the Civil Code of Québec. Some notable decisions include *Luxme International Ltd. v. Lasnier*, 2016 QCCS 6389, among others.
Common law jurisdiction	Recent 2024 cases include: → *Vaultose Digital Asset Services Inc. v. Kunz*, 2023 ONSC 5790 → *SHAC Solutions Inc. v. Guenther*, 2024 ABKB 145 → *FLS Transportation Services Limited v. TRAFFIX Group Inc.*, 2024 BCSC 1078	In Canada, there is no federal trade secrets act. Trade secret law is based on common law principles, enforced through claims including torts such as breaches of contract or confidence.
National security	National Security Act, 2017 (SC 2019, c 13)	No definition of "national security" from which to inform interpretation of the other legislative frameworks mentioned herein.
Investment regulations	The Investment Canada Act, RSC 1985, c 28 (1st Supp) and corresponding regulations and guidelines make reference to the concept of being "injurious to national security" and net benefit reviews.	No definition of national security is provided; however, information relating to the process of national security reviews can be found on related Innovation, Science and Economic Development Canada (ISED) webpages[8] (ISED 2021).
Munitions of war	Section 20 of the Patent Act, RSC 1985, c P-4	Provides specific guidance on government-owned patents related to "any invention in instruments or munitions of war."

Source: Authors.
Note: This table contains non-exhaustive sources of legislation that address IP (in particular, trade secrets) and IA of economic value in a national security context.

8 See https://ised-isde.canada.ca/site/investment-canada-act/en/what-investment-canada-act#s4.2.

but also potentially for many years thereafter, and that security concerns may arise only later in its development (Brenneis 2024; World Health Organization 2021; Krelina 2021). This is complexified by the strict and short deadlines imposed by the international IP regime (Durand 2025), which dictate that IP protections must usually be established from the start, often long before all possible uses of an emerging technology are clear. A thoughtful and deliberate approach to controlling the IA/IP assets arising from publicly funded research, even in cases where the security implications are not immediately apparent, provides enhanced optionality with respect to long-term security implications. But such a strategy requires a cohesive approach, executed early in the technology's life cycle. This makes effective management of the IA/IP associated with emerging technologies a prerequisite to managing downstream security implications. In this paper, the authors suggest practical means by which this complexity can be addressed through the identification of both offensive and defensive use of IA/IP (Barrett 2002; Boettiger and Chi-Ham 2007); highlight areas where Canadian legal frameworks fall short of providing the required tools; and make practical recommendations toward addressing the problem.

How Are IA/IP Assets Attacked?

The term "lawfare" was coined in reference to a set of exploitative but legal tactics of subthreshold warfare that overlaps significantly with economic warfare (Kittrie 2016). Front-door techniques include the use of legal mechanisms to acquire Canadian IA/IP assets, such as mergers and acquisitions (M&A), share or asset purchase agreements and more. Public-private partnerships are often vectors for this kind of activity, where contracts relating to research and collaboration[9] (including licensing agreements) can be used to legally gain control over IP assets under non-disclosure and confidentiality agreements. Defensive publication, or use of patent (He 2021) and non-patent (Brainard and Normile 2022; Qiu, Steinwender and Azoulay 2024; Dhand et al. 2024) literature to bar acquisition of IP protection, is on the rise. The tools of lawfare cut across different legal domains (for example, immigration and citizenship). This fragmentation enables "jurisdiction shopping," wherein a failed attempt to exfiltrate a key IA through one jurisdiction can be mitigated simply by trying a different jurisdictional attack vector. Of particular concern to Canada is the conflict inherent between principles of academic freedom, institutional autonomy, open science and access to research mandates on the one hand, and the security implications of emerging technologies on the other. The authors elaborate on this issue in detail in later sections, building on previous work (Briggs, Durand and Alhamad 2025; Durand and Briggs 2025) to suggest practical means to address the nexus between emerging technology, research security and academic freedom.

Destructors of IP are not limited to legal considerations. A recent alert by the Canadian Security Intelligence Service (CSIS) highlighted concerns of espionage in academic research (Bell 2025), and corporate and academic espionage has been well documented (Blackwell 2020; The Canadian Press 2024; Wark 2024), leading to high-profile cases of immigration challenges.[10] Filing of IP in violation of employment contracts and security clearances (Tunney 2024) is also a concern, given that the damage done may far exceed what is recoverable through contractual litigation and that no legal punishment can undo said damage. In addition, cyberattacks are on the rise, representing enormous costs to Canadian businesses (Cloutier and Ledoux 2025; Statistics Canada 2024a). The economic value of confidential information made public "need not have an inherent value, such as a client list might have, for example. The value of information ultimately 'depends upon the use that may be made of it, and its market value will depend upon the market place, who may want it and for what purposes, a value that may fluctuate widely over time"[11] (Michaelides et al. 2024; Thawe and Nador 2023). Given the complexity involved in estimating the value of IA, it is practically very difficult to quantify the extent of the harm, but as noted by Dan Ciuriak and Maria Ptashkina (2021, 1), "governments worldwide have been introducing new legislation

9 *Security of Research Partnerships*, *supra* note 4.

10 *Gao v Canada (Citizenship and Immigration)*, 2022 FC 64 (CanLII); *Zhang v Canada (Public Safety and Emergency Preparedness)*, 2023 CanLII 123767 (CA IRB).

11 *Merck Frosst Canada Ltd v Canada (Health)*, 2012 SCC 3 (CanLII).

to broaden and toughen the protection for trade secrets, citing estimates of the cost of trade secret theft in the order of one–three percent of the GDP of advanced countries or in the order of hundreds of billions of dollars annually." Certainly, this is a lower bound given that trade secret theft is just one of many ways that IA value can be lost.

Table 1 lists an overview of the numerous and disconnected ways in which various Canadian legal frameworks assess the intersection between trade secrets and national security, highlighting the extent of the challenge posed by policy fragmentation in just this one subclass of IA. Note that, in some cases, key concepts on which these frameworks depend, such as ideas of "Canada's economic interests," are not actually defined in the relevant legislation.

Canadian Economic Security

Research Security and Emerging Technology

Canada's research institutions produce a large quantity of high-quality research, but Canada has long struggled to translate research excellence into economic benefit. Several reports have highlighted the issues at play (ISED 2023a; Government of Canada 2011; Council of Canadian Academies 2025), pointing to various key contributors such as a failure to bridge research from academia to industry; the lack of a clear link between research and any identified market need; the fragmentation of and inconsistencies between institutional IP policies; and systemic risk intolerance. However, very little has changed despite actionable recommendations (Lowey 2024). This is particularly problematic considering the recent recognition by NATO that emerging technologies[12] represent key strategic assets in the form of technology with dual-use potential (Baldwin 2024; Brenneis 2024; World Health Organization 2021; Krelina 2021). If properly governed, Canada's world-class research infrastructure could be focused on national and economic security goals, technological sovereignty and international relationship building.

Security in research begins with the choice of participants. From 2018 to 2023, "academics at 10 of Canada's leading universities published more than 240 joint papers on topics including quantum cryptography, photonics and space science with Chinese military scientists" (Fife and Chase 2023). In light of this, concerns have been raised over Canada's public-private research partnership frameworks and private entities with connections to China[13] (Business Council of Canada 2023). In response, since 2023, ISED (2024) published a guide to securing quantum R&D, and universities have been required to check partners in research on topics deemed sensitive against the Named Research Organizations list (ISED 2023b) (a blacklist of organizations representing the highest threat to Canadian security). In the authors' view, blacklisting is the least secure option when seeking to exclude threats, given the ease with which new entities can be established as compared to the difficulty of properly vetting them. Onus is placed on universities themselves to conduct due diligence, a process that they are generally not equipped to undertake and for which the university in question may be conflicted by the monetary implications of finding a security issue, especially considering recent financial pressures (MacDonald 2024).

Management of IA/IP assets arising from publicly funded research has been a topic of significant debate. A 2023 report found that more than half of the IP arising from Canadian publicly funded research institutions left the country (Hinton, Witzel and Wajda 2023), with Senator Colin Deacon stating that "over the past 20 years, the number of Canadian-invented patents transferred to foreign firms has tripled from 18% to 56%....Half of our IP is commercialized outside of Canada."[14] These numbers are contentious among Canadian academic institutions and research funding agencies, with pushback and criticism mainly predicated on the definition of IP used in these studies, which is typically limited to registered IP assets and only takes into account ownership transfer. The National Crowdfunding & Fintech Association (2024) provides an overview of the debate as it pertains to artificial intelligence (AI) in particular.

The authors argue that the numbers are largely irrelevant and that the objections miss the point.

12 See www.nato.int/cps/en/natohq/topics_184303.htm.

13 *Security of Research Partnerships, supra* note 4.

14 *Senate Debates*, 44-1, vol 153, No 68 (6 October 2022) at 2078 (Hon George J. Furey).

The fact that there can be any debate at all about the extent of the problem is itself central to the problem, pointing to a systemic failure by every part of the innovation pipeline, including universities and funding bodies, to collect and make public actionable metrics on which to base policy decisions. Simplistic arguments based on the percentage of IA over which we lose control — without awareness of the nature and long-term impact of those assets — misses the fact that where emerging technology is concerned, a minority of IA accounts for a majority of the value. Even a one percent loss of control over IA/IP arising from publicly funded research is too much if it is the one percent with the highest security implications. Without data on long-term control over and access to IP assets, combined with a robust threat assessment framework for IA/IP, we are operating in the dark.

The Natural Sciences and Engineering Research Council of Canada (NSERC) Alliance Advantage[15] program is one of the primary means through which academic-industry-partnered research is funded in Canada. Under the NSERC Alliance Advantage program, $0.7 billion was spent funding partnered research among Canadian universities and both for-profit and not-for-profit partners between 2019 and 2024, inclusively. The tri-council, including NSERC, does not appear to take an active position on IP governance arising from funded research, leaving any related licensing deals to the host university. In practice, most of the IP arising during academic-industry partnerships is controlled by, or is at least accessible to, the private sector partner (Statistics Canada 2008). To be eligible for NSERC Alliance funding, a company must be registered in Canada, have staff with relevant expertise, conduct R&D and/or produce goods or supply services, and have "the financial, managerial, and technical capacity to exploit the results of the proposed research in Canada."[16] In short, while there are careful checks in place to ensure benefit to Canada, it is possible for Canadian subsidiaries of foreign firms to receive Alliance funding as industry research partners.

Using a variety of public data sources (see Appendix 2), the authors can demonstrate that for the NSERC Alliance Advantage program, 43 percent of the spending has gone into supporting research with at least one partner that is a subsidiary of a foreign firm, with 22 percent of funding going to projects for which all partners are such subsidiaries. When the authors limited their analysis to projects involving at least one for-profit partner as a proxy for the subset of projects that are expected to generate IP with commercial value (comprising $567 million in total spending), they found that 52 percent of funding was awarded to projects that had at least one partner that is a subsidiary of a foreign firm, and 33 percent to projects in which the only for-profit partners are Canadian subsidiaries of a foreign-controlled company.

