Business Council of Canada

ECONOMIC SECURITY IS NATIONAL SECURITY

The Case for an Integrated Canadian Strategy

Report

Table of Contents

99 Bank, Suite / bureau 1001, Ottawa, Canada K1P 6B9

Key Takeaways

1. Canadian companies are in the crosshairs of state-sponsored actors seeking to advance their interests in ways that undermine Canada's national and economic security.

2. Successive governments have been slow to respond to a new geopolitical reality that poses an unprecedented national security threat to the economic well-being of all Canadians.

3. Canada should follow the path of many of its closest allies by integrating economic security considerations into a national security strategy that helps identify and mitigate strategic threats.

4. An integrated Canadian security strategy should strengthen economic security architecture, bolster innovative capabilities, and expand international security partnerships.

99 Bank, Suite / bureau 1001, Ottawa, Canada K1P 6B9 THEBUSINESSCOUNCIL.CA

Canada requires an integrated national security strategy

Canada's national security is dependent on the economic vitality and resiliency of our nation. It is only through our enduring economic prosperity where we find the talent, resources, and innovation necessary to achieve our national ambitions, protect the lives and livelihoods of Canadians, and play a positive and influential role on the world stage.

The converse is also true. Absent a strong national security environment, it is impossible to have a healthy and productive economy.

Many of Canada's closest allies recognize this "mutually reinforcing link"[1], and have developed integrated approaches to economic and national security that seek to enhance their prosperity, safety, and sovereignty in a period of heightened geopolitical risk.

Canada has not. For decades now, successive Canadian governments have overlooked, taken for granted, or simply ignored the principle that *economic security is national security*.

This neglect has made us vulnerable. In an era of renewed geopolitical rivalry, where countries' ability to foster economic growth is the foundation upon which military, economic, and cultural power now rests, Canadian companies of all sizes are increasingly finding themselves in the crosshairs of strategic threat actors[2] seeking to advance their national interests in ways that can, and do, undermine Canada's national and economic security.

These threats have the potential to wreak large-scale havoc on Canadians' daily lives. The impacts include mass layoffs caused by the theft of intellectual property, disruptions to Canadians' ability to heat and power their homes due to paralyzing cyberattacks, and skyrocketing cost of everyday household products because of weaponized supply chains.

Defending Canada's economic security is too important an undertaking to be left to either the public or private sectors working alone. Both must work together seamlessly to detect, deter, and disrupt a broad range of emerging and evolving threats.

That is why this report calls on the Government of Canada to work with Canadian businesses to develop and implement a national security strategy that, for the first time, establishes economic security as a central pillar.

Based on in-depth consultations with the leaders of Canada's most innovative and successful companies, security experts, and former government officials, this report examines the threats facing Canadians, explores the consequences of inaction, and recommends measures to address the most glaring gaps in Canada's economic security posture.

[1] See Government of Australia, "Strong and Secure: A Strategy for Australia's National Security", 2013, page 4, link: https://www.files.ethz.ch/isn/167267/Australia%20A%20Strategy%20for%20National%20Securit.pdf

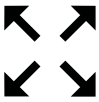
[2] This paper collectively refers to state-sponsored actors whose activities pose economic and national security threats to Canada as "strategic threat actors."

99 Bank, Suite / bureau 1001, Ottawa, Canada K1P 6B9 THEBUSINESSCOUNCIL.CA

The paper's recommendations are organized around three themes:

Strengthening Canada's economic security architecture, including by creating a legal framework allowing the Canadian Security Intelligence Service to proactively share timely and actionable threat intelligence with companies targeted by attacks;

Bolstering Canada's economic and innovative capabilities, including by incentivizing high-risk, high-reward research in disruptive and emerging fields which are foundational to spurring economic growth and are strategic from a national security perspective; and



Expanding and reinvigorating Canada's international security partnerships, including by spearheading measures to collectively counter weaponized supply chains, such as a "NATO for trade."

In a world where security is a prerequisite for prosperity, and prosperity a prerequisite for security, Canada will be unable to sustain a healthy and prosperous society without a national security strategy that safeguards our economic security. Now is the time for Canadian policymakers to recognize this reality and to come together with Canadian companies to protect the economic vitality and resiliency of our nation.

99 Bank, Suite / bureau 1001, Ottawa, Canada K1P 6B9 THEBUSINESSCOUNCIL.CA

Strategic threat actors are advancing their national interests at our expense

Canada now finds itself in the midst of the greatest, most complex, and unpredictable security environment in a generation.

The free, open, and relatively stable unipolar order that prevailed following the conclusion of the Cold War – and which provided Canada with unprecedented levels of safety, security, and prosperity – is giving way to a new, more turbulent, multipolar reality marked by geopolitical rivalry.[3]

The splintering of the global commons into rival camps struggling for strategic superiority has sharpened competition and confrontation among states in wide-ranging areas. This is no truer than in the fields of business, economics, and technology.

As in past eras defined by heightened geopolitical competition,[4] countries' ability to foster economic growth – especially through the invention, diffusion, and adoption of emerging and disruptive technologies – is the foundation upon which military, economic, and cultural power now rest.[5]

Recognizing this reality, strategic threat actors have shown both a capacity and willingness to steal, sabotage, and disrupt their way up the economic ladder to strengthen their geopolitical might and to unilaterally reshape the existing international order into something more favourable to themselves.[6]

[3] See Task Force on National Security, "A National Security Strategy for the 2020s," Graduate School of Public and International Affairs, University of Ottawa, May 2020, pages 4-5, link: https://socialsciences.uottawa.ca/public-international-affairs/sites/socialsciences.uottawa.ca.public-international-affairs/files/natsec_report_gspia_may2022.pdf; Aaron Shull and Wesley Wark, "Reimagining a Canadian National Security Strategy," Centre for International Governance Innovation, December 6 2021, pages 11-12 link: https://www.cigionline.org/publications/reimagining-a-canadian-national-security-strategy/.

[4] The greatest periods of technological innovation have often coincided with intense geopolitical rivalry. The foundations of the computing and telecommunications revolution, to give the most recent example of security-driven innovation, had its roots in Cold War competition.

[5] Economic power bolsters a country's capacity to wage war. It gives states leverage over global supply chains. It buys a country's soft power through the export of their values. In short, a country's ability to project power on the international stage now largely depends on its ability to compete in advanced industries where competition is at its fiercest. See Task Force on National Security, "A National Security Strategy for the 2020s," Graduate School of Public and International Affairs, University of Ottawa, May 2020, page 9, link: https://socialsciences.uottawa.ca/public-international-affairs/sites/socialsciences.uottawa.ca.public-international-affairs/files/natsec_report_gspia_may2022.pdf; Aaron Shull and Wesley Wark, "Reimagining a Canadian National Security Strategy," Centre for International Governance Innovation, December 6 2021, pages 14-18 link: https://www.cigionline.org/publications/reimagining-a-canadian-national-security-strategy/.

[6] See Privy Council Office, "Speech by the National Security and Intelligence Advisor to the Prime Minister to the Centre for International Governance Innovation", Government of Canada, June 8 2021, link: https://www.canada.ca/en/privy-council/services/national-security-intelligence-advisor-challenges.html; Intelligence and Security Committee of Parliament, "China", Parliament of the United Kingdom, July 13 2023, paragraphs 9 and 49, link: https://isc.independent.gov.uk/wp-content/uploads/2023/07/ISC-China.pdf.

99 Bank, Suite / bureau 1001, Ottawa, Canada K1P 6B9 THEBUSINESSCOUNCIL.CA

New technological advances, especially in cyberspace, have enabled these actors to both broaden and tailor their tactics to better penetrate our defences and achieve their revisionist aims.

The result: Canadian companies, in almost every region and sector of our economy, now face unprecedented dangers. They are operating on an increasingly skewed playing field in which traditional private commerce is always at a disadvantage.

Canada's lacklustre economic performance is adding to this threat.[7] Canada underperforms its global rivals in a range of areas essential to spurring innovation, scaling companies, and capturing global market share in advanced industries vital to our prosperity and security.[8] Indeed, Canada leads in none of the forty-four advanced technology categories – such as artificial intelligence, quantum, or advanced cybersecurity – identified by one think tank as being essential to a country's economic and national security.[9]

[7] Canada is predicted to have the worst performing economy amongst industrialized nations between 2020 and 2030. See Organization for Economic Co-operation and Development, "The Long Game: Fiscal Outlooks to 2060 Underline Need for Structural Reform", October 19 2021, page 13, link: https://www.oecd-ilibrary.org/docserver/a112307e-en.pdf?expires=1687548464&id=id&accname=guest&checksum=D17CE43CD7BF119FB92D4E3A68B5A310.

[8] This includes corporate expenditure on research and development, intellectual property commercialization, and talent retention. Canada ranked 22nd out of 44 nations tracked by the Organisation for Economic Co-operation and Development in domestic expenditure on research and development as a proportion of gross domestic product in 2020. See Organisation for Economic Co-operation and Development, "OECD Main Science and Technology Indicators Highlights", March 2022, page 2, link: https://www.oecd.org/sti/msti-highlights-march-2022.pdf. Canada ranked 17th in World Intellectual Property Organization's Global Innovation Index 2020. Canada's innovation input rank (9th) exceeded its innovation output rank (22nd) substantially. See Canadian Intellectual Property Office, "IP Canada Report 2019", Government of Canada, September 2019, page 6, link: https://www.ic.gc.ca/eic/site/cipointernet-internetopic.nsf/vwapj/IP_Canada_Report_2019_eng.pdf/$file/IP_Canada_Report_2019_eng.pdf. In the 2022 Global Talent Competitiveness Index, Canada fell to 15th place, down from 9th place in 2015, with its lowest scores for immigrant retention (19th). See INSEAD, "The Global Talent Competitiveness Index 2022," November 2022, page 32, link: https://www.insead.edu/sites/default/files/assets/dept/fr/gtci/GTCI-2022-report.pdf.

