Research at risk: Global challenges, international perspectives, and Canadian solutions

Alex Wilner, Sarah Beach-Vaive, Catherine Carbonneau, Graeme Hopkins and Félix Leblanc
Carleton University, Ottawa, ON, Canada

Abstract
Although traditionally viewed as paragons of international cooperation, research institutions and universities are becoming venues for hostile foreign activity. Research security (RS) refers to the measures that protect the inputs, processes, and products that are part of scientific research, inquiry, and discovery. While RS traces its roots to the 1940s, global economic and research and development competition, the nexus between dual-use technology and military power, a cluster of newly emerging industries, scientific responses to the COVID-19 pandemic, and societal shifts towards digitization, combine to challenge RS in unique ways. With an eye on safeguarding traditional notions of open science, our article refurbishes Canadian RS within the context of emerging challenges and international responses. Detailing the legal, extralegal, illegal, and other ways in which RS is threatened, we use a comparative assessment of emerging responses in the US, Australia, Japan, and Israel to draw lessons for Canada.

Keywords
Research security, open science, cybersecurity, science, dual-use technology, export controls, university research, national security

Corresponding author:
Alex Wilner, Carleton University, Norman Paterson School of International Affairs (NPSIA), Richcraft Hall, 1125 Colonel By Drive, Ottawa, ON K1S 5B6, Canada.
Email: alex.wilner@carleton.ca
Although traditionally viewed as paragons of international cooperation, research institutions are increasingly becoming venues for hostile activity conducted by foreign actors. The type of research targeted often relates directly to a country’s economic prosperity and national security. Foreign governments, for instance, in geopolitical competition with Canada and its allies, exploit the inherently open nature of its research institutions to gain access to cutting-edge research and intellectual property. They do so to acquire an economic, political, or strategic advantage. Indeed, high-profile instances of data theft and foreign espionage on research institutes are increasingly commonplace. Research security (RS)—as a distinct sub-study of national security—refers to the measures that protect the inputs, processes, and products that are part of scientific research, inquiry, and discovery. Historically, RS traces its roots to the Cold War period, an era characterized by state espionage of military technology; many of the RS approaches still in use today were first formulated to tackle these specific challenges. And yet, contemporary RS is undergoing dramatic and uncertain change: global economic and research and development (R&D) competition, the nexus between dual-use technology and military power, emerging industries in space, robotics, computer science, and nano and additive manufacturing, public health and scientific responses to the COVID-19 pandemic, and larger societal shifts towards digitization, combine to challenge contemporary RS in new and unique ways.

Canadian allies and other liberal democracies are exploring and enacting new policies, strategies, and regulations for enhancing RS in response. Canada, as an important global player in academic research, scientific discovery, and economic development, has much to lose from evolving challenges to RS and much to learn from international perspectives and responses. Unfortunately, the topic is largely overlooked by Canadian scholarship, and only recently has the Canadian government begun raising the alarm. In July 2021, for illustration, the Canadian Security Intelligence Service (CSIS) “went into overdrive in an effort to warn universities and researchers” of the evolving nature of international espionage. Since 2020, and within the backdrop of a spike in malicious activity targeting Canadian pandemic and medical research, CSIS began briefing thousands of researchers at hundreds of research and industry groups and laboratories, warning them of the challenges ahead. CSIS acknowledged that part of its larger goal in openly discussing RS with researchers was to “influence an academic mindset” prevalent in Canada that champions scientific and international openness at the potential expense of national and economic security.\(^1\)

Our article seeks to reapply and refurbish Canadian RS within the context of emerging challenges and international responses with an eye on safeguarding traditional Canadian notions of open science.\(^2\) It is presented in four sections. The first

---

1. Joe Friesen, “CSIS warns Canadian universities to be on alert for international espionage,” The Globe and Mail, 26 July 2021.
2. This article is partially derived from a 2021 project conducted as part of the Capstone in Canadian Security Policy course, taught by Professor Alex Wilner in collaboration with Government of Canada partners at Public Safety Canada. The views contained herein are those of the authors alone.
section provides a brief overview of RS dating back to the Cold War, illustrating where, how, and why domestic responses were developed as they were. RS has a lengthy and prominent history among highly industrialized countries, a history that continues to affect Canada’s conceptualization of the topic today. The second section highlights the way contemporary research is threatened, focusing on the legal, extralegal, illegal, and other domestic (i.e., Canadian) RS challenges. The third section provides a comparative assessment of evolving RS responses among four liberal democracies: the US, Australia, Japan, and Israel. Each faces a unique set of RS challenges but all share a common backdrop of having traditionally and historically promoted global science that stretches beyond national borders and national security considerations, suggesting a broad range of lessons that Canada might consider and adopt. The fourth section, functioning as the article’s conclusion, unpacks these international lessons along four themes—centralization, collaboration, controls, and cybersecurity—providing contextual insight for Canada’s own evolving approach to the topic.

Research security: Past and present

Protecting domestic research has long been a concern of states. Following World War II, countering foreign state espionage of military technology—especially as it pertained to nuclear and atomic science—was of primary concern. Among Canada’s allies, special attention was placed on countering Soviet efforts to leverage ideological sympathizers residing in the West for access to sensitive research. Counterintelligence strategies were developed and deployed in response. As the Cold War evolved, concerns pivoted towards the Soviets’ apparent quantitative superiority in military force; American RS priorities shifted towards maintaining the US’s own technological advantage. Doing so required the US to better control the flow of dual-use technologies by implementing a series of export controls, classification laws, and visa regulations on foreign researchers. Moreover, the US pressed its allies to develop matching policies and programs. Many of the Canadian laws and regulations developed during this period are still in place and help govern and inform contemporary approaches to RS.