The analysis above is not an argument for conducting less partnered research with subsidiaries of foreign firms, nor are the authors suggesting that all such cases of foreign access to Canadian IA/IP assets are problematic. Rather, if Canada is to continue to fund public-private research with foreign partners, the value of the outputs of such research as strategic assets must be acknowledged, with partners chosen deliberately as part of intelligence-sharing agreements and actionable data collected on access to, and control over, the resulting IA/IP assets over the long term. Some level of FDI in the context of research is likely desirable (Matthews and Rice 2022) and, if used as a deliberate part of an intelligence-sharing strategy with allies, could be a core element of Canada's contribution to NATO and the Five Eyes alliance. However, considering the value and importance of emerging technology[17] as an intelligence and security asset (Baldwin 2024), this does provide an argument for granting agencies taking an active position on use of and access to the IP arising from partnered research projects.

Data Sovereignty

Recent literature suggests that trade in digital products could reach about 15 percent of global trade by 2030 (Stojkoski et al. 2024, 5). Many authors have compared data to oil in terms of its importance as a resource in a world increasingly focused on AI (Farronato, forthcoming 2026; Szczepanski 2020). While the parallel is not perfect (Stach 2023), it is certainly true that data suitable for the training of AI models is a key IP asset, the value of which cannot be overstated, and data has generally long been recognized as being core to enterprise value (Ciuriak 2023). As such, access to, and (more importantly)

15 See www.nserc-crsng.gc.ca/NSERC-CRSNG/FundingDecisions-DecisionsFinancement/Alliance-Alliance/index_eng.asp.

16 See www.nserc-crsng.gc.ca/Innovate-Innover/alliance_society-alliance_societe/partners-partenaires_eng.asp.

17 See www.nato.int/cps/en/natohq/topics_184303.htm.

control over, data assets represent a key element of economic security (Irion 2012; Kushwaha, Roguski and Watson 2020) on which Canada is a laggard, and our data is largely captured and exfiltrated tax-free, duty-free and royalty-free (Department of Finance Canada 2025) by the big three American cloud providers (Amazon, Google and Microsoft) — a situation that some have referred to as a Canadian data sovereignty crisis (Kushwaha and Watson 2019). In recognition of the rapidly multiplying and increasingly valuable use cases for data of all kinds (Durand 2019; Knitl and Durand 2025; Sullivan, Brennan-Tonetta and Marxen 2017), countries around the world are actively developing frameworks to manage and control data beyond just personal data (Casalini, López-González and Nemoto 2021; Organisation for Economic Co-operation and Development [OECD] 2023a, 2023b; Davies and Fumega 2022; Struett, Aaronson and Zable 2024).

Data writ large is subject to a rapidly increasing number of cyberattacks (FortiGuard Labs 2025), unauthorized access and publication, and harmful misuse. Beyond the commonly considered harmful impacts of unlawful disclosure or use of personal data, data increasingly represents the moat that protects a company's competitive advantage, particularly where AI training data of any kind is concerned. In such cases, publication of key data, even beyond the personal data of customers, could remove the business's entire value in a matter of seconds, as this IA/IP could constitute all or most of a company's assets.

Being almost entirely reliant on foreign cloud service providers, Canada has very little control over its own data. Physical domestic storage requirements, as with trade secrets, are left to the provinces (Government of Canada 2020). This creates significant vulnerability to foreign influence (Aaronson 2025), and there is a growing call for data infrastructure as a key nation-building project in response (Slavens and Sanathkumar 2025; Clement 2018). The concept of data sharing and disclosure differs significantly among the intelligence, business, legal and academic communities. Depending on the group in question, different objectives apply, imposed by a wide variety of regulatory/legal frameworks and mandates that include the Patent Act, the CSIS Act[18] (CSIS 2024), security clearances, academic missions, grant-funding requirements and more, most of which were developed independently of one another. Associated regulation modernization with respect to storage and use of data beyond just personal data will be a key component of an effective response: regulations that must acknowledge the complexities of the various stakeholder groups in Canada, including Indigenous peoples (Connell 2025).

A lack of Canadian data sovereignty, near-complete dependence on foreign service providers for management of economically critical data and a severely outdated framework for data protection (Lloyd 2024) combine to represent a significant threat to economic security. Related modernization efforts are in progress in the form of the proposed Artificial Intelligence and Data Act (AIDA), but they have been heavily criticized as being too ambiguous to be practically useful (Brown 2024), and "many of these obligations are left to be fleshed out in regulations, including even the definition of the 'high impact' AI, to which the AIDA will apply" (Scassa 2023, 1).

Recommendations

There is no panacea for the challenges identified above, and the interconnected nature of the challenges obviates fragmented policy solutions. The nexus of IA/IP, economic and national security, and Canada's vulnerability to economic warfare requires a multi-faceted and cohesive approach that involves development of both offensive and defensive capabilities centred on our IP management regime. Below, the authors make five overarching suggestions for actions that Canada should undertake as the foundation for longer-term efforts to reduce economic dependence on both allies and adversaries.

Establish an AI-First OSINT Agency

Effective response to a set of rapidly evolving economic threats and issues of IP loss to both allies and exfiltration to adversarial states requires a proactive approach to related intelligence gathering and the ability to map global IP and emerging technology trends in real time. While Canada does not have a foreign intelligence agency, intelligence gathering in the present day need

18 *Countering Foreign Interference Act*, SC 2024, c 16, online: <https://laws-lois.justice.gc.ca/eng/AnnualStatutes/2024_16/>.

not necessarily be based on methods that have characterized statecraft since the Second World War.

Building on one of the recommendations of a report among the CIGI series on updating Canadian national security (Fyffe 2021), the authors propose the creation of an OSINT agency — one focused on separating the signal from the noise in open-source data to combat subthreshold threats, particularly in relation to the security-IP nexus. As evidenced by the example of analysis of NSERC Alliance Advantage funding, there is valuable intelligence to be gleaned from cross-referencing disparate open-source data, especially if public information can be augmented by private data held by the Canadian government (for example, by Statistics Canada, the Canada Revenue Agency or other agencies).

The primary focus would be to identify exploitable patterns and correlations in the emerging tech space, to proactively identify vulnerabilities in Canada's approach to emerging technologies and to provide recommendations for mitigation through allocation of a portion of Canada's world-class research infrastructure. This could be done, for example, by continuously reviewing public research funding announcements and patent disclosures (Zhao et al. 2020) as leading and lagging indicators, respectively, of emerging technological clusters. Through analysis of public information on global patent trends (Fraser 2010), it is, for example, possible to carve out strategic IP protections for technologies (or file improvements thereupon) that are deemed important for Canada's economic security. These insights would inform continuously updated IA/IP SWOT analyses with respect to an emerging technology focus globally, which could in turn provide a basis for "export controls on emerging dual-use technologies and protect strategic intellectual property so that technology developed for Allies is not easily available to rival states like Russia and China" (Baldwin 2024, 19).[19] It could further identify innovation "white spaces" (Eckelt et al. 2016) that represent opportunities for Canada's research machinery to contribute directly to national security. Such white spaces can be exploited both by directing research to fill the identified gaps and by finding opportunities for offensive IP registration or open-source publication at the margins of adversarial states' areas of focus (McFaul and Engelke 2025; Quinn and Omorogieva 2025). These capabilities dovetail well with both the recent calls (ISED 2025a) to focus more on demand-driven research (Edler 2019; ISED 2023; Dias et al. 2020) and the need to provide a clearer framework through which to identify national security concerns by providing a basis of data on which to make these decisions.

US-based software company Palantir provides a clear example as to the power of OSINT when cross-referenced with government data sources, but it obviously fails to align with Canadian values with respect to privacy and is ineligible as a related service provider given issues of data sovereignty.

To maximize its utility, this organization will need to be able to access privileged information from within Canadian government servers to cross-reference public data and will need to be able to act quickly to distill its findings into actionable security recommendations. Given the scope of accessible information, unlike the example of Palantir, this entity should not be a private sector service provider. If CIGI's previous recommendations are adopted, this agency could fall under the umbrella of the proposed Canadian National Security Council (Fyffe 2021). Alternatively, the requirements suggest that this agency could belong under the umbrella of the Privy Council Office as its organizational structure may allow for agile policy recommendations to go directly to the Prime Minister's Office on issues of national security concern. While Public Safety Canada, DND or CSIS are other possible homes for this agency, the authors note that historical challenges in making actionable public recommendations, given secrecy restrictions, may reduce potential impact without related reform that builds on recent policy changes intended to address this issue (CSIS 2024).

While such an intelligence agency would have been challenging to staff and run even a few short years ago (given the volume of information available from which to glean insight), the proliferation of AI could dramatically accelerate this data filtering, increasing the signal-to-noise ratio while leaving decision making in the hands of human analysts. With advancements in AI and non-relational databases, it is possible to extract and analyze rich economic (Taillard 2012, chapter 19) and IP-related information from public and private comprehensive data sets to perform predictive analytics to identify technological advancements and manage risk

19 *Regulation (EU) 2021/821, supra* note 4; see also www.international.gc.ca/controls-controles/military-militaires/handbook-manuel.aspx?lang=eng.

(Eckelt et al. 2016; Fang, Li and Lu 2025; Rauf et al. 2024; Jamarani et al. 2024; Li et al. 2024).

In particular, this agency should, as a first task, develop a nuanced threat assessment framework for IA/IP assets in the context of research partnerships with foreign partners, taking into account:

- the partner (ally, neutral or adversary);
- the type of research being conducted (curiosity-driven research versus research into emerging technology with dual-use potential and the immediacy and obviousness of that potential);
- the terms under which control over the resulting IP is vested among the participants (licensing terms or ownership); and
- the relative level of interest in the space from both allied and adversarial states.

Secure Canadian Research and Invest in Emerging Technology

Securing Canadian IP requires comprehensive and cohesive reform of all elements of the IP management process. Protection of IA/IP assets is insufficient to ensure benefit, as an IP asset is only valuable if developed and used. Given that transfer or licensing of publicly funded IP to Canadian-controlled companies remains a bottleneck predicated on a patchwork approach to IP policy among both academic and government research institutions, the authors and others recommend the adoption of express licensing frameworks (Durand and Briggs 2025; Briggs, Durand and Alhamad 2025; Council of Canadian Innovators 2025) by both Canadian universities and government labs. They also recommend the inclusion of dedicated resources for tech transfer and IP protection activities as part of research grants that are allowed within the above framework. In federal labs in particular, policies regarding technology transfer to the private sector make it challenging to license IP to start-ups. This is problematic given increasing recognition that start-ups are much more effective vehicles for disruptive innovation than established companies (Fraser 2010; [name redacted] 2012; Keller and Block 2013; Lanahan 2016; Park et al. 2024; Swamidass 2013; Valdivia 2013; Christensen 1997) in combination with a relative dearth of established Canadian anchor firms to act as IP receptors, which, in combination, are a loss driver of IP arising from Canadian publicly funded research.