[9] See Australian Strategic Policy Institute, "Critical Technology Tracker, Appendix 1.1: Top 5 country visual snapshot", April 2023, link: https://ad-aspi.s3.ap-southeast-2.amazonaws.com/2023-03/PB69-CriticalTechTracker-Appendix-1.1_0.pdf?VersionId=A_QAiK_ps0.4cYJ.qfJB1eoEk15SlqYq.

99 Bank, Suite / bureau 1001, Ottawa, Canada K1P 6B9 THEBUSINESSCOUNCIL.CA

Economic security threats represent serious risks of substantial harm to our society

To be clear, not all attacks directed against Canadian companies represent economic security threats requiring a national security response. Most threats today can be countered by conventional tools, such as civil litigation.

Economic security threats are distinct. They represent serious risks of substantial harm to our country as a whole – to our sovereignty, values, economy, and people. As such, they are well beyond the capacity of conventional tools to address alone and require a coordinated national response.

Canada faces a series of interconnected economic security threats that erode Canada's economic competitiveness by tilting the playing field to others' advantage. The list is long. It includes mercantilism, weaponized trade, espionage, cyberattacks, malign foreign influence, and co-opted academic research.

State-sponsored actors are the primary perpetrators.[10] The Government of Canada regularly identifies the disruptive activities of countries, such as China, Russia, Iran, and North Korea, as posing the "greatest strategic threats" to Canada's security.[11]

[10] The activities of non-state actors also present risks to Canada's security. For instance, most criminal activity does not rise to the level of an economic security threat. But where criminality has the potential to harm Canadians on a scale that is potentially unbounded or indiscriminate, it will be transformed into a threat requiring a national security response. Ransomware directed against critical infrastructure is a prime example. However, it is also important to stress that the distinction between state and non-state actors has become increasingly blurred. The Canadian Centre for Cyber Security, for instance, notes that it is "almost certain" that the intelligence services of multiple countries "maintain associations with cybercriminals that engage in ransomware schemes." In these mutually beneficial relationships, "cybercriminals share stolen data with intelligence services while the intelligence service allows the cybercriminals to operate free from law enforcement." See Canadian Centre for Cyber Security, "National Cyber Threat Assessment: 2020", Government of Canada, November 16 2020, page 22, link: https://www.cyber.gc.ca/sites/default/files/cyber/publications/ncta-2020-e-web.pdf.

[11] See Canadian Centre for Cyber Security, "National Cyber Threat Assessment: 2020", Government of Canada, November 16 2020, page 5, link: https://www.cyber.gc.ca/sites/default/files/cyber/publications/ncta-2020-e-web.pdf; Canadian Centre for Cyber Security, "National Cyber Threat Assessment: 2023-2024", Government of Canada, October 28 2022, page 12, link: https://www.cyber.gc.ca/sites/default/files/ncta-2023-24-web.pdf; Standing Committee on Public Safety and National Security, "Caroline Xavier's Testimony", Assessment of Canada's Security Posture in Relation to Russia, Meeting #37, 44th Parliament, 1st Session, October 6 2022, link: https://www.ourcommons.ca/DocumentViewer/en/44-1/SECU/meeting-37/evidence; Privy Council Office, "Speech by the National Security and Intelligence Advisor to the Prime Minister to the Centre for International Governance Innovation", Government of Canada, June 8 2021, link: https://www.canada.ca/en/privy-council/services/national-security-intelligence-advisor-challenges.html; National Canadian Security Intelligence Service, "Remarks by Director David Vigneault to the Centre for International Governance Innovation", Government of Canada, February 9 2021, link: https://www.publicsafety.gc.ca/cnt/trnsprnc/brfng-mtrls/prlmntry-bndrs/20210625/28-en.aspx; Canadian Security Intelligence Service, "CSIS Transition Material for the Minister of Public Safety and Emergency Preparedness", Government of Canada, February 25 2022, link: https://www.canada.ca/en/security-intelligence-service/corporate/transparency/briefing-material/2021-transition-binder/threat-overview.html.

Mercantilism: competing against “State, Inc.”

Canada and its allies adhere to a common set of market values – such as the rule of law – that ensure that economic competition takes place on a level playing field.[12]

Strategic threat actors reject these globally recognized rules. They are increasingly adopting mercantilist practices aimed at giving their state champions the advantages necessary to replace imports with domestic production, climb global value chains, and seize dominant global market share in strategic sectors.[13]

The catalogue of predatory practices is lengthy. It extends well beyond generally accepted support for home-grown industries, to include manipulating local currencies to give their state champions an unfair price advantage in foreign markets, requirements for foreign firms to transfer advanced technology to state champions as a prerequisite to access their markets, and the showering of massive industrial subsidies on state champions that allow them to engage in unprofitable activity that wipes out foreign competition.[14]

These mercantilist interventions mean that Canadian firms are not competing with a typical commercial company. Instead, they are operating on a skewed playing field, competing with the full strength and resources of a foreign state.[15] In other words: “State, Inc.”

Mercantilism undermines Canadian society by introducing into our economy uncompetitive and inefficient enterprises that can accept significant financial losses to outbid and undercut Canadian businesses because they are governed by state interests and not shareholders.[16] This, in turn, destroys domestic industries and gives Canada no choice but to rely on state champions for critical economic inputs.[17]

---

[12] Stephanie Carvin notes that “[f]ree market/capitalist systems require a level playing field and rule of law in order to operate efficiently. See Stephanie Carvin, Stand on Guard: Reassessing Threats to Canada’s National Security, Toronto University Press, May 2021, page 144.

[13] See Stephanie Carvin, Stand on Guard: Reassessing Threats to Canada’s National Security, Toronto University Press, May 2021, page 144; Robert D. Atkinson, “What is Chinese ‘Innovation Mercantilism’ and How Should the UK and Allies Respond?”, Information Technology and Innovation Foundation, June 2021, pages 1-3, link: https://static1.squarespace.com/static/5f75a6c74b43624d99382ab6/t/60d9958153ee2b4b30210fc0/1624872326116/China+Research+Group+-+NATO+for+Trade+-+June.pdf.

[14] See Robert D. Atkinson, “What is Chinese ‘Innovation Mercantilism’ and How Should the UK and Allies Respond?”, Information Technology and Innovation Foundation, June 2021, pages 1-3, link: https://static1.squarespace.com/static/5f75a6c74b43624d99382ab6/t/60d9958153ee2b4b30210fc0/1624872326116/China+Research+Group+-+NATO+for+Trade+-+June.pdf; See Robert D. Atkinson, “Innovation Drag: China’s Economic Impact on Developed Nations”, Information Technology and Innovation Foundation, January 6 2020, link: https://itif.org/publications/2020/01/06/innovation-drag-chinas-economic-impact-developed-nations/.

[15] Stephanie Carvin notes that strategic threat actors’ “strategies and tactics combined are aimed at skewing the Canadian economic landscape.” See Stephanie Carvin, Stand on Guard: Reassessing Threats to Canada’s National Security, Toronto University Press, May 2021, page 144.

[16] See Sephanie Carvin, Stand on Guard: Reassessing Threats to Canada’s National Security, Toronto University Press, May 2021, page 144-145.

[17] See Stephanie Carvin, Stand on Guard: Reassessing Threats to Canada’s National Security, Toronto University Press, May 2021, page 144.

That reliance is especially problematic. The blurred lines between state policy and private pursuits means that even ostensibly private firms often have no choice but to support their government's national security objectives. This includes providing support, assistance, and cooperation to intelligence agencies.[18]

Weaponized trade: turning a positive sum activity into a zero sum game

Canadians' prosperity relies on a fair, predictable, and open international trading system. This system creates good, well-paying jobs for Canadians; promotes competition and product choice; and lowers consumer prices.

Our reliance on international trade also makes us vulnerable. Strategic threat actors seek to expand their global influence by weaponizing Canada's dependence on trade to pressure, induce, or influence the Government of Canada into taking actions that conform with their national priorities.[19]

Strategic threat actors use diverse tactics to coerce the Government of Canada. They can restrict the movement of critical goods for which there are no substitutes, withhold reciprocal access to domestic markets, and subject Canadian goods to onerous import inspections and conditions.[20]

With Canadian exports supporting more than one out of every six jobs in the country,[21] weaponized trade can directly threaten the livelihoods of Canadians. Indeed, between 2019 and 2020, China's targeting of the canola sector cost Canadian farmers upwards of $2.35 billion in lost exports and lower prices.[22]

Weaponized trade may also have broader societal costs.[23] As Russia's unprovoked invasion of Ukraine has highlighted for our European allies, overreliance on a strategic threat actor for critical economic inputs, especially one with systemically divergent values and interests, can prove both costly[24] and deadly[25] for society during a crisis.

---

[18] See Murray Scot Tanner, "Beijing's New National Intelligence Law: From Defense to Offense," Lawfare, July 20 2017, link: https://www.lawfareblog.com/beijings-new-national-intelligence-law-defense-offense; Intelligence and Security Committee of Parliament, "China", Parliament of the United Kingdom, July 13 2023, paragraph 8, link: https://isc.independent.gov.uk/wp-content/uploads/2023/07/ISC-China.pdf.

[19] See Matthew Reynolds and Matthew P Goodman, "Deny, Deflect, Deter: Countering China's Economic Coercion", Centre for Strategic and International Studies, March 2023, https://csis-website-prod.s3.amazonaws.com/s3fs-public/2023-03/230321_Goodman_CounteringChina%27s_EconomicCoercion.pdf?VersionId=UnF29lRogQV4vH6dy6ixTpfTnWvftd6v.