Governance guidelines should be developed and imposed as conditions of funding by the Canadian tri-council and other agencies that provide public funds in support of research. In cases where partner organizations are not Canadian-controlled or are Canadian subsidiaries of foreign-controlled organizations, these guidelines should include provisions to ensure that a Canadian commercialization attempt remains possible, regardless of the country (or countries) controlling the partner organizations. Inspiration can be drawn from the Bayh-Dole framework, specifically the "manufactured substantially" provision (Stokkan Smith 2023). A set of metrics to track the long-term outcome of technology development efforts should be established (Office of the Auditor General of Ontario 2015, chapter 3, section 14) to monitor all entities that have access to, or control over, IP arising from publicly funded research, in particular mandating the reporting of licensing arrangements that are rarely made public presently. At a bare minimum, details of licensing arrangements between research participants and the universities participating in the research, if provided to the proposed OSINT agency, could be used to map the flow of control over, and access to, key IP assets.

In service of this goal, the authors have independently developed the Simple Agreement for Innovation Licensing (SAIL), which mandates the collection of metrics compatible with the above OSINT agency (Briggs, Durand and Alhamad 2025) and is compatible with all existing Canadian university IP policies. The authors recommend that Canadian federal and provincial research support-granting agencies take an active and cohesive position with respect to target outcomes for IP arising from publicly funded research rather than leaving it up to individual institutions. To achieve this goal, the authors present SAIL as a practical, community-built tool that does not require policy change at the institution level, though as noted above, policy change with respect to technology transfer to start-ups is necessary among federal research institutions.

While the NSERC Alliance Advantage program examined above is a small fraction of Canada's overall research budget, the failure of Canadian research granting agencies to enact IP governance policies is endemic (United States Trade Representative 2025; Loise and Stevens 2010; World Intellectual Property Organization 2024). Given the importance of the outputs

of Canada's research investments as strategic intelligence assets, even research in partnership with friendly countries should be explicitly part of a deliberate and cohesive intelligence-sharing framework rooted in sound IP policy.

The blacklisting approach (default allow, with a finite and easily circumvented list of disallowed entities) used by the Named Research Organizations list should be scrapped in favour of a whitelist (default disallow, with a finite list of allowed entities) of partner organizations vetted by an organization with the resources and qualifications to properly conduct threat assessments rather than individual universities (for example, the OSINT agency proposed above, supported by existing intelligence frameworks). A whitelist approach forces affirmative security clearance and requires data collection on research partners at the input end of the innovation pipeline, allowing the choice of research partners to align with economic security goals — goals that are not necessarily within the priorities or even capabilities of universities.

Not all IP should be protected through public registration. Where IP is of national security concern, and especially if one takes the position that Canada is at economic war (Garbers 2025b, 2025c), it is often more appropriate to retain IA/IP assets as trade secrets to avoid the need for registration-related public disclosure to secure more formal protection. Here, Canada lags behind other jurisdictions in how trade secrets are managed (Malone 2020, 2021a, 2021b, 2021c, 2023b). In matters of defence, there exist infrequently used mechanisms to file secret patent applications,[20] which enable "new inventions that might threaten national security and defence…[to be] hidden from public view under secret federal cabinet orders" (MacLeod 2014). Unlike the United States Patent and Trademark Office (2022, chapter 0100, section 120), which has detailed policies on secrecy orders, equivalents cannot be found in the Canadian *Manual of Patent Office Practice* (Canadian Intellectual Property Office 2019). A detailed discussion of this issue is beyond the scope of this paper, as addressing Canada's problematic approach to trade secrets is of greater importance.

Clearly, there exists a tension between academic freedom to publish and a security-focused approach to IP management. As previously noted, in jurisdictions with functional trade secrets legislation, it is often preferable to maintain IP with security implications as trade secrets rather than registering them as patents or other publication-based IA. While acknowledging the importance of academic freedom in a democratic society, registered IP assets are a requirement where academic outputs are concerned, which Canadian universities are woefully under-resourced to manage.

Weaving through all of these research-focused recommendations is the idea that Canada must recognize the value of its world-class research apparatus as a generator of defence assets and IA. With the recent push from Canadian industry groups and provincial governments to focus on demand-driven research, explicit attention should be given to demand from our allies (in service of repurposing some of Canada's research infrastructure toward directly addressing, first, our own domestic economic and national security concerns and, second, the needs of NATO [Blais-Savoie 2025] and Five Eyes), allowing some of Canada's renewed NATO spending commitments to support required reform. To be effective, process transparency is critical, as "governments need to be transparent about why particular restrictions are essential both to convince national actors and to reassure the international community that security arguments are not simply providing cover for protectionism" (Baldwin 2024, 12).

Supported by calls for the procurement and use of demand-side levers as tools of innovation policy (Council of Canadian Innovators 2025; ISED 2023), this renewed focus on defence represents a golden opportunity to invest in Canadian technology development, bolstering the domestic economy and promoting technological independence while directly strengthening our national security. Here, Canada's incumbent advantage in quantum-sensing technologies represents a key opportunity for IP-mediated value capture, enhancing economic prosperity and security and increasing our contribution to allied defence at the same time (ISED 2025b). Canadian research institutions are well positioned to contribute to Canadian defence, security and sovereignty, if (and only if) our research can first be secured at the source.

20 See *Patent Act*, RSC 1985, c P-4, s 20 and *NATO Agreement on Safeguarding Defence-Related Inventions*, 21 September 1960 (entered into force 12 January 1961).

Reform Foreign Investment Controls and Acquire Foreign Tech

While investment in Canadian research and emerging technology will go a long way toward incentivizing building and owning emerging technology in Canada by creating conditions that promote it, a "carrot"-based approach to incentivizing IP retention is not always sufficient. Canada's economic security regime centres on its FDI controls under the ICA, trade controls under various regimes and research security initiatives as discussed above. As noted in other contexts, this fragmented approach presents numerous vulnerabilities and modernization is still needed.

The subset of transactions and business combinations that are subject to ICA review should be expanded. Non-traditional investment approaches — including reverse mergers, loans with non-traditional terms and private contractual licensing arrangements — can all result in the effective granting of rights equivalent to those conferred through acquisition without triggering ICA review under existing rules. To achieve this, it will be necessary to harmonize the legislature with respect to what constitutes national security under a federal national interest test. ICA decisions can then be based on this test, supported by a proactive and case-by-case SWOT analysis conducted in close consultation with the new agency suggested above. Transactions involving assets that are flagged by this test should require pre-registration and preliminary review (even to enter negotiations) to minimize costs to the parties involved, should the transaction be blocked pre-emptively. Resources and IP education should be made available to administrators to support effective preliminary reviews and to avoid abuse.

In cases where a transaction is blocked, particularly in cases in which the object of concern is an IA/IP asset, the ICA has no provision for supporting companies or IP portfolios. While a blocked transaction may be a survivable event for an established company, a small company (for example, a start-up) whose value is based entirely on the asset in question may be considering acquisition as a matter of existential need. Without support following a blocked acquisition, a company is vulnerable to bankruptcy, and the IP (if it cannot be sold) may enter the public domain or lose any protection. In such cases, the harm that the ICA sought to avoid may instead be accelerated.

If ICA review results in a blocked transaction, the IP is considered to be valuable for purposes of national or economic security. It follows that it is in the public interest to take proactive steps to ensure that IP assets that underlie a decision to block a transaction under the ICA remain supported and in Canadian control. Funding should be available to offset the harmful impact of a blocked transaction under the ICA. To do otherwise, as is done currently, would be extremely prejudicial to the company. In extreme cases where a private sector solution is not possible, nationalization via a Crown corporation could be considered as a vehicle to advance the technology until such time as it can be securely privatized.

Finally, supported by the intelligence agency suggested above, Canada should also invest in proactively acquiring IP that is in its security interests. Canada has set aside billions of dollars through a wide range of fragmented innovation support programs (Deacon et al. 2024) that are clearly underperforming in aggregate. These programs should be reviewed for long-term impact and a portion of the underperforming capital repurposed both to match the investment of Canadian companies making strategic acquisitions of foreign tech with security importance and to support continued operations of companies whose exit is blocked on national security grounds as discussed above. While in the normal course of business, such subsidized M&A activity might be viewed as anti-competitive, national security concerns and the backdrop of economic warfare may provide considerable leeway.

Invest in Sovereign Cloud Storage and Compute, Including Quantum

Comprehensive overhaul and modernization of privacy law, including the Personal Information Protection and Electronic Documents Act, is critical. In doing so, it is important to recognize that it is not only personal data at stake — AI can be trained on an enormous variety of data (OECD 2025), including creative endeavours normally covered by copyright law and the outputs of Canadian research. These assets are presently governed by a patchwork of legislative frameworks — if they are governed at all — while increasingly representing potential

intelligence assets that can support emerging technology development (Cockburn, Henderson and Stern 2018; Laursen 2024; Pyzer-Knapp et al. 2022; Sarker 2022; Sullivan, Brennan-Tonetta and Marxen 2017) or being used as the basis for predictive analytics (Eckelt et al. 2016; Fang, Li and Lu 2025; Rauf et al. 2024; Jamarani et al. 2024; Li et al. 2024).

Securing Canadian data is not simply a matter of legislation, however, given that Canada lacks the domestic infrastructure to support sovereign data warehousing. Investments in domestic storage and cloud compute infrastructure are foundational to the practical implementation of any sovereign data regime. Most of the spending under Canada's AI plan should be focused on compute and data storage infrastructure, acknowledging that it is far too late for Canada to be relevant in the global AI race and instead focusing on securing domestic data assets in support of data sovereignty.

The push toward sovereign cloud and compute, Canadian emerging technology leadership, and the need for increased defence spending and to secure key IA/IP assets in the research phase all intersect in quantum computing. Consideration should be given to setting aside a portion of this budget to support the procurement of quantum computing hardware, serving the threefold purpose of providing Canada's world-leading quantum companies with a reason to stay Canadian in the face of pressure from the US Defense Advanced Research Projects Agency (2025), which could lead to the loss of large swathes of dual-use quantum IP in as little as 12 months (Briggs 2025); building the "quantum sandbox"[21] necessary to create the application layer that will make quantum computing practically useful; and directly supporting new defence-spending targets while actively building Canadian economic prosperity.

Harmonize Key Legal Frameworks Under Federal Jurisdiction

Common to all the recommendations made above is a need to centralize legislative power relating to key legal frameworks from the provinces to Parliament. Harmonization of IP governance frameworks under federal jurisdiction has plenty of international precedent, having been completed in 1980 in the United States, for example, with the Bayh-Dole Act (Loise and Stevens 2010). Precedent also exists where trade secrets are concerned, since Parliament already has legislative control of all IP-related laws (patents of invention and discovery, copyright, trademark, industrial designs and so on), except for trade secrets. It would most likely require the submission of a reference question to the Supreme Court of Canada to obtain an advisory opinion on whether trade secrets should fall under federal jurisdiction, especially considering Canada's legal obligations under several international trade agreements; the importance of data (in other words, sensitive and confidential information); the nature of the technology that Canada seeks to invest in, including defence; and emerging dual-use technologies, AI and quantum, among other technologies of national interest.

The division of legislative powers is not conducive to efficient and effective action where national security is concerned, and Canada's fragmented approach to IA/IP and data management leaves numerous vulnerabilities through which our most valuable assets are leaking. The national security concerns imposed by these issues provide federal regulators with considerable leeway in imposing harmonized frameworks to mitigate the threat. In particular, the authors suggest that a federally defined national interest test be created, supported by the OSINT agency suggested above, to serve as the basis of both updates to the International Compliance Association and research security decision making; that IP policy at research institutions be superseded by a unified national framework for research IP management where such IP falls under the umbrella of this national interest test; and that a framework for trade secret management and enforcement be developed that supersedes provincial frameworks in the same circumstances to ensure a unified approach to national and economic security as defined above.

Acknowledgements

The authors would like to thank Raquel Garbers, Robert Mazzolin, Lisa Lambert and Tara June Misra for their insights and comments in the writing of this paper; Gonzalo Lavin, engineer, for patent research in quantum sensing; as well as Aaron Shull, managing director and general counsel at CIGI, for the opportunity to write this paper.

21 House of Commons, *How Can Canada Remain a Leader in the Global Quantum Marathon?* (September 2022) (Chair: Joël Lightbound) at 33.

Appendix 1: What Are AI and IP, and How Are They Secured?

The International Financial Reporting Standards (IFRS) specifies a hierarchy of intangibles: most broadly, intellectual capital, a subset of which can be considered an IA, of which a further subset represents IP. In this work, the authors focus on IA and IP, wherein lie most of the economic value and vulnerability. According to the IFRS, "an intangible asset is an identifiable non-monetary asset without physical substance. Such an asset is identifiable when it is separable, or when it arises from contractual or other legal rights. Separable assets can be sold, transferred, licensed, etc."[22] IA are *valuable*, *transactable* and *vulnerable*.

IP, a subset of IA, refers to creations of the mind such as inventions (patents); literary and artistic works (copyright); designs; symbols, names and images used in commerce (trademarks); industrial designs; plant breeder rights; and trade secrets, confidential information and data, among other possibilities. In many cases, IP is protected in law, which enables people to earn recognition or profit from what they invent or create and prevents others from using it to achieve monetary gain. This could take the form of providing a right to exclude others from using an IP right (or asset) (for example, in the case of patents, copyright, trademarks, industrial designs and so forth) in cases of infringement. IP is further subdivided into registered and unregistered IP, depending on the details of the legal frameworks through which these assets are protected.

Like tangible property, IP is an economic right that is transactable and can be sold, licensed (Ciuriak 2017, 2020) or used as collateral (Desjardins and Hatzikiriakos 2024; World Intellectual Property Organization 2023) (though the authors note that Canada recently defunded the Business Development Bank of Canada's IP-backed financing fund — the bank's only source of such financing [McIntyre 2025]). However, current accounting standards do not capture IA/IP assets on company balance sheets or financial statements until they have been subjected to a business combination (for example, acquisition) and/or a purchase price allocation, thereby leaving a "systemic blind spot" (Durand 2024a, 2024b).[23] To complicate matters, transactions involving IP are typically motivated more by corporate interests than by national security interests, and rights granted through IP control can be transferred by numerous mechanisms, including informally, often occurring out of the public view through private contractual means.

IP is also vulnerable to attack, and considering that IP is only a legal right, it can be attacked in many ways. At the application and/or registration stage, savvy competitors can take advantage of legal mechanisms, such as protests, re-examinations and other procedures, to challenge the validity of patents (Government of Canada 2019; Wilkinson 2014) or other forms of IP. Once granted, IP protection has practical limits: legal considerations only protect against those who cooperate. For adversarial states, registered IP assets such as patents instead provide a public instruction manual. As such, careful consideration must be given to registering IA/IP assets versus maintaining control through secrecy (i.e., trade secrets) (Lenarczyk, Minssen and Aboy 2025). This tension is particularly problematic at the intersection of academic research and emerging technologies with dual-use potential, since secrecy is directly at odds with the principles of academic freedom and tenure (rooted in the 1915 declaration that bears the same name).

A final IA class worth addressing separately is data. To date, most data governance frameworks focus on personally identifying information, with the European General Data Protection Regulation leading the charge with respect to sovereign control over personal data (Aljeraisy et al. 2022; Office of the Privacy Commissioner of Canada 2020; Bakare et al. 2024). As AI systems continue to develop, the strategic and economic importance and value of data of all kinds are becoming clear (Institute of Innovation & Knowledge Exchange 2024; Ciuriak 2023), but related regulatory frameworks have not been able to keep up with the pace of change, and data is — out of necessity — typically managed as a trade secret.

IA that remain trade secrets avoid the need for public disclosure, but Canada lacks a unified federal trade secrets statute. Instead, unlike in the case of other IP classes that fall under federal law, trade

22 See www.ifrs.org/issued-standards/list-of-standards/ias-38-intangible-assets/.

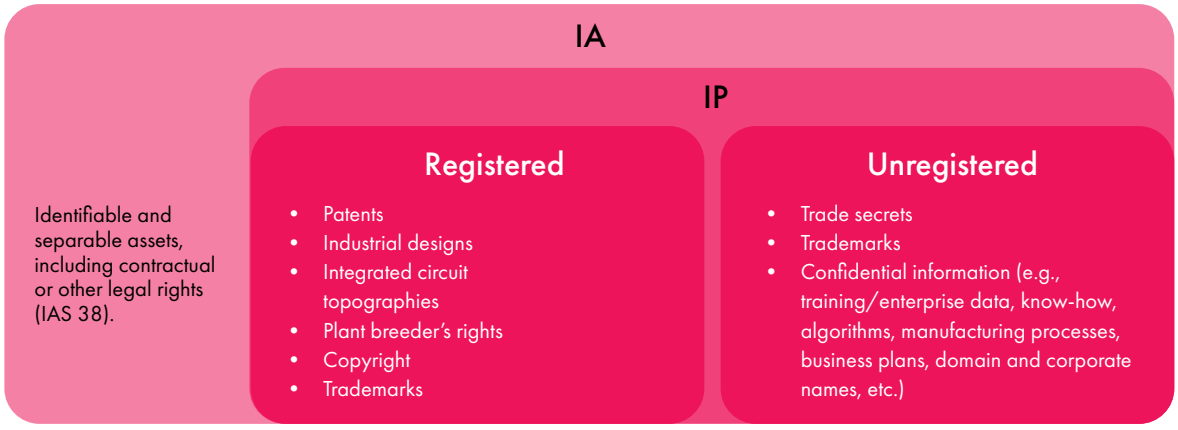
23 See www.wipo.int/en/web/ip-financing/w/news/2025/recap-value-of-intangible-assets.

secrets are covered by a patchwork of common law, civil law and criminal provisions that vary among provinces. As such, Canada's approach differs from the robust and unified trade secret legal frameworks that exist elsewhere (Raffetto and Friese 2022; Malone 2023b), which further limits options for effective IP control. Given Canada's constitutional distribution of legislative powers, trade secret law is contextually complex, with enforcement options under federal law (that is, criminal statute, requiring that the highest standard of proof — "beyond a reasonable doubt" — be met for a conviction), common law or civil law in Quebec, with lesser burdens of proof (that is, balance of probabilities). Canada's woefully fragmented trade secret laws have prompted calls for the establishment of a unified Canadian legal framework for trade secrets protection (Malone 2021a; Norton and Miller 2024). As noted by Matthew Malone (2023a, 2023b) in his parliamentary submission, "for years, the Canadian Security Intelligence Service has warned that theft of trade secrets and confidential information is a threat to our economic security, but we have had no prosecutions to show for it. The Wang prosecution is the first and only one." Work by CIGI provides a basis of evidence from US trade secret litigation that can serve as a rubric for an updated Canadian approach (Ciuriak and Ptashkina 2021). Figure 1 shows a Venn diagram illustrating the relationship between IA and IP and the various approaches used in their protection.

Appendix 2: NSERC Alliance Advantage Analysis Methodology

The analysis of NSERC data was carried out by cross-referencing grant decisions from the NSERC Alliance funding decisions webpage[24] from 2019 to 2024 (inclusive) against the country of control designated in the Statistics Canada (2024b) tables on intercorporate ownership where possible (that is, where the parent company of a research partner is publicly traded), and through searches of company websites, related news sources and other publicly available webpages in cases where they are not listed. The country of control of a company was designated as the country of control of its ultimate parent company in the aforementioned tables. If such information was not available, news sources were used to find details of any acquisitions or mergers, and the analysis was repeated to identify the ultimate parent of the acquirer. Failing that, the country of control was designated according to the location of the company's headquarters. In case of ambiguity or in the absence of any information to the contrary, partner organizations were assumed to be Canadian controlled. While errors in attribution are possible, they are more

Figure 1: Types of Intangible and IP Assets



Source: Authors.

Note: This diagram includes a non-exhaustive set of examples of different classes of each type of asset and the means (registered versus unregistered) through which they are protected.

24 See www.nserc-crsng.gc.ca/NSERC-CRSNG/FundingDecisions-DecisionsFinancement/Alliance-Alliance/index_eng.asp.

likely to mistakenly attribute a foreign-controlled company as Canadian than vice versa under this procedure. The authors note that this analysis is imperfect, for a number of reasons. The issue of ultimate beneficial ownership or significant control[25] (Vautour 2021) is not fully accounted for, which would require additional resources and data to assess.[26] Finally, the analysis does not account for the timing of any change of control as compared to the timing of the grant awarded, which is to say that a company that was Canadian controlled at the time a grant was provided, but subsequently changed status, would be designated as foreign controlled.

25 See https://fintrac-canafe.canada.ca/guidance-directives/client-clientele/bor-eng.

26 See https://ised-isde.canada.ca/site/corporations-canada/en/how-find-information-about-individuals-significant-control; https://ised-isde.canada.ca/site/atip-services/en/references/pia-corporations-canada-beneficial-ownership-transparency.

Works Cited

Aaronson, Susan Ariel. 2025. *A Difficult Balance: Privacy, National Security and the Free Flow of Data*. CIGI Paper No. 330. Waterloo, ON: CIGI. www.cigionline.org/publications/a-difficult-balance-privacy-national-security-and-the-free-flow-of-data/.

Aljeraisy, Atheer, Masoud Barati, Omer Rana and Charith Perera. 2022. "Exploring the Relationships between Privacy by Design Schemes and Privacy Laws: A Comparative Analysis." October 10. Preprint, arXiv. https://doi.org/10.48550/ARXIV.2210.03520.

Araya, Daniel and Mai Mavinkurve. 2022. *Emerging Technologies, Game Changers and the Impact on National Security*. Reimagining a Canadian National Security Strategy Report No. 9. Waterloo, ON: CIGI. www.cigionline.org/publications/emerging-technologies-game-changers-and-the-impact-on-national-security/.

Ashton, Lisa. 2025. *Food first: How agriculture can lead a new era for Canadian exports*. RBC Thought Leadership, February 25. Royal Bank of Canada. www.rbc.com/en/thought-leadership/the-trade-hub/food-first-how-agriculture-can-lead-a-new-era-for-canadian-exports/.

Azzi, Mounia, Gordon C. McCauley, Bethany Moir, Ana Monia Nunes and Sarah Williams. 2025. "Does Canada Own its Life Sciences Future?" White Paper. adMare Institute. www.admarebio.com/en/admare-institute.