[20] See Matthew Reynolds and Matthew P Goodman, "Deny, Deflect, Deter: Countering China's Economic Coercion", Centre for Strategic and International Studies, March 2023, https://csis-website-prod.s3.amazonaws.com/s3fs-public/2023-03/230321_Goodman_CounteringChina%27s_EconomicCoercion.pdf?VersionId=UnF29lRogQV4vH6dy6ixTpfTnWvftd6v.

[21] See Global Affairs Canada, "2022 Canada's State of Trade: The Benefits of Free Trade Agreements", Government of Canada, August 1 2022, page 14, link: https://www.international.gc.ca/transparency-transparence/state-trade-commerce-international/2022.aspx?lang=eng.

[22] See Left Field Commodity Research, "Case Study – Impacts of the Chinese Trade Restrictions on the Canadian Canola Industry," Final Report, February 2021, page 22, link: https://www.canolacouncil.org/wp-content/uploads/2021/03/CCC-Market-Access-Impact-Report-China-Final.pdf.

[23] As a middle power with a trade-dependent economy, Canada is reliant on the rules-based international trading system to advance its national economic interests. Weaponized trade jeopardizes this system by putting into doubt widely accepted international norms and laws. Despite being the ninth largest economy globally, Canada stands third out of 164 World Trade Organization members in terms of frequency of disputes being brought for resolution, and sixth in the number of disputes being defended. See Valerie Hughes, "Canada: A Key Player in WTO Dispute Settlement", Centre for International Governance Innovation, February 2018, page 2, link: https://www.cigionline.org/static/documents/documents/Reflections%20Series%20Paper%20no.11%20HughesWEB.pdf.

99 Bank, Suite / bureau 1001, Ottawa, Canada K1P 6B9 THEBUSINESSCOUNCIL.CA

Canada is dependent on strategic threat actors for a broad range of commodities vital to Canadians' safety, security, and prosperity. Using data compiled by the United Nations, a recent study found that Canada is strategically dependent upon China, a country with a history of weaponizing trade, for at least 367 categories of goods.[26] Eighty-three of these categories service the critical infrastructure that Canadians rely upon daily to heat and power their homes, move their products to and from international markets, and communicate with their loved ones across our vast nation.[27]

Espionage: using Canadian ingenuity against Canadians

As an advanced, free-market economy home to many of the world's most successful and innovative companies, Canada has become an attractive target for states seeking to advance their domestic industries through espionage.[28]

Strategic threat actors use a wide range of methods to covertly steal commercially valuable information, such as confidential business plans, proprietary manufacturing processes, and intellectual property.

They include the use of intelligence officers and state-affiliated hackers, corporate insiders with legitimate access, as well as seemingly benign joint ventures and university research partnerships.[29]

Businesses are typically targeted directly. The 2022 arrest of a power utility employee for allegedly stealing trade secrets for China's benefit provides an example.[30]

[24] Without access to cheap Russian energy import, Germany, Europe's economic engine, has lost a key source of its industrial might. This could threaten prosperity across the continent. See Constanze Stelzenmüller, "A German has crisis will cause jitters across Europe", The Brookings Institution, July 18 2022, link: https://www.brookings.edu/articles/a-german-gas-crisis-will-cause-jitters-across-europe/; Matthew Karnitschnig, "Rust Belt on the Rhine", POLITICO, July 13 2023, link: https://www.politico.eu/article/rust-belt-on-the-rhine-the-deindustrialization-of-germany/.

[25] Modelling shows that high energy prices, resulting from a loss of cheap Russian energy imports, claimed up to 68,000 European lives in the Winter of 2022-2023. See The Economist, "Expensive energy may have killed more Europeans than covid-19 last winter", May 10 2023, link: https://www.economist.com/graphic-detail/2023/05/10/expensive-energy-may-have-killed-more-europeans-than-covid-19-last-winter.

[26] See James Rogers, Dr Andrew Foxall, Matthew Henderson, and Sam Armstrong, "Breaking the China Supply Chain: How the 'Five Eyes' can Decouple from Strategic Dependency", Henry Jackson Society, May 14 2020, page 5, link: https://henryjacksonsociety.org/publications/breaking-the-china-supply-chain-how-the-five-eyes-can-decouple-from-strategic-dependency/.

[27] See James Rogers, Dr Andrew Foxall, Matthew Henderson, and Sam Armstrong, "Breaking the China Supply Chain: How the 'Five Eyes' can Decouple from Strategic Dependency", Henry Jackson Society, May 14 2020, page 5, link: https://henryjacksonsociety.org/publications/breaking-the-china-supply-chain-how-the-five-eyes-can-decouple-from-strategic-dependency/.

[28] See Stephanie Carvin, Stand on Guard: Reassessing Threats to Canada's National Security, Toronto University Press, May 2021, page 119; Canadian Security Intelligence Service, "Remarks by Director David Vigneault to the Centre for International Governance Innovation", Government of Canada, February 9 2021, link: https://www.publicsafety.gc.ca/cnt/trnsprnc/brfng-mtrls/prlmntry-bndrs/20210625/28-en.aspx.

[29] See Canadian Security Intelligence Service, "Remarks by Director David Vigneault to the Centre for International Governance Innovation", Government of Canada, February 9 2021, link: https://www.publicsafety.gc.ca/cnt/trnsprnc/brfng-mtrls/prlmntry-bndrs/20210625/28-en.aspx.

[30] See Royal Canadian Mounted Police, "Hydro-Québec employee charged with espionage," Government of Canada, November 14 2022, link: https://www.rcmp-grc.gc.ca/en/news/2022/hydro-quebec-employee-charged-espionage.

However, corporate information will be targeted wherever it may reside.[31] In 2014, it was discovered that a Chinese state-sponsored cyber actor had compromised the digital systems of the National Research Council.[32] The actor stole more than 40,000 files, including "intellectual property and advanced research and proprietary business information" from the government agency's private sector partners.[33]

The theft of Canadian ingenuity is used to build or enhance state champions' products. Without having to make decades worth of costly investments, such as in research and development, state theft gives these companies a leg up over Canadian businesses.[34]

Stolen information is also used to give state champions insights into Canadian companies' business dealings, such as in bids for large overseas procurements.[35] As one expert notes, "[i]f the bottom line of a Canadian firm is already known, it will be easy for the other side to outbid or negotiate around them."[36]

These tactics collectively destroy the incentive for Canadian businesses to enter new markets, innovate and grow.[37] Over time, they may permanently hollow out Corporate Canada.[38]

While no precise estimate of the cost of economic espionage currently exists in this country, based on studies from the United States,[39] the cost to Canadians is likely tens of billions of dollars annually.

---

[31] According to the National Security and Intelligence Committee of Parliamentarians, governments "hold enormous amounts of data about…Canadian businesses and innovative sectors." Strategic threat actors recognize this fact. The Committee asserts that strategic threat actors seek to compromise government systems in order to "sap the vitality of individual companies and of the economy." See National Security and Intelligence Committee of Parliamentarians ,"Special Report on the Government of Canada's Framework and Activities to Defend its Systems and Networks from Cyber Attack," Government of Canada, February 14 2022, paragraph 1, link: https://www.nsicop-cpsnr.ca/reports/rp-2022-02-14/2022-cyber-attack-framework-report-en.pdf. The same logic applies to academic institutions. The Committee emphasises that strategic threat actors "seek to utilize the open and innovative features of these [Canadian postsecondary education] institutions to further their own objectives, which include…espionage and intellectual property theft." See National Security and Intelligence Committee of Parliamentarians, "Annual Report 2019", Government of Canada, March 12 2020, paragraph 171, link: https://www.nsicop-cpsnr.ca/reports/rp-2020-03-12-ar/annual_report_2019_public_en.pdf;

[32] See National Security and Intelligence Committee of Parliamentarians ,"Special Report on the Government of Canada's Framework and Activities to Defend its Systems and Networks from Cyber Attack," Government of Canada, February 14 2022, page 92, link: https://www.nsicop-cpsnr.ca/reports/rp-2022-02-14/2022-cyber-attack-framework-report-en.pdf.

[33] See National Security and Intelligence Committee of Parliamentarians ,"Special Report on the Government of Canada's Framework and Activities to Defend its Systems and Networks from Cyber Attack," Government of Canada, February 14 2022, page 92, link: https://www.nsicop-cpsnr.ca/reports/rp-2022-02-14/2022-cyber-attack-framework-report-en.pdf.

[34] See Stephanie Carvin, Stand on Guard: Reassessing Threats to Canada's National Security, Toronto University Press, May 2021, page 119.

[35] See Stephanie Carvin, Stand on Guard: Reassessing Threats to Canada's National Security, Toronto University Press, May 2021, page 119.

[36] See Stephanie Carvin, Stand on Guard: Reassessing Threats to Canada's National Security, Toronto University Press, May 2021, page 119.

[37] See Robert D. Atkinson, "Innovation Drag: China's Economic Impact on Developed Nations", Information Technology and Innovation Foundation, January 6 2020, link: https://itif.org/publications/2020/01/06/innovation-drag-chinas-economic-impact-developed-nations/.

[38] See Robert D. Atkinson, "Innovation Drag: China's Economic Impact on Developed Nations", Information Technology and Innovation Foundation, January 6 2020, link: https://itif.org/publications/2020/01/06/innovation-drag-chinas-economic-impact-developed-nations/.

Cyberattacks: disrupting the backbone of Canadian society

Just as the Industrial Revolution brought about enormous benefits for society, the unfolding digital revolution[40] has the potential to do the same. It can help companies reach new buyers and markets; make products faster and more efficiently; and improve consumer convenience, choice, and value.

However, as international interactions shift into cyberspace, we have seen skyrocketing levels of cyberattacks directed at Canadian businesses.