Bakare, Seun Solomon, Adekunle Oyeyemi Adeniyi, Chidiogo Uzoamaka Akpuokwe and Nkechi Emmanuella Eneh. 2024. "Data Privacy Laws and Compliance: A Comparative Review of the EU GDPR and USA Regulations." *Computer Science & IT Research Journal* 5 (3): 528–43. https://doi.org/10.51594/csitrj.v5i3.859.

Baldwin, Harriett. 2024. *Critical Dual-Use Technologies: Commercial, Regulatory, Societal and National Security Challenges*. General Report 051 ESC 24 E rev.2 fin. NATO Parliamentary Assembly, Economics and Security Committee. www.nato-pa.int/document/2024-dual-use-technologies-report-baldwin-051-esc.

Barrett, Bill. 2002. "Defensive use of publications in an intellectual property strategy." *Nature Biotechnology* 20 (2): 191–93. https://doi.org/10.1038/nbt0202-191.

Baskaran, Gracelin and Meredith Schwartz. 2025. "The Consequences of China's New Rare Earths Export Restrictions." Center for Strategic & International Studies, April 14. www.csis.org/analysis/consequences-chinas-new-rare-earths-export-restrictions.

Bell, Stewart. 2025. "CSIS issues espionage alert about suspect seeking sensitive information for Chinese intelligence." Global News, July 5. https://globalnews.ca/news/11274203/csis-espionage-advisory-china/.

Bellochio, Andrew. 2023. "Maintenance Operating Periods in Multi-Domain Operations." In *Cutting through the Haze: Grey Zone Operations and Contemporary Threats*, edited by Christopher Maternowski and Aditi Malhotra, 43–50. The Canadian Army Journal and the NATO Association of Canada.

Blackwell, Tom. 2020. "Exclusive: Did Huawei bring down Nortel? Corporate espionage, theft, and the parallel rise and fall of two telecom giants." *National Post*, February 20. https://nationalpost.com/news/exclusive-did-huawei-bring-down-nortel-corporate-espionage-theft-and-the-parallel-rise-and-fall-of-two-telecom-giants.

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/.

Boettiger, Sara and Cecilia Chi-Ham. 2007. "Defensive Publishing and the Public Domain." In *Intellectual Property Management in Health and Agricultural Innovation: A Handbook of Best Practices*, vol. 2, edited by Anatole Krattiger, Richard T. Mahoney, Lita Nelsen, Jennifer A. Thomson, Alan B. Bennett, Kanikaram Satyanarayana, Gregory D. Graff et al., 879–96. Oxford, UK: Centre for the Management of Intellectual Property in Health Research and Development and Public Intellectual Property Resource for Agriculture.

Brainard, Jeffrey and Dennis Normile. 2022. "China rises to first place in most cited papers." *Science*, August 17. https://doi.org/10.1126/science.ade4585.

Brenneis, Andreas. 2024. "Assessing dual use risks in AI research: necessity, challenges and mitigation strategies." *Research Ethics* 21 (2): 302–30. https://doi.org/10.1177/17470161241267782.

Briggs, Kyle. 2025. "Now or Never: Interviews with Canadian Quantum Computing Leadership." *CanInnovate*, July 15. www.caninnovate.ca/p/now-or-never-interviews-with-canadian-quantum-leadership.

Briggs, Kyle, David Durand and Rami Alhamad. 2025. "Simple Agreement for Innovation Licensing (SAIL)." Version 3.0. May 5. www.howtosail.ca/.

Brown, Derek. 2024. "Canada's Proposed Artificial Intelligence and Data Act (AIDA): A Critical Review." *SSRN*, February 1. https://doi.org/10.2139/ssrn.4687995.

Business Council of Canada. 2023. *Economic Security is National Security: The Case for an Integrated Canadian Strategy*. Ottawa, ON: Business Council of Canada. www.thebusinesscouncil.ca/report/economic-security-is-national-security/.

Butollo, Florian, Cornelia Staritz, Felix Maile and Tobias Wuttke. 2024. "The End of Globalized Production? Supply-Chain Resilience, Technological Sovereignty, and Enduring Global Interdependencies in the Post-Pandemic Era." *Critical Sociology* 51 (4-5): 779–98. https://doi.org/10.1177/08969205241239872.

Canadian Intellectual Property Office. 2019. *Manual of Patent Office Practice (MOPOP)*. Otttawa, ON: Canadian Intellectual Property Office. https://s3.ca-central-1.amazonaws.com/manuels-manuals-opic-cipo/MOPOP_English.html.

Casalini, Francesca, Javier López-González and Taku Nemoto. 2021. "Mapping Commonalities in Regulatory Approaches to Cross-Border Data Transfers." OECD Trade Policy Paper No. 248. https://doi.org/10.1787/ca9f974e-en.

Chen, Ling S. and Miles M. Evers. 2023. "'Wars without Gun Smoke': Global Supply Chains, Power Transitions, and Economic Statecraft." *International Security* 48 (2): 164–204. https://doi.org/10.1162/isec_a_00473.

Christensen, Clayton M. 1997. *The Innovator's Dilemma: When New Technologies Cause Great Firms to Fail*. Boston, MA: Harvard Business School Press.

Ciuriak, Dan. 2017. *Intellectual Property Proliferation: Strategic Roots and Strategic Responses*. CIGI Paper No. 121. Waterloo, ON: CIGI. www.cigionline.org/publications/intellectual-property-proliferation-strategic-roots-and-strategic-responses/.

———. 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/.

———. 2022. "Geo-economics in a Multipolar World: Rules of Engagement for the Small, Open Economy." Calgary, AB: Canadian Global Affairs Institute. May. www.cgai.ca/geo_economics_in_a_multipolar_world_rules_of_engagement_for_the_small_open_economy.

———. 2023. *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/.

———. 2025. "A Faulty Case: Deconstructing Trump's Case for Trade War on Canada." SSRN, April 3 (last revised March 9). https://doi.org/10.2139/ssrn.5124350.

Ciuriak, Dan and Patricia Goff. 2021. *Economic Security and the Changing Global Economy*. Reimagining a Canadian National Security Strategy Report No. 8. Waterloo, ON: CIGI. www.cigionline.org/publications/economic-security-and-the-changing-global-economy/.

Ciuriak, Dan and Maria Ptashkina. 2021. *Quantifying Trade Secret Theft: Policy Implications*. CIGI Paper No. 253. Waterloo, ON: CIGI. www.cigionline.org/publications/quantifying-trade-secret-theft-policy-implications/.

Clement, Andrew. 2018. "Canadian Network Sovereignty: A Strategy for Twenty-First-Century National Infrastructure Building." In *Data Governance in the Digital Age*, 26–33. Waterloo, ON: CIGI. www.cigionline.org/publications/data-governance-digital-age/.

Cloutier, David and Isabelle Ledoux. 2025. "Cyberattacks: Too many risks to ignore." Business Development Bank of Canada, February 20. www.bdc.ca/en/articles-tools/blog/cyberattacks-small-businesses-remain-denial.

Cockburn, Iain M., Rebecca Henderson and Scott Stern. 2018. "The Impact of Artificial Intelligence on Innovation." NBER Working Paper 24449. Cambridge, MA: National Bureau of Economic Research. https://doi.org/10.3386/w24449.

Connell, Alyea Cyr. 2025. "Indigenous Data Sovereignty (DDN3-A11)." Government of Canada, January 8. www.csps-efpc.gc.ca/tools/articles/indigenous-data-sovereignty-eng.aspx.

Corneau-Tremblay, Guillaume. 2022. "Did a Russian spy operate out of two of Canada's universities?" *Policy Options*, December 6. https://policyoptions.irpp.org/magazines/december-2022/russian-spy-canadian-universities/.

Costigan, Sean S. and Michael A. Hennessy. 2024. *Hybrid Threats and Hybrid Warfare: Reference Curriculum*. June. Brussels, Belgium: NATO Headquarters.

Council of Canadian Academies. 2025. *The State of Science, Technology, and Innovation in Canada 2025*. Ottawa, ON: Expert Panel on the State of Science, Technology, and Innovation in Canada. https://doi. org/10.60870/0zkv-5q08.

Council of Canadian Innovators. 2025. *A Mandate To Innovate*. May. Toronto, ON: Council of Canadian Innovators. www.canadianinnovators.org/content/a-mandate-to-innovate.

CSIS. 2024. "Amendments to *CSIS Act* Disclosure Authorities." September 27. www.canada.ca/en/security-intelligence-service/corporate/publications/amendments-to-csis-act/amendments-to-csis-act-disclosure-authorities.html.

Davies, Tim and Silvana Fumega. 2022. *Global Data Barometer – First Edition*. Zenodo. https://doi.org/10.5281/ZENODO.6488349.

Deacon, Colin, Ryan Laberge, Benedicta Arthur and David Dlab. 2024. "Federal Programs for Business Innovation." Discussion Paper. Office of the Honourable Senator Colin Deacon. October. www.colindeacon.ca/federal-innovation-programs.

Defense Advanced Research Projects Agency. 2025. "DARPA eyes companies targeting industrially useful quantum computers." April 3. www.darpa.mil/news/2025/companies-targeting-quantum-computers.

Department of Finance Canada. 2025. "Canada rescinds digital services tax to advance broader trade negotiations with the United States." June 29. www.canada.ca/en/department-finance/news/2025/06/canada-rescinds-digital-services-tax-to-advance-broader-trade-negotiations-with-the-united-states.html.

Desjardins, Lisa and Kiriakoula Hatzikiriakos. 2024. "Episode 34: How to use IP for financing." January 3, in *Canadian IP Voices*, produced by Canadian Intellectual Property Office, podcast, 43:45. https://ised-isde.canada.ca/site/canadian-intellectual-property-office/en/episode-34-how-use-ip-financing.

Dhand, Ritu, Amy Lin, Aman Ganpatsingh and Mithu Lucraft. 2024. *Global Research Pulse: China*. Springer Nature. https://stories.springernature.com/global-research-pulse-china/.

Dias, Ana Gama, Mauricio Horn, Eunice Mercado-Lara, Momanyi Mokaya and Francois Provencher. 2020. *Improving Demand-Driven Innovation Policies in Canada*. Policy Lab Report. July 8. Max Bell School of Public Policy, McGill University. www.mcgill.ca/maxbellschool/article/articles/policy-lab-2020-improving-demand-driven-innovation-policies-canada.

DND. 2022. "DAOD 3003-2, Management, Security and Access Requirements Relating to Dual-Use Goods." September 28 (last modified December 14, 2023). www.canada.ca/en/department-national-defence/corporate/policies-standards/defence-administrative-orders-directives/3000-series/3003/3003-2-management-security-and-access-requirements-relating-to-dual-use-goods.html.

Doblanko, Tesia. 2021. "Yes, the Federal Government Can Put a Price on Greenhouse Gas Emissions – Part 2." Centre for Constitutional Studies. July 11. www.constitutionalstudies.ca/2021/07/yes-the-federal-government-can-put-a-price-on-greenhouse-gas-emissions-part-2.

Dubinsky, Zach and Elizabeth Thompson. 2023. "Who's behind Canada's new pulp-and-paper powerhouse, and where's the money coming from?" CBC News, March 9. www.cbc.ca/news/business/paper-excellence-pulp-china-1.6772654.

Durand, David. 2019. "Consultation on transfers for processing data — Reframed discussion document." Letter to Office of the Privacy Commissioner of Canada, August 6. www.durand-lex.com/_files/ugd/214ca8_4dbc909cc79042c0ad861d01cc1cb14c.pdf.

———. 2024a. "Benefits of reporting intellectual property on balance sheets and financial statements." MVIP, February 7. www.mvip.solutions/post/benefits-of-reporting-intellectual-property-on-balance-sheets-and-financial-statements.

———. 2024b. "Measuring the impact of IA/IP on GDP and/or economic growth: Can it be truly calculated?" MVIP, October 18. www.mvip.solutions/post/measuring-the-impact-of-ip-on-gdp-and-or-economic-growth-can-it-be-truly-calculated.

———. 2025. "30-Month Window to Maximize Your Value." MVIP, May 21. www.mvip.solutions/post/30-month-window-to-maximize-your-value.

Durand, David and Kyle Briggs. 2025. "Rocking the SAILboat: A Novel Approach to Technology Transfer Informed by A Comparative Analysis of Express Licences." SSRN, February 24. https://dx.doi.org/10.2139/ssrn.5115205.

Durand, David and Aaron Shull. 2023. "With an unruly China, safeguarding intellectual property is vital to national security." *The Globe and Mail*, March 6. www.theglobeandmail.com/business/commentary/article-china-foreign-interference-national-security/.

Eckelt, Daniel, Christian Dülme, Jürgen Gausemeier and Simon Hemel. 2016. "Detecting White Spots in Innovation-Driven Intellectual Property Management." *Technology Innovation Management Review* 6 (7): 34–47. https://doi.org/10.22215/timreview/1003.

Edler, Jakob. 2019. "A Costly Gap: The Neglect of the Demand Side in Canadian Innovation Policy." IRPP Insight No. 28. May. Montreal, QC: Institute for Research in Public Policy. https://irpp.org/wp-content/uploads/2019/05/A-Costly-Gap-The-Neglect-of-the-Demand-Side-in-Canadian-Innovation-Policy.pdf.

Edler, Jakob, Knut Blind, Henning Kroll and Torben Schubert. 2023. "Technology sovereignty as an emerging frame for innovation policy. Defining rationales, ends and means." *Research Policy* 52 (6): 104765. https://doi.org/10.1016/j.respol.2023.104765.

Eggen, Karen-Anna. 2024. "Designing around NATO's deterrence: Russia's Nordic information confrontation strategy." *Journal of Strategic Studies* 47 (3): 410–34. https://doi.org/10.1080/01402390.2024.2332328.

Fang, Hanming, Ming Li and Guangli Lu. 2025. "Decoding China's Industrial Policies." NBER Working Paper 33814. Cambridge, MA: National Bureau of Economic Research. https://doi.org/10.3386/w33814.

Farronato, Chiara. Forthcoming 2026. "Data As the New Oil: Parallels, Challenges, and Regulatory Implications." In *The Political Economy of Artificial Intelligence*, edited by Ajay Agrawal, Joshua Gans, Avi Goldfarb and Catherine E. Tucker. Chicago, IL: University of Chicago Press.

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/.

Førland, Tor Egil. 1993. "The History of Economic Warfare: International Law, Effectiveness, Strategies." *Journal of Peace Research* 30 (2): 151–62. https://doi.org/10.1177/0022343393030002003.

FortiGuard Labs. 2025. *2025 Fortinet Global Threat Landscape Report*. A Report by FortiGuard Labs. Fortinet. May 1. www.fortinet.com/content/dam/fortinet/assets/threat-reports/threat-landscape-report-2025.pdf.

Fraser, John. 2010. "Academic Technology Transfer: Tracking, Measuring and Enhancing its Impact." *Industry and Higher Education* 24 (5): 311–17. https://doi.org/10.5367/ihe.2010.0001.

Fyffe, Greg. 2021. *Prepared: Canadian Intelligence for the Dangerous Decades*. Reimagining a Canadian National Security Strategy Report No. 6. Waterloo, ON: CIGI. www.cigionline.org/publications/prepared-canadian-intelligence-for-the-dangerous-decades/.

Garbers, Raquel. 2025a. "Canada at Economic War — Economic Statecraft Is Not Economic War." Directed and produced by Henry Daeman, Centre for International Governance Innovation, July 29. Video, 5:08. www.cigionline.org/multimedia/canada-at-economic-war-economic-statecraft-is-not-economic-war/.

———. 2025b. *Canada at Economic War: Being Outplayed by Beijing*. Policy Brief No. 204. Waterloo, ON: CIGI. www.cigionline.org/static/documents/no.204_Garbers.pdf.

———. 2025c. *Canada at Economic War: Setting the Scene*. Policy Brief No. 194. Waterloo, ON: CIGI. www.cigionline.org/publications/canada-at-economic-war-setting-the-scene/.

———. 2025d. "Chatham House Rule Meeting on the Subject of Economic Warfare." US Embassy, Ottawa, ON, July 11.

Gizewski, Peter and Nancy Teeple. 2023. "Close Engagement in the Gray Zone: Challenges and Opportunities." In *Cutting through the Haze: Gray Zone Operations and Contemporary Threats*, edited by Christopher Maternowski and Aditi Malhotra, 9–19. The Canadian Army Journal and the NATO Association of Canada.

Gopinath, Gita, Pierre-Olivier Gourinchas, Andrea F. Presbitero and Petia Topalova. 2024. "Changing Global Linkages: A New Cold War?" IMF Working Paper WP/24/76. https://doi.org/10.5089/9798400272745.001.

Government of Canada. 2011. *Innovation Canada: A Call to Action*. Review of Federal Support to Research and Development — Expert Panel Report. Ottawa, ON: Public Works and Government Services Canada. https://publications.gc.ca/collections/collection_2011/ic/Iu4-149-1-2011-eng.pdf.

———. 2019. *Manual of Patent Office Practice*. October. Ottawa, ON: Government of Canada. https://manuels-manuals.opic-cipo.gc.ca/w/ic/MOPOP-en.

———. 2020. "Government of Canada White Paper: Data Sovereignty and Public Cloud." Last modified October 31, 2025. www.canada.ca/en/government/system/digital-government/digital-government-innovations/cloud-services/digital-sovereignty/gc-white-paper-data-sovereignty-public-cloud.html.

Gupta, Kirti, Andrei Iancu, Walter G. Copan and Chris Borges. 2025. *Protecting Intellectual Property for National Security: A Transition Report for the New Administration*. A Report of CSIS LeadershIP and Renewing American Innovation. Center for Strategic & International Studies. www.csis.org/analysis/protecting-intellectual-property-national-security-transition-report.

Hakala, Janne and Jazlyn Melnychuk. 2021. *Russia's Strategy in Cyberspace*. Riga, Latvia: NATO Strategic Communications Centre of Excellence. https://stratcomcoe.org/publications/russias-strategy-in-cyberspace/210.

Halbert, Debora. 2016. "Intellectual property theft and national security: Agendas and assumptions." *The Information Society* 32 (4): 256–68. https://doi.org/10.1080/01972243.2016.1177762.

He, Alex. 2021. "What Do China's High Patent Numbers Really Mean?" Opinion, Centre for International Governance Innovation, April 20. www.cigionline.org/articles/what-do-chinas-high-patent-numbers-really-mean/.

Hinton, James W., Mardi Witzel and Joanna Wajda. 2023. *An Economic Mirage: How Canadian Universities Impact Freedom to Operate*. CIGI Paper No. 274. Waterloo, ON: CIGI. www.cigionline.org/publications/an-economic-mirage-how-canadian-universities-impact-freedom-to-operate/.

Hogue, Marie-Josée. 2025. *Public Inquiry into Foreign Interference in Federal Electoral Processes and Democratic Institutions*. Final Report. January 28. Ottawa, ON: Foreign Interference Commission.

Institute of Innovation & Knowledge Exchange. 2024. "Data as NATO New Strategic Asset." News release, November 5. https://ikeinstitute.org/news/2024/november/data_as_nato_new_strategic_asset.

Irion, Kristina. 2012. "Government Cloud Computing and National Data Sovereignty." *Policy & Internet* 4 (3–4): 40–71. https://doi.org/10.1002/poi3.10.

ISED. 2021. "Guidelines on the National Security Review of Investments." March 24. https://ised-isde.canada.ca/site/investment-canada-act/en/investment-canada-act/guidelines/guidelines-national-security-review-investments.

———. 2023a. *Report of the Advisory Panel on the Federal Research Support System*. Ottawa, ON: ISED. https://ised-isde.canada.ca/site/panel-federal-research-support/en/report-advisory-panel-federal-research-support-system.

———. 2023b. *Named Research Organizations*. Ottawa, ON: Government of Canada. https://science.gc.ca/site/science/en/safeguarding-your-research/guidelines-and-tools-implement-research-security/sensitive-technology-research-and-affiliations-concern/named-research-organizations.

———. 2024. "Securing Canadian Quantum Research and Development." September. Ottawa, ON: ISED. https://ised-isde.canada.ca/site/national-quantum-strategy/en/securing-canadian-quantum-research-and-development.

———. 2025a. "Advanced technologies for open-source intelligence due diligence." Last modified August 15. https://ised-isde.canada.ca/site/innovative-solutions-canada/en/advanced-technologies-open-source-intelligence-due-diligence.

———. 2025b. "National Quantum Strategy Roadmap: Quantum Sensing." February 17. Ottawa, ON: ISED. https://ised-isde.canada.ca/site/national-quantum-strategy/en/national-quantum-strategy-roadmap-quantum-sensing.

Jamarani, Amirhossein, Saeid Haddadi, Raheleh Sarvizadeh, Mostafa Haghi Kashani, Mohammad Akbari and Saeed Moradi. 2024. "Big data and predictive analytics: A systematic review of applications." *Artificial Intelligence Review* 57 (7): 176. https://doi.org/10.1007/s10462-024-10811-5.

Keller, Matthew R. and Fred Block. 2013. "Explaining the transformation in the US innovation system: the impact of a small government program." *Socio-Economic Review* 11 (4): 629–56. https://doi.org/10.1093/ser/mws021.

Kittrie, Orde F. 2016. *Lawfare: Law as a Weapon of War*. Oxford, UK: Oxford University Press.

Knitl, Walter and David Durand. 2025. "The AIoT Opportunity for Canada — when Artificial Intelligence and the Internet of Things meet." White Paper. AIoT Canada. www.aiotcanada.ca/whitepaper.

Krelina, Michal. 2021. "Quantum technology for military applications." *EPJ Quantum Technology* 8, 23: 1–53. https://doi.org/10.1140/epjqt/s40507-021-00113-y.

Kushwaha, Neal, Przemyslaw Roguski and Bruce W. Watson. 2020. "Up in the Air: Ensuring Government Data Sovereignty in the Cloud." *12th International Conference on Cyber Conflict (CyCon)*, 43–61. https://ieeexplore.ieee.org/document/9131718.

Kushwaha, Neal and Bruce W. Watson. 2019. "Crown in the clouds: a Canadian data sovereignty crisis." Conference Paper Presented at the 15th International Conference on Cyber Warfare and Security. https://doi.org/10.34190/ICCWS.20.132.