Canadian companies represent more than half of all known cyber victims in this country and are the most frequent focus of geopolitically inspired cyberattacks against Canada.[41] To give a sense of the problem's scale, two out of every five companies in this country were the victims of a cyberattack within the last two years.[42]

The impact is staggering. Attacks often result in reputational damage, lost revenues and business opportunities, legal repercussions, as well as lasting damage to business infrastructure and operations. By one estimate, ransomware[43] alone cost the Canadian economy US$4.3 billion in paid ransoms and lost productivity in 2021.[44]

Cyberattacks against critical infrastructure – such as electrical grids, telecommunication networks, and natural gas pipelines – are particularly troubling, given their potential to wreak large-scale havoc on Canadians' everyday lives.

Critical infrastructure operators will continue to be at high risk from cybercriminals, including those affiliated with nation states, because of operators' "deep pockets" and the "impact of operational downtime on the customers [operators] serve."[45] State actors are expected to continue to target critical infrastructure "to pre-position in the case of future hostilities, and as a form of power projection and intimidation."[46]

---

[39] An independent commission in the United States estimated that a strategic threat actors' economic espionage and intellectual property theft cost the American economy up to US$600 billion annually by discouraging the capital investments required for innovation and undermining American employer's overseas competitiveness. See The Commission on the Theft of American Intellectual Property, "Written Comments on Behalf of the Commission on the Theft of American Intellectual Property to the United States Trade Representative," Government of the United States, May 11 2018, page 3, link: https://www.nbr.org/wp-content/uploads/pdfs/publications/ustr_written_comments_301_tariffs-may2018.pdf.

[40] The Canadian economy is undergoing digitalization at breakneck speed. Over the past decade, Canada's digital economy grew roughly forty percent faster than, and generated almost four times as many jobs as, the overall economy. See Statistics Canada, "Measuring digital economic activities in Canada, 2010 to 2017", Government of Canada, May 3 2019, link: https://www150.statcan.gc.ca/n1/daily-quotidien/190503/dq190503a-eng.htm.

[41] See Center on Multidimensional Conflicts, "Geopolitical Cyber Incidents in Canada: 2023 Assessment", Université du Québec à Montréal, July 2023, page 5, link: https://dandurand.uqam.ca/wp-content/uploads/2023/06/2023-06-05-rapport-OCM-ENG.pdf.

[42] See Statistics Canada, "Cybersecurity incidents in 2020 compared with 2019, by business characteristics", Government of Canada, May 28 2021, link: https://www150.statcan.gc.ca/t1/tbl1/en/cv.action?pid=3310035801;

[43] Ransomeware is a type of malicious software designed to block access to a computer system until a sum of money is paid.

[44] See Emisoft Malware Lab, "The Cost of Ransomware in 2021. A Country-by-Country Analysis", April 27 2021, link: https://www.emsisoft.com/en/blog/38426/the-cost-of-ransomware-in-2021-a-country-by-country-analysis/.

[45] See Canadian Centre for Cyber Security, "National Cyber Threat Assessment: 2023-2024", Government of Canada, October 28 2022, page 12, link: https://www.cyber.gc.ca/sites/default/files/ncta-2023-24-web.pdf.

[46] See Canadian Centre for Cyber Security, "National Cyber Threat Assessment: 2023-2024", Government of Canada, October 28 2022, page 11, link: https://www.cyber.gc.ca/sites/default/files/ncta-2023-24-web.pdf.

Recent incidents in Canada involving critical infrastructure include:

- In May 2022, a "Russian-speaking cybercrime group" disrupted the operations of a Canadian aerospace company providing engineering and research and development services to the Canadian Armed Forces. The firm had recently been selected to participate in the modernization of the CH-146 Griffon helicopter fleet.[47]

- In April 2023, a "pro-Russia" hacker group engaged in a string of distributed denial-of-service attacks during the Ukrainian Prime Minister's visit to Canada. The attacks caused the websites of major Canadian businesses in the utility, transportation, and banking sectors to crash.[48]

- In April 2023, leaked intelligence revealed that "Russian-backed hackers" gained access to and control over a Canadian natural gas distributor's digital systems.[49] The Head of the Canadian Centre for Cyber Security asserted that the hackers "had the potential to cause physical damage" to the distributors' pipeline network.[50]

It is difficult to overstate critical infrastructures' importance to Canadians' safety, security, and prosperity. While not resulting from a cyberattack, a power outage in August 2003 that lasted less than a week caused an estimated $2.3 billion loss to Ontario's economy, contributed to a 0.7% decrease in Canada's GDP in August, and very likely led to loss of life.[51] Given the growth of the Canadian economy in the 20 years since then, the impact of a similar cyber-induced outage would be several orders of magnitude larger.

[47] See Center on Multidimensional Conflicts, "Geopolitical Cyber Incidents in Canada: 2023 Assessment", Université du Québec à Montréal, July 2023, page 4, link: https://dandurand.uqam.ca/wp-content/uploads/2023/06/2023-06-05-rapport-OCM-ENG.pdf; Lyle Adriano, "National defence contractor suffers cyberattack", Insurance Business, June 10 2022, link: https://www.insurancebusinessmag.com/ca/news/cyber/national-defence-contractor-suffers-cyberattack-409136.aspx.
[48] See Lillian Roy, "Pro-Russia hackers say they were behind Hydro-Quebec cyberattack", CTV News, April 13, 2023, link: https://montreal.ctvnews.ca/pro-russia-hackers-say-they-were-behind-hydro-quebec-cyberattack-1.6353627; Tom Blackwell, "'Trudeau's being cocky': Russian hackers claim attacks on PM, Pearson airport and others", National Post, April 14 2023, link: https://nationalpost.com/news/canada/russian-cyber-attacks-canada; Sidhartha Banerjee, "Cyberattack knocks out Hydro-Québec's website, mobile app", The Canadian Press, April 13 2023, link: https://globalnews.ca/news/9620864/hydro-quebec-cyber-attack/.
[49] See Amanda Stephenson, "Apparent leaked U.S. docs suggest pro-Russian hackers accessed Canada's gas network. Should we be concerned?", Canadian Press, April 10 2023, link: https://www.cbc.ca/news/politics/energy-sector-target-cyberattacks-experts-1.6806300.
[50] See Catherine Tunney, "Intelligence agency says cyber threat actor 'had the potential' to damage critical infrastructure", Canadian Broadcasting Corporation, April 13 2023, link: https://www.cbc.ca/news/politics/cse-critical-infrastructure-1.6809645.
[51] See Canadian Centre for Cyber Security, "Cyber threat bulletin: The cyber threat to Canada's electricity sector," Government of Canada, November 30 2020, link: https://www.cyber.gc.ca/en/guidance/cyber-threat-bulletin-cyber-threat-canadas-electricity-sector.

Malign foreign influence: eroding Canadians' trust and confidence

Foreign states seek to influence Canadian society. Most of this activity is perfectly legitimate. It is both lawful and appropriate for foreign states to have views of Canada's domestic affairs and to express those views with Canadians.[52]

However, foreign states veer from diplomacy into unacceptable malign foreign influence when their activities are covert, deceptive, or threatening.[53]

The current narrative surrounding malign foreign influence is rightly focused on the integrity of democratic processes and the safety and security of targeted ethnic or cultural groups.

However, strategic threat actors actively target all aspects of Canadian society to advance their strategic interests to our detriment.[54] This includes the use of third parties wielding deceptive tactics online to damage strategically important sectors of the Canadian economy.

In June 2022, a malicious actor with possible links to China deployed thousands of inauthentic social media accounts to carry out a coordinated disinformation campaign against a Canadian company developing a rare earth mine in northern Saskatchewan.[55]

Shortly after the miner announced its project, inauthentic social media posts began to target locals with false claims regarding the project's environmental and labour record.[56]

A post from "Ashely Wilson" stated: "[t]he protection of the lake, everyone's responsibility, if once mining, how to ensure the health of workers, firmly resist."[57] Another user, "Farrah", stated: "[i]t's not exciting, our lakes will be destroyed."[58] "Brown Emily" and "Gonzales Bonnie" were equally appalled, respectively referring to the discovery as "terrible" and "terrifying."[59]

---

[52] See The Right Honourable David Johnston, Independent Special Rapporteur on Foreign Interference, "First Report", Government of Canada, May 23 2023, page 11, link: https://www.canada.ca/content/dam/di-id/documents/rpt/rapporteur/Independent-Special-Rapporteur%20-Report-eng.pdf; Stephanie Carvin, Stand on Guard: Reassessing Threats to Canada's National Security, Toronto University Press, May 2021, page 186.
[53] See The Right Honourable David Johnston, Independent Special Rapporteur on Foreign Interference, "First Report", Government of Canada, May 23 2023, page 11, link: https://www.canada.ca/content/dam/di-id/documents/rpt/rapporteur/Independent-Special-Rapporteur%20-Report-eng.pdf.
[54] See Public Safety Canada, "Enhancing Foreign Influence Transparency: Exploring Measures to Strengthen Canada's Approach", Government of Canada, March 10 2023, link: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2023-nhncng-frgn-nfluence/index-en.aspx.
[55] See Mandiant, "Pro-PRC DRAGONBRIDGE Influence Campaign Targets Rare Earths Mining Companies in Attempt to Thwart Rivalry to PRC Market Dominance", June 28 2022, link: https://www.mandiant.com/resources/blog/dragonbridge-targets-rare-earths-mining-companies.
[56] See Mandiant, "Pro-PRC DRAGONBRIDGE Influence Campaign Targets Rare Earths Mining Companies in Attempt to Thwart Rivalry to PRC Market Dominance", June 28 2022, link: https://www.mandiant.com/resources/blog/dragonbridge-targets-rare-earths-mining-companies.
[57] See Mandiant, "Pro-PRC DRAGONBRIDGE Influence Campaign Targets Rare Earths Mining Companies in Attempt to Thwart Rivalry to PRC Market Dominance", June 28 2022, link: https://www.mandiant.com/resources/blog/dragonbridge-targets-rare-earths-mining-companies.
[58] See Mandiant, "Pro-PRC DRAGONBRIDGE Influence Campaign Targets Rare Earths Mining Companies in Attempt to Thwart Rivalry to PRC Market Dominance", June 28 2022, link: https://www.mandiant.com/resources/blog/dragonbridge-targets-rare-earths-mining-companies.
[59] See Mandiant, "Pro-PRC DRAGONBRIDGE Influence Campaign Targets Rare Earths Mining Companies in Attempt to Thwart Rivalry to PRC Market Dominance", June 28 2022, link: https://www.mandiant.com/resources/blog/dragonbridge-targets-rare-earths-mining-companies.