Lanahan, Lauren. 2016. "Multilevel public funding for small business innovation: a review of US state SBIR match programs." *The Journal of Technology Transfer* 41 (2): 220–49. https://doi.org/10.1007/s10961-015-9407-x.

Laursen, Lucas. 2024. "This AI-Powered Invention Machine Automates Eureka Moments." *IEEE Spectrum*, October 8. https://spectrum.ieee.org/ai-inventions.

Lenarczyk, Gabriela, Timo Minssen and Mateo Aboy. 2025. "IP in Superposition: Patents, Trade Secrets and Open Innovation in Quantum Information Technology." Preprint, Elsevier BV. https://doi.org/10.2139/ssrn.5363171.

Li, Zhenhui, Fan Zhou, Zhiyuan Wang, Xovee Xu, Leyuan Liu and Guangqiang Yin. 2024. "Measuring and classifying IP usage scenarios: a continuous neural trees approach." *Scientific Reports* 14 (1): 5144. https://doi.org/10.1038/s41598-024-55750-x.

Lloyd, Ron. 2024. "Canada's Security Classification Framework: The Biggest Impediment to Realizing Our Digital Ambition." CGAI: Canadian Global Affairs Institute, June 1. https://coilink.org/20.500.12592/b8gtr07.

Loise, Vicki and Ashley J. Stevens. 2010. "The Bayh-Dole Act Turns 30." *Science Translational Medicine* 2 (52). https://doi.org/10.1126/scitranslmed.3001481.

Lorinc, Jacob and Brian Platt. 2024. "China to keep investing in Canadian mining despite crackdown, envoy says." *Financial Post*, March 14. https://financialpost.com/commodities/mining/china-invest-canadian-mining-despite-crackdown-envoy.

Lowey, Mark. 2024. "Government must stop IP supported by public funding from flowing to other countries and not benefitting canada." Re$earch Money, December 11. https://researchmoneyinc.com/article/government-must-stop-ip-supported-by-public-funding-from-flowing-to-other-countries-and-not-benefitting-canada.

Mačák, Kubo, Talita Dias and Ágnes Kasper. 2025. *Handbook on Developing a National Position on International Law and Cyber Activities: A Practical Guide for States*. University of Exeter and NATO Cooperative Cyber Defence Centre of Excellence. https://ccdcoe.org/uploads/2025/05/Handbook-on-Developing-a-National-Position-on-International-Law-and-Cyber-Activities_A-Practical-Guide-for-States.pdf.

MacDonald, Moira. 2024. "International student fallout hits the bottom line." *University Affairs*, December 16. https://universityaffairs.ca/news/international-student-fallout-hits-the-bottom-line/.

MacLeod, Ian. 2014. "Secrecy cloaks patents on inventions hidden far from public eye by Industry Canada." *Ottawa Citizen*, January 8. https://ottawacitizen.com/news/secrecy-cloaks-patents-on-inventions-hidden-far-from-public-eye-by-industry-canada.

Malone, Matt. 2020. "Criminal Enforcement of Trade Secret Theft: Strategic Considerations for Canadian SMEs." *Technology Innovation Management Review* 10 (11): 40–46. https://doi.org/10.22215/timreview/1402.

———. 2021a. "Canadian businesses need a trade secrets act." *Toronto Star*, September 26. www.thestar.com/business/canadian-businesses-need-a-trade-secrets-act/article_846d84df-09e9-5430-8062-b7455a450286.html.

———. 2021b. "Consequences of the Criminalization of Trade Secret Theft in Canada." *UBC Law Review* 54 (3). https://commons.allard.ubc.ca/ubclawreview/vol54/iss3/7.

———. 2021c. "Why We Need a Canada Trade Secrets Act." Slaw, November 26. www.slaw.ca/2021/11/26/why-we-need-a-canada-trade-secrets-act/.

———. 2023a. "Re: Study re Support for the Commercialization of Intellectual Property." Letter from Matthew Malone to Members of the Standing Committee on Science and Research, April 6. www.ourcommons.ca/Content/Committee/441/SRSR/Brief/BR12334784/br-external/MaloneMatt-e.pdf.

———. 2023b. *The Law of Trade Secrets and Confidential Information in Canada*. Toronto, ON: LexisNexis Canada.

Matthews, Mairead and Faun Rice. 2022. *Context Matters: Strengthening the Impact of Foreign Investment on Domestic Innovation*. March. Ottawa, ON: Information and Communications Technology Council. https://ictc-ctic.ca/reports/context-matters.

McFaul, Cole and Peter Engelke. 2025. *Navigating the US-PRC tech competition in the Global South*. April 16. Washington, DC: Atlantic Council. www.atlanticcouncil.org/in-depth-research-reports/report/navigating-the-us-prc-tech-competition-in-the-global-south/.

McGee, Niall. 2023. "Canada wants to be a global leader in critical minerals. Why is Australia eating our lunch?" *The Globe and Mail*, October 13. www.theglobeandmail.com/business/article-canada-critical-minerals-mining-australia/.

McIntyre, Catherine. 2025. "BDC cuts intellectual property fund and slashes deep-tech team." The Logic, April 3. https://thelogic.co/news/exclusive/bdc-funds-closed-cuts-venture-capital.

Michaelides, Alexander, Andreas Milidonis, Vitaliy Ryabinin and Yupana Wiwattanakantang. 2024. "The Value of Trade Secrets: Evidence from Economic Espionage." Preprint, Elsevier BV. https://doi.org/10.2139/ssrn.4866808.

Ministry of Defence. 2021. *Defence in a competitive age*. March. London, UK: Ministry of Defence. www.gov.uk/government/publications/defence-in-a-competitive-age.

Morgan, Horatio M. 2024. "An Integrative Institutional Framework of the Canada-US Business Performance Gap." *Canadian Public Policy* 50 (2): 171–201. https://doi.org/10.3138/cpp.2023-023.

Mulder, Nicholas. 2022. *The Economic Weapon: The Rise of Sanctions as a Tool of Modern War*. New Haven, CT: Yale University Press.

[name redacted]. 2012. *The Bayh-Dole Act: Selected Issues in Patent Policy and the Commercialization of Technology*. Congressional Research Service, March 16.

National Crowdfunding & Fintech Association. 2024. "A Look Inside Canada's AI Commercialization Challenge." June 27. https://ncfacanada.org/a-look-inside-canadas-ai-commercialization-challenge/.

NATO. 2022. *NATO Standard AJP-01: Allied Joint Doctrine*. Edition F, Version 1. NATO Standardization Office. December. www.coemed.org/files/stanags/01_AJP/AJP-01_EDF_V1_E_(1)_2437.pdf.

———. 2023. *NATO Standard AJP-10: Allied Joint Doctrine for Strategic Communications*. Edition A, Version 1. NATO Standardization Office. March. https://assets.publishing.service.gov.uk/media/6525459d244f8e00138e7343/AJP_10_Strat_Comm_Change_1_web.pdf.

Nelson, John. 2022. "Developing a NATO Intermediate Force Capabilities Concept." *Connections: The Quarterly Journal* 21 (2): 67–84. https://doi.org/10.11610/Connections.21.2.05.

Norton, Matthew and Emily Miller. 2024. "Protecting trade secrets and confidential business information in Canada." Smart & Biggar, September 11. www.smartbiggar.ca/insights/publication/protecting-trade-secrets-and-confidential-business-information-in-canada.

OECD. 2023a. "AI Language Models: Technological, Socio-economic and Policy Considerations." OECD Digital Economy Paper No. 352. Paris, France: OECD Publishing. https://doi.org/10.1787/13d38f92-en.

———. 2023b. "Moving Forward on Data Free Flow with Trust: New Evidence and Analysis of Business Experiences." OECD Digital Economy Paper No. 353. Paris, France: OECD Publishing. https://doi.org/10.1787/1afab147-en.

———. 2025. "Intellectual Property Issues in Artificial Intelligence Trained on Scraped Data." OECD Artificial Intelligence Paper No. 33. Paris, France: OECD Publishing. https://doi.org/10.1787/d5241a23-en.

Oermann, Nils Ole and Hans-Jürgen Wolff. 2022. *Trade Wars: Past and Present*. Oxford, UK: Oxford University Press. https://doi.org/10.1093/oso/9780192848901.003.0005.

Office of the Auditor General of Ontario. 2015. *Annual Report 2015*. Toronto, ON: Office of the Auditor General of Ontario. www.auditor.on.ca/en/content/annualreports/arbyyear/ar2015.html.

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/#heading-0-0-1.

Park, Andrew, Elicia Maine, Riccardo Fini, Einar Rasmussen, Alberto Di Minin, Lawrence Dooley, Letizia Mortara et al. 2024. "Science-based innovation via university spin-offs: the influence of intangible assets." *R&D Management* 54 (1): 178–98. https://doi.org/10.1111/radm.12646.

Paul, T. V. 2023. "The Specter of Deglobalization." *Current History* 122 (840): 3–8. https://doi.org/10.1525/curh.2023.122.840.3.

Policy Exchange. 2020. "Future Defence: The Integrated Operating Concept." September 30. YouTube video, 25:05. www.youtube.com/watch?v=SRJU7b1VcC4&t=3s.

Privy Council Office. 2004. *Securing an Open Society: Canada's National Security Policy*. April. Ottawa, ON: Privy Council Office. https://publications.gc.ca/collections/Collection/CP22-77-2004E.pdf.

Pyzer-Knapp, Edward O., Jed W. Pitera, Peter W. J. Staar, Seiji Takeda, Teodoro Laino, Daniel P. Sanders, James Sexton et al. 2022. "Accelerating materials discovery using artificial intelligence, high performance computing and robotics." *npj Computational Materials* 8, 84. https://doi.org/10.1038/s41524-022-00765-z.

Qasrawi, Yazan, Peter Gizewski, Abdeslem Boukhouta, Peter Dobias and Michael A. Rostek. 2023. "Army Sustainment in the Gray Zone: Emergent Technologies as Double-Edged Sword Challenges and Opportunities." In *Cutting through the Haze: Gray Zone Operations and Contemporary Threats*, edited by Christopher Maternowski and Aditi Malhotra, 20–31. The Canadian Army Journal and the NATO Association of Canada.

Qiao, Liang and Xiangsui Wang. 2015. *Unrestricted Warfare: China's Master Plan to Destroy America.* Brattleboro, VT: Echo Point Books & Media.

QinetiQ. 2020. *Confidence in Chaos: How to Use Emerging Technologies to Combat Grey Zone Threats.* Lorton, VA: QinetiQ. www.qinetiq.com/en-us/insights/confidence-in-chaos-2.

Qiu, Jack Linchuan, Peter K. Yu and Elisa Oreglia, eds. 2024. *The Geopolitics of Chinese Internets.* 1st ed. Oxford, UK: Routledge.

Qiu, Shumin, Claudia Steinwender and Pierre Azoulay. 2024. "Paper Tiger? Chinese Science and Home Bias in Citations." NBER Working Paper 32468. Cambridge, MA: National Bureau of Economic Research. https://doi.org/10.3386/w32468.