The plan of attack was clear: whip up local opposition against the project, force the stoppage of the miner's operations, and undermine a sector essential to Canada's security and prosperity.[60]

In an era of heightened geopolitical rivalry, these attacks are increasingly becoming the norm. Other recent attacks targeting the Canadian economy include Russian and Iranian disinformation campaigns advancing narratives critical of energy pipelines and the Government of Canada's immigration policies.[61]

Co-opted academic research: exploiting Canadian openness and collaboration

Open and collaborative academic research is indispensable to pushing the boundaries of Canadian science and technology. However, strategic threat actors exploit this feature of our academic institutions to advance their priorities at our expense.[62]

They may deploy visiting faculty, private sector collaborators, or not-for-profit organizations to gain unauthorized access to valuable information, expertise, or technology.[63]

In some scenarios, the co-opting of Canadian-led research can lead to advancements in foreign states' strategic, military or intelligence capabilities.[64]

For instance, instead of strengthening Canada's defensive capacities through the domestic development and commercialization of cutting-edge technologies, we have repeatedly seen Canadian academic institutions enter into partnerships that support foreign states' military ambitions.

From 2018 to 2023, academics at ten of Canada's leading universities published more than 240 joint papers on advanced research topics, including quantum cryptography, photonics, and space science, with military scientists working out of China's top military institution.[65]

---

[60] See Mandiant, "Pro-PRC DRAGONBRIDGE Influence Campaign Targets Rare Earths Mining Companies in Attempt to Thwart Rivalry to PRC Market Dominance", June 28 2022, link: https://www.mandiant.com/resources/blog/dragonbridge-targets-rare-earths-mining-companies; Fortunately, the disinformation campaign failed. According to the security firm that uncovered the attacks, malicious actor's poor execution – evidenced by Ashley Wilson's nearly incomprehensible tweet – was the limiting factor in the campaign gaining enough traction to scuttle the mining project.
[61] See Roberto Rocha and Jeff Yates, "Twitter trolls stoked debates about immigrants and pipelines in Canada, data show", Canadian Broadcasting Corporation, February 12 2019, link: https://www.cbc.ca/news/canada/twitter-troll-pipeline-immigrant-russia-iran-1.5014750.
[62] See Canadian Security Intelligence Service, "Protect your research", Government of Canada, January 31, 2022, link: https://www.canada.ca/content/dam/csis-scrs/documents/publications/2021/protect-your-research/AOSE_Regional_Factsheet_ONTARIO_DIGITAL_ISBN_A.pdf; National Security and Intelligence Committee of Parliamentarians, "Annual Report 2019", Government of Canada, March 12 2020, paragraph 171, link: https://www.nsicop-cpsnr.ca/reports/rp-2020-03-12-ar/annual_report_2019_public_en.pdf.
[63] See Intelligence and Security Committee of Parliament, "China", Parliament of the United Kingdom, July 13 2023, paragraphs 51-53, link: https://isc.independent.gov.uk/wp-content/uploads/2023/07/ISC-China.pdf.
[64] See Task Force on National Security, "A National Security Strategy for the 2020s," Graduate School of Public and International Affairs, University of Ottawa, May 2020, page 9, link: https://socialsciences.uottawa.ca/public-international-affairs/sites/socialsciences.uottawa.ca.public-international-affairs/files/natsec_report_gspia_may2022.pdf.
[65] See Steven Chase and Robert Fife, "Canadian universities conducting joint research with Chinese military scientists," The Globe and Mail, January 30 2023, link: https://www.theglobeandmail.com/politics/article-chinese-military-scientists-canadian-universities/.

99 Bank, Suite / bureau 1001, Ottawa, Canada K1P 6B9 THEBUSINESSCOUNCIL.CA

Failure to address growing threats puts our country at risk

Canada's new geopolitical reality means that economic security – repeatedly taken for granted, overlooked, or simply ignored – is now central to the preservation of our national security.

Therein lies the challenge for the country.

Our decades' long neglect of economic security issues has made us vulnerable. To use the Canadian Security Intelligence Services' own words, Canada has become an "attractive and permissive target."[66]

Failure to address this challenge with urgency and ambition will have serious, long-term consequences for Canadians. The Chief of the Communications Security Establishment explained it this way: "Cyber security is not abstract. Cyber systems, digital systems, they do not exist in a vacuum. They exist in relation to people with real-world implications for their privacy, their prosperity, their wellbeing."[67]

If left unchecked, attempts to degrade our economic capacity will result in the loss of secure, well-paying jobs for Canadian workers; forgone tax revenues to pay for essential public services, like health care and public transit; as well as lost leadership in advanced industries vital to the country's national strength and long-term economic health.[68]

This point takes on increased significance as the Government of Canada spends tens of billions of dollars annually to promote Canada's transition to a net-zero economy.[69] If economic security considerations – such as measures to tackle espionage – are not baked into the Government of Canada's investments in industrial capacity, taxpayers' hard-earned money will likely end up subsidizing others' net-zero industries.

---

[66] See National Security and Intelligence Committee of Parliamentarians, "Annual Report 2019", Government of Canada, March 12 2020, paragraph 294, link: https://www.nsicop-cpsnr.ca/reports/rp-2020-03-12-ar/annual_report_2019_public_en.pdf; Stephanie Carvin has noted that "espionage against Canadian businesses is very much alive and well." See Stephanie Carvin, Stand on Guard: Reassessing Threats to Canada's National Security, Toronto University Press, May 2021, page 116.

[67] Communications Security Establishment, "Chief Shelly Bruce's speech for Centre for International Governance Innovation", Government of Canada, May 18, 2021, link: https://www.cse-cst.gc.ca/en/information-and-resources/chief-shelly-bruces-speech-centre-international-governance-innovation-may.

[68] An examination of scholarly literature has shown that, by shrinking market opportunities and reducing the profits that innovators need to invest, strategic threat actors' practices have slowed the process of innovation in Western nations. Innovation is the single most important long-term driver of economic growth for advanced economies like Canada. Thus, allowing strategic threat actors' practices to continue unabated will hinder our economy's capacity to generate opportunities and prosperity for Canadians. See Robert D. Atkinson, "Innovation Drag: China's Economic Impact on Developed Nations", Information Technology and Innovation Foundation, January 6 2020, link: https://itif.org/publications/2020/01/06/innovation-drag-chinas-economic-impact-developed-nations/; The Director of the Canadian Security Intelligence Service has noted that "By subverting our ability to innovate and commercialize research, espionage results in lost jobs and diminished economic growth." See Canadian Security Intelligence Service, "Remarks by Director David Vigneault to the Centre for International Governance Innovation", Government of Canada, February 9 2021, link: https://www.publicsafety.gc.ca/cnt/trnsprnc/brfng-mtrls/prlmntry-bndrs/20210625/28-en.aspx.

[69] See Department of Finance Canada, "Budget 2023, Chapter 3: A Made-In-Canada Plan: Affordable Energy, Good Jobs, and a Growing Clean Economy", Government of Canada, March 28 2023, link: https://www.budget.canada.ca/2023/home-accueil-en.html.

Attacks directed against Canadian businesses also erode the beliefs we cherish most as Canadians. This includes the principle of free enterprise and fair competition; the tenet that all persons are accountable to the law, equally enforced and independently adjudicated; and the values that our laws promise, such as Canadians' rights to privacy or security of the person.[70]

The threat of punitive cyberattacks against critical infrastructure is illustrative. Russian-aligned cyber actors have targeted Canadian energy companies for its "psychological impact," including to "weaken Canadian [military and humanitarian] support for Ukraine."[71] By creating consequences for challenging illiberal behavior on the international stage, punitive cyberattacks complicate Canada's ability to independently assert its values.

We also must be mindful that Canada's closest allies are moving fast in this era of heightened geopolitical risk to improve their abilities to identify and mitigate economic security threats.[72]

If Canada fails to move in lockstep with its closest allies in building out its economic security capacity, it risks being perceived as a "weak link." This would jeopardize the country's relationships with its closest allies at a pivotal moment when the global order is being reshaped and partnership matters most.

There are already troubling signs that Canada's closest allies are taking note of our reluctance to seriously confront growing security threats. Some argue that has resulted in the country increasingly sitting on the sidelines when it comes to vital conversations around security.[73]

---

[70] See Communications Security Establishment, "Chief Shelly Bruce's speech for Centre for International Governance Innovation", Government of Canada, May 18 2021, link: https://www.cse-cst.gc.ca/en/information-and-resources/chief-shelly-bruces-speech-centre-international-governance-innovation-may.

[71] See Canadian Centre for Cyber Security, "The Cyber Threat to Canada's Oil and Gas Sector", Government of Canada, June 22 2023, page 7, link: https://www.cyber.gc.ca/sites/default/files/cyber-threat-oil-gas-e.pdf.