Quinn, Kelsey and Eric Omorogieva, eds. 2025. *Future-Proofing U.S. Technology: Strategic Priorities Amid Chinese Tech Advancement.* April. Washington, DC: New Lines Institute for Strategy and Policy. https://newlinesinstitute.org/wp-content/uploads/20250307-Future-Proofing-US-Tech-Compendium__-.pdf.

Raffetto, Joe and Anna-Katharina Friese. 2022. "Trade Secret Global Guide." Hogan Lovells. www.hoganlovells.com/-/media/hogan-lovells/pdf/2022-pdfs/2022_10_10_global-trade-secrets-guide.pdf.

Rauf, Md Abdur, Md Majadul Islam Jim, Md Mahfuzur Rahman and Md Tariquzzaman. 2024. "AI-Powered Predictive Analytics for Intellectual Property Risk Management in Supply Chain Operations: A Big Data Approach." *International Journal of Science and Engineering* 1 (4): 32–46. https://doi.org/10.62304/ijse.v1i04.184.

Sarker, Iqbal H. 2022. "AI-Based Modeling: Techniques, Applications and Research Issues Towards Automation, Intelligent and Smart Systems." *SN Computer Science* 3, 158. https://doi.org/10.1007/s42979-022-01043-x.

Scassa, Teresa. 2023. "Regulating AI in Canada: A Critical Look at the Proposed *Artificial Intelligence and Data Act*." *The Canadian Bar Review* 101 (1).

Segal, Hugh and Ann Fitz-Gerald. 2021. *Emerging Security Challenges for Canada in the Coming Decade.* Reimagining a Canadian National Security Strategy Report No. 3. Waterloo, ON: CIGI. www.cigionline.org/publications/emerging-security-challenges-for-canada-in-the-coming-decade/.

Senat Français. 2025. *Audition de MM. Anton Carniaux, directeur des affaires publiques et juridiques, et Pierre Lagarde, directeur technique du secteur public, de Microsoft France.* www.senat.fr/compte-rendu-commissions/20250609/ce_commande_publique.html.

Serrato, Ray and Jake Wallis. 2020. "Covid-19 and the reach of pro-Kremlin messaging." Covid-19 disinformation and social media manipulation. October. Australian Strategic Policy Institute. www.aspi.org.au/report/covid-19-disinformation/.

Shull, Aaron and Wesley Wark. 2021. *Reimagining a Canadian National Security Strategy.* Special Report. Waterloo, ON: CIGI. www.cigionline.org/publications/reimagining-a-canadian-national-security-strategy/.

Slavens, Steven and Sairam Sanathkumar. 2025. "Digital infrastructure and data sovereignty as national priority projects." Torys, April 17. www.torys.com/en/our-latest-thinking/publications/2025/04/digital-infrastructure-and-data-sovereignty-as-national-priority-projects.

Stach, Christoph. 2023. "Data Is the New Oil — Sort of: A View on Why This Comparison Is Misleading and Its Implications for Modern Data Administration." *Future Internet* 15 (2): 71. https://doi.org/10.3390/fi15020071.

Statistics Canada. 2008. "Survey of Intellectual Property Commercialization in the Higher Education Sector." Catalogue No. 88-222–X. Ottawa, ON: Statistics Canada, Science, Innovation and Electronic Information Division, November. www150.statcan.gc.ca/n1/en/pub/88-222-x/88-222-x2008000-eng.pdf.

———. 2024a. "Impact of cybercrime on Canadian businesses, 2023." *The Daily*, October 21. www150.statcan.gc.ca/n1/daily-quotidien/241021/dq241021a-eng.htm.

———. 2024b. "Inter-corporate Ownership, 2023." June 17. www150.statcan.gc.ca/n1/pub/61-517-x/61-517-x2023001-eng.htm.

Stojkoski, Viktor, Philipp Koch, Eva Coll and César A. Hidalgo. 2024. "Estimating digital product trade through corporate revenue data." *Nature Communications* 15 (1): 5262. https://doi.org/10.1038/s41467-024-49141-z.

Stokkan Smith, Sunniva Jane. 2023. "Public money, public goods? The Bayh Dole Act and its 'manufactured substantially' provision." Master's thesis, University of Bergen. https://hdl.handle.net/11250/3081868.

Strick, Ben. 2020. "Attempted influence in disguise: the Iranian influence operation disguised as British journalists, activists and hobby fanatics posting about Covid-19, US politics and Black Lives Matter." Covid-19 disinformation and social media manipulation. December. Australian Strategic Policy Institute. www.aspi.org.au/report/covid-19-disinformation/.

Struett, Thomas, Susan Ariel Aaronson and Adam Zable. 2024. "Data Governance Mapping Project Year 4." Washington, DC: Digital Trade and Data Governance Hub. https://globaldatagovernancemapping.org/.

Sullivan, Kevin P., Peggy Brennan-Tonetta and Lucas J. Marxen. 2017. "Economic Impacts of the Research Collaboratory for Structural Bioinformatics (RCSB) Protein Data Bank." RCSB Protein Data Bank, May 1. https://doi.org/10.2210/rcsb_pdb/pdb-econ-imp-2017.

Swamidass, Paul M. 2013. "University startups as a commercialization alternative: lessons from three contrasting case studies." *The Journal of Technology Transfer* 38 (6): 788–808. https://doi.org/10.1007/s10961-012-9267-6.

Szczepanski, Marcin. 2020. "Is data the new oil? Competition issues in the digital economy." European Parliamentary Research Service Briefing PE 646.117. January. www.europarl.europa.eu/RegData/etudes/BRIE/2020/646117/EPRS_BRI(2020)646117_EN.pdf.

Taillard, Michael. 2012. *Economics and Modern Warfare: The Invisible Fist of the Market*. New York, NY: Palgrave Macmillan. https://doi.org/10.1057/9781137282255_21.

Thawe, Natalia and Anita Nador. 2023. "Confidential information, know-how and trade secrets: The importance of definition in valuation." Gowling WLG, September 12. https://gowlingwlg.com/en/insights-resources/articles/2023/distinction-confidential-information-know-how.

The Canadian Press. 2024. "New charges for alleged Chinese spy who worked for Hydro-Québec." Global News, February 7. https://globalnews.ca/news/10278941/charges-alleged-chinese-spy-hydro-quebec/.

Thomas, Elise. 2020. "Possible inauthentic activity promoting the *Epoch Times* and Truth Media targets Australians on Facebook." Covid-19 disinformation and social media manipulation. September. Australian Strategic Policy Institute. www.aspi.org.au/report/covid-19-disinformation/.

Thomas, Elise, Albert Zhang and Emilia Currey. 2020. "Pro-Russian vaccine politics drives new disinformation narratives." Covid-19 disinformation and social media manipulation. August. Australian Strategic Policy Institute. www.aspi.org.au/report/covid-19-disinformation/.

Treasury Board of Canada Secretariat. 1993. *Access to Information Manual*. Ottawa, ON: Treasury Board of Canada Secretariat. www.canada.ca/en/treasury-board-secretariat/services/access-information-privacy/access-information/access-information-manual.html#cha11_14.

Tunney, Catharine. 2024. "Lies and scandal: How two rogue scientists at a high-security lab triggered a national security calamity." CBC News, March 2. www.cbc.ca/news/politics/winnipeg-lab-firing-documents-released-china-1.7130284.

United States Patent and Trademark Office. 2022. *Manual of Patent Examining Procedure*. Washington, DC: United States Patent and Trademark Office. www.uspto.gov/web/offices/pac/mpep/s120.html.

United States Trade Representative. 2025. *2025 Special 301 Report*. Washington, DC: Office of the United States Trade Representative. https://ustr.gov/sites/default/files/files/Issue_Areas/Enforcement/2025%20Special%20301%20Report%20(final).pdf.

Valdivia, Walter D. 2013. "University Start-Ups: Critical for Improving Technology Transfer." Center for Technology Innovation at Brookings. November. www.brookings.edu/articles/university-start-ups-critical-for-improving-technology-transfer/.

Vatanparast, Roxana. 2021. "Data Governance and the Elasticity of Sovereignty." *Brooklyn Journal of International Law* 46 (1). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3839847.

Vautour, André. 2021. "New corporate transparency requirements in Canada, Québec and the U.S. – What Canadian and Québec companies need to know." Lavery, February 21. www.lavery.ca/en/publications/our-publications/5360-new-corporate-transparency-requirements-in-canada-quebec-and-the-u-s-what-canadian-and-quebec-companies-need-to-know.html.

Waldman, Suzanne. 2023. "Narrative as a Force Multiplier in the Information Battlefield." In *Cutting through the Haze: Gray Zone Operations and Contemporary Threats*, edited by Christopoher Maternowski and Aditi Malhotra, 32–42. The Canadian Army Journal and the NATO Association of Canada.

Wark, Wesley. 2024. "Security breaches at the NML: internal and public paths to truth-telling." *Wesley Wark's National Security and Intelligence Newsletter*, March 6. https://wesleywark.substack.com/p/security-breaches-at-the-nml-internal.

Wilkinson, Anna. 2014. "Improper Selection: A Separate Ground of Patent Invalidity in Canada?" *Osgoode Hall Review of Law and Policy* 3 (1): 19–58. https://digitalcommons.osgoode.yorku.ca/ohrlp/vol3/iss1/2/.

Williams-Jones, Bryn, Catherine Olivier and Elise Smith. 2014. "Governing 'dual-use' research in Canada: A policy review." *Science and Public Policy* 41 (1): 76–93. https://doi.org/10.1093/scipol/sct038.

Wong Leung, Jennifer, Stephan Robin and Danielle Cave. 2024. *ASPI's two-decade Critical Technology Tracker: The rewards of long-term research investment*. Barton, Australia: Australian Strategic Policy Institute. August. www.aspi.org.au/report/aspis-two-decade-critical-technology-tracker/.

World Health Organization. 2021. *Emerging technologies and dual-use concerns: a horizon scan for global public health*. Geneva, Switzerland: World Health Organization. www.who.int/publications/i/item/9789240036161.

World Intellectual Property Organization. 2023. Unlocking IP-backed Financing: Country Perspectives. Report Series. Geneva, Switzerland: World Intellectual Property Organization. www.wipo.int/publications/en/series/index.jsp?id=241.

———. 2024. *Models of Intellectual Property Governance and Administration*. Geneva, Switzerland: World Intellectual Property Organization. https://doi.org/10.34667/TIND.49741.

World Nuclear Association. 2025. "Uranium in Canada." https://world-nuclear.org/information-library/country-profiles/countries-a-f/canada-uranium.

Yuzue, Natsuya and Takashi Sekiyama. 2025. "Defining economic security through literature review." *Frontiers in Political Science 7* (April): 1501986. https://doi.org/10.3389/fpos.2025.1501986.

Zhao, Rongxiang, Yu Uny Cao, Xianrong Zheng and Hu Wang. 2020. "The innovation economy calls for proactive growth of intellectual property by various innovation carriers — A China case." *Global Transitions Proceedings* 1 (1): 23–31. https://doi.org/10.1016/j.gltp.2020.04.001.

Zheng, Guan. 2021. "Trilemma and tripartition: The regulatory paradigms of cross-border personal data transfer in the EU, the U.S. and China." *Computer Law & Security Review* 43 (November): 105610. https://doi.org/10.1016/j.clsr.2021.105610.

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