[72] This includes revamping policies, legislating new tools and authorities, and seeking new partnerships. See Task Force on National Security, "A National Security Strategy for the 2020s," Graduate School of Public and International Affairs, University of Ottawa, May 2020, pages 1-2, link: https://socialsciences.uottawa.ca/public-international-affairs/sites/socialsciences.uottawa.ca.public-international-affairs/files/natsec_report_gspia_may2022.pdf. According to National Security and Intelligence Committee of Parliamentarians, Australia is "at the forefront of Western nations in addressing the threat of foreign interference." The Committee notes that "Australia has passed a suite of legislative tools to...address the threat, including the introduction of new offences in that country's Criminal Code in relation to espionage and foreign interference, and amendments to other offences such as treason and treachery. The Committee goes on to assert that "[t]he legislation creates a new transparency scheme that prescribes the registration of persons acting as agents of foreign principals and requires regular public disclosures" and that "Australia also established a National Counter Foreign Interference Coordinator charged with delivering an 'effective, efficient and consistent national response to foreign interference by providing a focal point for coordinating policy and program development and leading engagement with private sector areas.'" See National Security and Intelligence Committee of Parliamentarians, "Annual Report 2019", Government of Canada, March 12 2020, paragraph 177, link: https://www.nsicop-cpsnr.ca/reports/rp-2020-03-12-ar/annual_report_2019_public_en.pdf.

[73] According to a group of leading security academics and practitioners, Canada is "falling behind our allies in taking practical, concrete steps to address national security threats." The group argues that "[o]ur lack of a firm response... presents a serious risk for our allies, and could affect our security and intelligence relations with them." See Task Force on National Security, "A National Security Strategy for the 2020s," Graduate School of Public and International Affairs, University of Ottawa, May 2020, pages 2, 4, 5, link: https://socialsciences.uottawa.ca/public-international-affairs/sites/socialsciences.uottawa.ca.public-international-affairs/files/natsec_report_gspia_may2022.pdf. Leaked American classified materials indicate that Canada's long-standing resistance to meeting its NATO's spending targets has resulted in mounting frustration among allies. According to one document, "[w]idespread defense shortfalls hinder Canadian capabilities, while straining partner relationships and alliance contributions." See Lili Bayer and Zi-Ann Lum, "NATO vs. Canada, its nicest truant", POLITICO, June 15 2023, link: https://www.politico.eu/article/nato-vs-canada-its-nicest-truant/; Christopher Hernandez-Roy, Vincent Rigby, and Henry Ziemer, "Canadian Membership in AUKUS: A Time for Action", Center for Strategic and International Studies, May 9 2023, link: https://www.csis.org/analysis/canadian-membership-aukus-time-action.

The Prime Minister's former National Security and Intelligence Adviser has written that "[t]he glacial pace at which Canada appears to be adapting to the realities of modern great power competition has left it far behind the curve, with consequences for...Ottawa's reputation among its allies."[74]

This likely contributed to Canada's exclusion from AUKUS, a security partnership between three of Canada's closest allies intended to align member states' defence and technology sectors to develop the next generation of military capabilities.[75]

The time for after-the-fact policy patches is over

The Government of Canada has been responding to our new geopolitical reality. But its actions have been slow, modest, and piecemeal.

This approach stems largely from a mode of governance that responds to immediate and pressing issues that arise without sufficient long-term planning for dealing with strategic threat actors which think well beyond the length of an average Canadian political cycle.

Canada's efforts to combat foreign interference demonstrates the weakness of this approach. According to the National Security and Intelligence Committee of Parliamentarians, "Canada's ability to address foreign interference is limited by the absence of a holistic approach."[76] In the Committee's view, Canada's "[r]eactions to foreign interference remain ad hoc and case-specific, rarely putting them in their broader context."[77]

The lack of information-sharing powers provided to the Canadian Security Intelligence Service offers another example of the approach's pitfalls. While the Minister of Public Safety tasked the Director of the Canadian Security Intelligence Service in May 2022 with ensuring that "organizations working in sensitive domains are aware of current and emerging economic security threats,"[78] the agency remains without the legislative powers to proactively share threat intelligence and advice with such organizations.[79]

This in no way represents a coherent approach to tackling strategic threat actors that think long-term and operate in sophisticated and pervasive ways. The time for after-the-fact policy patches is over.

---

[74] See Christopher Hernandez-Roy, Vincent Rigby, and Henry Ziemer, "Canadian Membership in AUKUS: A Time for Action", Center for Strategic and International Studies, May 9 2023, link: https://www.csis.org/analysis/canadian-membership-aukus-time-action.
[75] See Christopher Hernandez-Roy, Vincent Rigby, and Henry Ziemer, "Canadian Membership in AUKUS: A Time for Action", Center for Strategic and International Studies, May 9 2023, link: https://www.csis.org/analysis/canadian-membership-aukus-time-action.
[76] See National Security and Intelligence Committee of Parliamentarians, "Annual Report 2019", Government of Canada, March 12 2020, paragraph 296, link: https://www.nsicop-cpsnr.ca/reports/rp-2020-03-12-ar/annual_report_2019_public_en.pdf
[77] See National Security and Intelligence Committee of Parliamentarians, "Annual Report 2019", Government of Canada, March 12 2020, paragraph 294, link: https://www.nsicop-cpsnr.ca/reports/rp-2020-03-12-ar/annual_report_2019_public_en.pdf
[78] See Minister of Public Safety Canada, "2022 Director's Mandate Letter," Government of Canada, May 27, 2023, link: https://www.canada.ca/en/security-intelligence-service/corporate/transparency/mandate-dir-mandat-eng.html.
[79] Addressing a crowd of researchers at the University of Waterloo in 2021, the Director of Canadian Security Intelligence Service noted that, "[o]ur Act enables advice to government but limits our ability to provide relevant advice to key partners, including many of you listening today." See Canadian Security Intelligence Service, "Remarks by Director David Vigneault to the Centre for International Governance Innovation," Government of Canada, February 9 2021, link: https://www.publicsafety.gc.ca/cnt/trnsprnc/brfng-mtrls/prlmntry-bndrs/20210625/28-en.aspx.

Canada must catch up with its closest allies

Canada must fundamentally alter the way it approaches issues of national security. This will require an over-arching national security strategy that takes an eyes wide open approach to the complex ways strategic threat actors seek to undermine Canada,[80] while explicitly recognizing that economic security is central to a broader national vision of a more secure country.

Only by doing so can the Government of Canada take full advantage of all facets of its national power – including its diplomatic, defence, financial, economic, technological, and intelligence capabilities – to effectively safeguard our economic security and ensure our shared prosperity, safety, and sovereignty in this period of heightened geopolitical risk.

Canada's one and only national security policy – *Securing an Open Society*[81] – is not up to the task. Released almost two decades ago, when terrorist attacks, weapons of mass destruction, and the SARS outbreak were the preoccupation of the day, the policy makes almost no mention of the economic security threats now facing the country.

Securing an Open Society therefore falls significantly short of the modern national security strategies of Canada's closest allies:

The United States' 2022 national security strategy clearly articulates the principle that *economic security is national security*. The American strategy considers economic security from a broad, multi-faceted perspective, including trade and commerce, industrial strategy, and rules governing cyberspace. The strategy notes that "if the United States is to succeed..., we must invest in our innovation and industrial strength, and build our resilience, at home."[82]

Reflecting on "changes in [global] power balances and intensifying geopolitical competitions," Japan's 2022 national security strategy asserts that "issues not necessarily deemed as security targets in the past, such as supply chain vulnerabilities, increasing threats to critical infrastructures, and leadership struggles over advanced technologies, ha[ve]...become a major security challenge." Japan's security strategy thus argues that "the scope of security has expanded to include the economic sector, making economic measures even more necessary to ensure security."[83]

[80] See Aaron Shull and Wesley Wark, "Reimagining a Canadian National Security Strategy," Centre for International Governance Innovation, December 6 2021, link: https://www.cigionline.org/publications/reimagining-a-canadian-national-security-strategy/; Task Force on National Security, "A National Security Strategy for the 2020s," Graduate School of Public and International Affairs, University of Ottawa, May 2020, link: https://socialsciences.uottawa.ca/public-international-affairs/sites/socialsciences.uottawa.ca.public-international-affairs/files/natsec_report_gspia_may2022.pdf.

[81] See Privy Council Office, "Securing an Open Society: Canada's National Security Policy", Government of Canada, April 2004, link: https://publications.gc.ca/collections/Collection/CP22-77-2004E.pdf.

[82] See Government of the United States, "National Security Strategy", October 2022, page 11, link: https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf.

[83] See Government of Japan, "National Security Strategy of Japan," December 2022, pages 1 and 6, link: https://www.cas.go.jp/jp/siryou/221216anzenhoshou/nss-e.pdf.

Germany's 2023 national security strategy, suitably entitled *Integrated Security for Germany,* follows the same logic. It states: "in the 21st century, security…means making sure our heating works in winter,…[h]aving smartphones that work because supplies of the necessary microchips are reliable,…[g]etting to work safely because our trains are not paralysed by cyberattacks."[84]

Even Australia's 2013 national security strategy identifies key economic imperatives, such as the protection of intellectual property, critical infrastructure, and supply chains, as being essential to its national security. Australia's strategy notes that "there is a mutually reinforcing link between our national security and our economic wellbeing,…[a] healthy economy underpins our stability and security, which in turn is conducive to the pursuit of our personal and national economic goals."[85]

Canada requires a national security strategy that establishes economic security as a central pillar. That strategy should describe current and anticipated economic security challenges, the role of economic security in advancing Canada's national security, the objectives of economic security policy, and the ways and means by which Canada can deliver on these objectives over the short, medium, and long run.

The strategy must also be balanced. While it must be capable of tackling the threats facing Canadians at home and abroad, it must also remain consistent with Canada's democratic values as well as ensure that the domestic and international environment remains conducive to beneficial cross-border activities, such as trade and economic immigration, which are central to our national interests.

In other words, protecting Canada's economic security should not be used as a veiled excuse for the Government of Canada to undermine Canadians' rights, adopt protectionist trade and investment rules, or decouple its relations with certain foreign states altogether.

This point cannot be overlooked. Some of Canada's closest allies have responded to our new geopolitical reality in ways that do not always live up to their commitment to the rules-based international order.[86] In rare cases, these actions could prove to be equally damaging to Canada's economic prosperity as the threat posed by strategic threat actors.

[84] See Government of Germany, "Robust, Resilient, Sustain: Integrated Security for Germany", June 2023, page 6, link: https://www.nationalesicherheitsstrategie.de/National-Security-Strategy-EN.pdf.
[85] See Government of Australia, "Strong and Secure: A Strategy for Australia's National Security", 2013, page 4, link: https://www.files.ethz.ch/isn/167267/Australia%20A%20Strategy%20for%20National%20Securit.pdf.
[86] This includes efforts to undermine countries' ability to effectively enforce their rights according to globally recognized trade rules. See Keith Johnson, "How Trump May Finally Kill the WTO," Foreign Policy, December 9 2019, link: https://foreignpolicy.com/2019/12/09/trump-may-kill-wto-finally-appellate-body-world-trade-organization/. It also includes the adoption of protectionist economic measures, such as a willingness to use regulations and market power, to tilt the economic playing field in their direction. See Report of the Standing Committee on International Trade, "United States' Inflation Reduction Act of 2022: Trade Impacts on Certain Canadian Sectors," House of Commons, May 2023, pages 9-11, link: https://www.ourcommons.ca/content/Committee/441/CIIT/Reports/RP12414355/441_CIIT_Rpt9_PDF/441_CIIT_Rpt9-e.pdf.

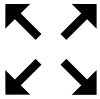
99 Bank, Suite / bureau 1001, Ottawa, Canada K1P 6B9 THEBUSINESSCOUNCIL.CA

Recommendations for an integrated national security strategy

To address the most glaring vulnerabilities in Canada's economic security posture, we urge that a new national security strategy adopt measures to:

Strengthen Canada's economic security architecture,

Bolster Canada's economic and innovative capabilities, and



Expand and reinvigorate Canada's international security partnerships.

Strengthen Canada's economic security architecture:

Strategic threat actors have no intention of undertaking the structural reforms needed to level the playing field for Canadian businesses. A latticework of new and interconnected laws, policies, and programs will therefore be required to improve Canadian companies' ability to deter, detect, and disrupt the threats facing our nation.

Recommendations:

1. The Government of Canada should comprehensively review and amend the *Canadian Security Intelligence Service Act* to align the agency's legislative mandate and powers with expanding expectations for it to identify, analyze, and disrupt threats to Canada's economic security. Among other things, an amended *Canadian Security Intelligence Service Act* should enable the agency to proactively share timely and actionable threat intelligence with stakeholders outside the federal government, including companies, where it is in the public interest and subject to all necessary safeguards and oversight.

2. The Government of Canada should provide the Canadian Security Intelligence Service with the resources necessary to launch a new division with an express mandate to provide training and advice to a broad range of private sector entities on how to defend themselves against economic threats. The agency should look to models established in allied countries, such as MI5's National Protective Security Authority.

3. To reduce risks to security of supply, prevent dependencies with respect to critical infrastructure, and counter the problematic transfer of sensitive technologies, the Government of Canada should move forward with amendments to the national security provisions of the *Investment Canada Act* to more precisely target and screen out malicious foreign investments. An amended *Investment Canada Act* should include a requirement for the Government of Canada to formally incorporate Canadian companies' unique perspectives on new and emerging national security threats within the investment review process.

4. To improve law enforcement's ability to thwart economic security threats, the Government of Canada should strengthen the *Security of Information Act's* economic espionage offence. Alongside this initiative, the Government of Canada should develop a new legal regime that allows the use of intelligence as evidence in the prosecution of criminal activities, while remaining compliant with the constitutional principle of the accused receiving a fair trial.

5. To enhance the cybersecurity and resiliency of critical infrastructure, the Government of Canada should:

    - Follow the United States' lead and legislate safe harbour protections[87] that eliminate legal obstacles that prevent companies from working voluntarily with each other and governments to address cyber challenges,

    - Explore new legal mechanisms to encourage developers of digital goods and services used by critical infrastructure operators to take all reasonable precautions to secure their products, and

    - Establish a centre of excellence within the Canadian Centre for Cyber Security to:

        › Bring together public and private sector partners to unify their defensive actions through synchronized cybersecurity planning, preparation and response, like what is done by the Joint Cyber Defense Collaborative of the United States' Cybersecurity and Infrastructure Security Agency;

        › Encourage more meaningful, two-way information sharing within and between government and critical infrastructure providers, including on emerging threats to critical cyber systems, the safety record of current technologies, and the relative benefits of different security measures;

        › Convene and support regular tabletop and threat hunting exercises where critical infrastructure providers and government stakeholders work through simulated events to improve their collective responses to major cyber incidents;

        › Establish a systemized process to review major cyber intrusions to capture and share lessons learned as well as make concrete recommendations for improving cybersecurity and resiliency; and

        › Offer onsite incident response services to critical infrastructure providers that require immediate assistance.

6. To safeguard our continued access to critical economic inputs, while strengthening the Government of Canada's capability to act independently on the global stage, the Government of Canada should work with sectors vulnerable to economic coercion to strengthen the depth and resilience of critical supply chains. This should include conducting vulnerability reviews, sharing threat information, developing robust mitigation strategies, curbing excessive dependence on strategic threat actors, and increasing the availability of commercial free-market alternatives.

[87] For instance, the Government of Canada should make explicit in the Competition Act that collaborations among competitors that have no have anti-competitive impacts are permissible.

99 Bank, Suite / bureau 1001, Ottawa, Canada K1P 6B9 THEBUSINESSCOUNCIL.CA

7. To blunt the impacts of mercantilist practices, the Government of Canada should create new legal mechanisms to block the import of foreign goods and services that have benefitted materially from unfair economic practices. The Government of Canada's initial focus should be on blocking strategic threat actors' market access to critical industries where they are using illegal means to catch up and surpass Canada.

8. To deter, denounce, and discipline those actors who threaten the integrity of critical infrastructure systems, the Government of Canada should follow the United States' lead and amend the *Criminal Code* to expressly criminalize willful or negligent acts that materially interfere with critical infrastructure through financial penalties, imprisonment, or both.

9. To prevent Canadian-led academic research from furthering strategic threat actors' interests at our expense, the Government of Canada should, in duly justified circumstances, ban entities linked to these states from participating in, or benefiting from, Canadian academic research.

10. To enable the earlier and more effective disruption of malign foreign influence, as well as to increase the public's awareness of the nature, scale, and extent of foreign activities in domestic affairs, the Government of Canada should move forward with the enactment of a foreign influence transparency regime. Like existing regimes in the United States, Australia, and the United Kingdom, Canada's scheme should require entities acting on behalf of a foreign state to publicly declare their activities intended to influence government decision-making or public opinion. The adoption of any registry must be consistent with the values we share in our democracy, including our commitment to be an open, free, and welcoming place to study, work, and invest.

Bolster Canada's economic and innovative capabilities:

We must abandon the notion that it is possible for Canadian businesses to compete on a level playing field with state champions in developing and commercializing emerging and disruptive technologies. They simply do not play by established rules.

To prevail in these circumstances, the Government of Canada will need to complement the economic and innovative capacity of Canadian companies with a modern industrial strategy. That strategy must increase our country's ability to systemically translate intellectual capital into world-leading technologies and internationally competitive businesses.

The Government of Canada must identify and support advanced technologies that are foundational to spurring economic growth, strategic from a national security perspective, and where companies on their own are not yet able to make the investments needed to develop and commercialize such technologies. The goal should be to help Canadian companies do what they do best – innovate, scale, and compete globally.

Together, these investments will support millions of secure, well-paying jobs by encouraging billions of dollars of economic activity. They will also increase our ability to act autonomously on the international stage by reducing Canada's vulnerability to economic coercion, and boost the country's economic clout, thereby providing the means to invest in our security.

99 Bank, Suite / bureau 1001, Ottawa, Canada K1P 6B9 THEBUSINESSCOUNCIL.CA

Recommendations:

1. The Government of Canada should modernize its science and technology architecture to reward high-risk, high-payoff research in emerging and disruptive technology fields essential to our economic and national security. In modernizing programs, special attention should be made to displacing problematic foreign sources of financing for academic research, as well as retaining and commercializing more advanced research at home.

2. The Government of Canada should stimulate Canadian innovation in emerging and disruptive technology fields essential to our economic and national security, while integrating new technologies into the Canadian government, through the strategic use of public sector procurement. In doing so, the Government of Canada should look to agile and challenge-based models used in allied countries, such as the United States' highly successful Defense Advanced Research Projects Agency.

3. To strengthen Canada's intelligence capabilities, support academic institutions, and create new economic opportunities for businesses, the Government of Canada should partner with trusted academic researchers and businesses to co-develop and deploy advanced security solutions across the Canadian intelligence community. The Government of Canada should emulate the approach adopted by the United States' Intelligence Advanced Research Projects Activity. This specialized government agency invests in high-risk, high-payoff research that pushes the boundaries of science and technology to empower the American intelligence community to do its work better and more efficiently.

4. Canada must invest in the input that lies at the core of economic growth and innovation: talent. The Government of Canada should:

    - Refocus Canada's economic-class immigration programs to ensure that sectors essential to Canada's economic and national security have quick and reliable access to the trusted, specialized, and high-skilled international talent they need to drive innovation, scale, and compete internationally;

    - Scale organizations with a proven track record of advancing the recruitment and training of underrepresented groups in fields of security, such as Rogers Cybersecure Catalyst;

    - Incent post-secondary institutions with leading security programs, such as the University of New Brunswick and Durham College, to increase enrollment rates and offer students more experiential learning opportunities; and

    - Increase Canada's ability to attract, cultivate, and retain world-class security talent by creating greater opportunities for personnel exchanges between trusted academic institutions, businesses and government departments and agencies, such as the Canadian Armed Forces, Communications Security Establishment, Royal Canadian Mounted Police, and Canadian Security Intelligence Service.

Expand and reinvigorate Canada's international security partnerships:

Canada's international security partnerships – including participation within the G7, Five Eyes, NORAD, and NATO – are some of the country's most important strategic assets. By providing a platform for security cooperation, Canada's international security partnerships act as a force multiplier, amplifying Canada's capacity to respond to shared economic security challenges that affect Canadians at home and abroad.

Canada must expand and reinvigorate its network of security alliances and partnerships to uphold and strengthen the principles, institutions, and rules-based international order that have enabled so much stability, prosperity, and growth. The end goal for Canada should be a world in which responsible state behaviour is the norm, and where irresponsible behaviour is isolating and costly.

Recommendations:

1. The Canadian military remains the guarantor of the country's peace, stability, and prosperity, as well as our commitment to allied nations. The Government of Canada should recommit to meeting the defence investment target of two percent of GDP set out under NATO's 2014 *Wales Summit Defence Investment Pledge*. Considering the most recent NATO summit in Vilnius, Lithuania, this pledge should be viewed as a "floor" and not a "ceiling".

2. To better monitor, mitigate, and respond to threats to Canada and the United States' heavily integrated cross-border infrastructure, the Government of Canada should work with the United States to create a formal bilateral public-private sector working group. Composed of a cross-section of public and private sector leaders, the goal of this group would be to facilitate the free, frank, and confidential exchange of strategic information about the evolving threat environment as well as the ways and means by which governments and businesses on both sides of our shared border can work together to build a stronger, more secure North America.

3. Given the importance of international trade and commerce to the security and prosperity of Canadians, the Government of Canada, in partnership with other like-minded allies, should reinforce the rules-based economic order by:

    - Strengthening the multilateral trading system with the World Trade Organization at its core;

    - Strengthening or joining international frameworks promoting free and fair international trade and investment among market-oriented countries, such as the Comprehensive and Progressive Trans-Pacific Partnership and the Indo-Pacific Economic Framework; and

    - Creating and enhancing plurilateral measures to collectively deter, withstand, and counter economic coercion and other unfair trade practices, such as through a "NATO for trade" whereby allied nations agree to come to the aid of each other when they are economically threatened. As a part of this initiative, Canada should leverage its economic advantages, such as in the production of energy, food, and minerals, to help reduce our allies' trade dependencies on strategic threat actors.

4. The Government of Canada should work closer with its Five Eyes partners and other like-minded allies to undermine malicious cyber actors, including by:

    - Jointly deterring, attributing, and responding to cyberattacks which breach global rules and norms in cyberspace;

    - Shutting down illegal online markets for cyber tools and services, which lower the start-up time and threshold of sophistication necessary for malicious actors to target and sabotage Canadian companies;

    - Better regulating crypto assets and exchanges, which are used by malicious actors to conceal their identities and obfuscate their activity from national security and law enforcement agencies; and

    - Increasing pressure on countries with lenient or non-existent laws and law enforcement related to cybercrime and other malicious cyber activities.

5. To build upon Canada's capabilities in cybersecurity, artificial intelligence, and quantum, the Government of Canada should pursue admission to *AUKUS*, the trilateral security and technology co-operation pact between the United States, United Kingdom, and Australia. The Government of Canada's initial focus should be on *AUKUS*' second institutional pillar, which focuses on advancing these and other important technologies.

6. International technical standards have a direct bearing on Canada's national security, including by curbing the abusive use of emerging and disruptive technologies that could threaten Canada's economic security. The Government of Canada should ratchet up its collaboration with Canadian businesses to support the development and implementation of international technical standards for next generation technologies that reflect our national interests as well as free-market and democratic values.

7. To enhance Canada's diplomatic influence, foster greater collaboration with like-minded nations, and advance Canada's economic interests, the Government of Canada should pursue a program of "economic diplomacy", whereby the country's industrial capacity is leveraged to help address global security challenges.

Execution and review will be critical

A new national security strategy is not the end of the road but the start. The strategy will only fulfill its purpose when its contents are fully executed. Measures included in a new strategy must therefore be implemented in a timely and effective manner.

Further, as much of the battleground that the Government of Canada needs to contest lies outside of its direct control, deep and sustained partnership with Canadian businesses, from the strategic to the tactical level, will be required to achieve success. Consultation will not suffice.

Lastly, to stay relevant in a rapidly evolving threat environment, a new strategy should be viewed as a "living document." It must be regularly and systematically evaluated, such as every three years, to ensure that it is satisfying its objectives. The Government of Canada should make necessary revisions to the strategy should it expect any material changes.

To ensure that these measures are taken and given adequate priority, we urge that:

1. The newly created cabinet committee on national security and intelligence – the National Security Council – be chaired by the Prime Minister and staffed by all relevant ministers and senior government officials with a security mandate, so as to provide the sustained and forward-looking leadership and decision-making needed to implement the new national security strategy;

2. The role of the National Security and Intelligence Advisor be established in legislation and enhanced to better organize and coordinate the intelligence community as well as consult, engage, and partner with Canadian businesses;

3. The Prime Minister amend the mandate letters of all relevant ministers, including public safety, foreign affairs, defence, industry, and finance, to ensure that economic security considerations are incorporated into each of their priorities;

4. A dedicated economic security division be established within the Privy Council Office and that economic security units be created or enhanced within all major ministries, such as public safety, foreign affairs, defence, industry, and finance, to better plan and coordinate economic security policies in partnership with Canadian businesses;

5. The Government of Canada release annual implementation plans setting out the specific measures that the government intends to carry out within a given calendar year to implement the new strategy; and

6. Within eighteen months of the roll-out of a new national security strategy, the National Security and Intelligence Committee of Parliamentarians initiate, and the Government of Canada respond to, a special study of the Government of Canada's framework for tackling economic security threats with a view to:

    - Identifying gaps that exist in legislation, policies, or governance mechanisms;
    - Strengthening ministerial accountability; and
    - Improving transparency, including helping businesses better understand the roles of the government organizations responsible for serving them.

As a part of this study, the Committee should launch an economic security "roadshow", like the bi-partisan roadshows employed by the United States' Senate Select Committee on Intelligence, to gain insights from companies on the frontlines of attack.

Canada's most innovative and successful companies are ready to do their part

Every year, Canada's most innovative and successful companies spend billions of dollars to defend Canadians against a growing list of economic security threats. This includes investing in measures to detect, mitigate, and respond to attacks; establishing partnerships with post-secondary institutions to train security professionals and develop defensive technologies; as well as sharing threat intelligence, expertise and best practices with governments and industry peers.

For instance, in critical infrastructure sectors, like energy, transportation and telecommunications, most Business Council of Canada members individually invest well over $100 million per year in Canada on measures to prevent, detect and respond to cybersecurity incidents. A sizable number of these members individually invest over $500 million annually.

Drawing on their deep experience and expertise, Canada's most innovative and successful companies are ready to work constructively with the Government of Canada to develop and implement a new national security strategy. This includes, but is in no way limited to:

1. Strengthening Canada's economic resilience by increasing the amount they invest annually on measures to detect, prevent, and disrupt economic security threats to Canada;

2. Sharing more with the government about what threats they are seeing on the ground to better inform government policy, as well as improve national security agencies' ability to investigate, analyze and disrupt threats

3. Increasing their investments in Canadian academic research to help displace problematic foreign sources of funding and to retain and commercialize more advanced research at home; and

4. Better supporting their large and diverse supply chains, including through education, capacity building, and relationship brokering, to increase awareness of the threats facing small and medium sized businesses, as well as roles and responsibilities of the government organizations responsible for serving them.

99 Bank, Suite / bureau 1001, Ottawa, Canada K1P 6B9 THEBUSINESSCOUNCIL.CA

Conclusion

The free, open, and relatively stable unipolar order that provided Canadians with extraordinary levels of safety, security, and prosperity is now consigned to history.

In our new geopolitical reality, Canadians face a turbulent, multipolar landscape that poses an unprecedented national security threat to their economic well-being.

With the economic health of Canadians now intertwined like never before with questions of national security, the time has come for the Government of Canada to take bold steps to protect Canadians.

That is why this report calls on the Government of Canada to create a first-of-its-kind national security strategy that establishes economic security as a central pillar.

The recommendations contained in this report offer a path to help government and businesses successfully navigate this new, more turbulent world together.

99 Bank, Suite / bureau 1001, Ottawa, Canada K1P 6B9

Report Citation
Business Council of Canada, “Economic Security is National Security: The Case for an Integrated Canadian Strategy,” September 7, 2023.

About the Business Council of Canada
Founded in 1976, the Business Council of Canada is a not-for-profit, non-partisan organization representing business leaders in every region and sector of the country. The Council’s member companies employ more than two million Canadians, contribute the largest share of federal corporate taxes, and are responsible for most of Canada’s exports, corporate philanthropy, and private-sector investments in research and development. Through supply chain partnerships, service contracts and mentoring programs, Business Council members support many hundreds of thousands of small businesses and entrepreneurs in communities of all sizes, in every part of Canada.

Disclaimer
This report reflects the views of the Business Council of Canada. This report may or may not necessarily reflect the perspective of individual Business Council of Canada members, and therefore should not be attributed to any one or more members.

99 Bank, Suite / bureau 1001, Ottawa, Canada K1P 6B9 THEBUSINESSCOUNCIL.CA