Research security evolved again with the thawing of the Cold War. As private industry in the West expanded its leadership into R&D, it began falling prey to foreign

3. While private funding represents 42 percent of Canadian R&D, this article’s focus is on public R&D research security. While many concerns and recommendations overlap between the two, the private sector presents unique challenges, including limited government authority and foreign corporate ownership, which deserve their own substantial consideration. As such, it rests beyond the scope of the paper.

4. Cases were selected according to several criteria: liberal democratic (and market capitalist) structures; global-spanning education and innovation sectors; divergent regional, geopolitical, and/or security considerations; differing degrees of association with Canada (e.g., core alliance partner, security partnership, or economic partnership); diverging approaches to contemporary research security.

5. National Research Council of the National Academies (NRC), Beyond “Fortress America” (Washington DC: National Academies Press, 2009).
intellectual property (IP) theft. But as the global military standoff receded, target states increasingly focused their efforts on limiting the economic, rather than military, effects of research theft. The rise of industrial espionage likewise widened the threat nexus: China, India, and even allied Germany and France became countries of concern. By the 2000s, RS was marked by non-traditional challenges stemming from global private sector entities. Responses adapted in kind, with the US detailing more stringent measures on foreign researchers coming to work or study within fields related to an expanded list of dual-use technologies. These new measures targeting researchers, however, were met with sharp criticism. As foreigners faced greater scrutiny, domestic research communities fretted about the consequences RS might have on the open and global nature of scientific inquiry.

That tension between RS and open science (OS) marked the 2010s. It sparked new academic interest in the topic, with focus placed on exploring the nature of dual-use technologies within the context of globalized science and national/security interests. Most famously, for illustration, researchers developing a vaccine for Avian Flu (H5N1) created a new strain of the virus transmissible to humans. Publication of certain elements of the research presented biosafety concerns. Science and Nature both sought US National Science Advisory Board for Biosecurity advice, which recommended a censored version of the paper be published. That sparked an outcry in the international scientific community on the grounds that censorship undermined the principles of OS and research replicability. The episode brought OS to the forefront of RS discussions and aggravated the disconnect between researchers and government authorities, one that persists today. Even so, other emerging RS scholarship during the 2010s explored the nature of the challenge for Western academic research. Both China and Russia continued to garner attention, provoked by several high-profile cases of foreign nationals and citizens charged with transmitting research secrets. Attention was placed on understanding how hostile foreign actors infiltrated universities to steal and acquire sensitive research.

Today, RS is inherently tied to the COVID-19 pandemic. Since 2020, some foreign governments have sought to mitigate the public health emergency by leveraging intelligence agencies to identify and steal medical research. The importance of developing and administering vaccines and treatments in order to bolster economic

---

6. David Malakoff, “Spy inquiry is taking toll on non-U.S. researchers,” American Association for the Advancement of Science 284, no. 5416 (1999): 882.
7. Ori Lev and Bracha Rager-Zisman, “Protecting public health in the age of emerging infections,” Focus 16, no. 6 (2014).
8. Stéphane Lefebvre, “The PRC’s compromise of U.S. government information and technologies,” International Journal of Intelligence and CounterIntelligence 22, no. 4 (2009): 652–666; John Poreba, “Neutralizing China’s student-spy network,” International Journal of Intelligence and CounterIntelligence 25, no. 2 (2012): 260–291; Dan Golden, “Why Russian spies really like American universities,” ProPublica, 23 July 2018.
9. Leah West, Thomas Juneau, and Amarnath Amarasingam, eds., Stress Tested (Calgary, AB: University of Calgary Press, 2021).
recovery placed a target on institutions involved in COVID-19 research. A string of warnings were meted out: in May 2020, the FBI warned of Chinese hacking of COVID-19 research institutions; in July, the Department of Justice charged two Chinese nationals with spying on American medical companies with support from the Chinese Ministry of State Security; later, Microsoft noted that Canada was the target of 35 percent more cyberattacks in 2020 than in 2019 and was the third most targeted country for COVID-19-related data. The Canadian Centre for Cyber Security went on to release Cyber Security Advice and Guidance for Research and Development Organizations During COVID-19, a selection of best practices for researchers. Canadian, British, and American officials subsequently issued technical information about malicious online activities “almost certainly” linked to the Russian intelligence service. The advisory provided precise indicators of compromise alongside detection and mitigation advice, including to universities, who faced a barrage of sophisticated attacks that went far beyond what they traditionally dealt with. A University of Montreal professor commented that “given the level of sophistication and persistence of these attacks, researchers are very ill-equipped to deal with them on their own.” Similarly, work-from-home and isolation mandates forced countless researchers to rely on poorly secured home networks. Cyber threat actors took advantage, leveraging vulnerabilities in virtual private networks and cloud applications to gain access to research. For instance, The Citizen Lab—a leading interdisciplinary laboratory, based at the University of Toronto, that explores the nexus between technology, human rights, and security—reported that virtual communications platforms like Zoom could route data through China (even if all participants were located outside China), providing it a potential opportunity for espionage. Moreover, travel bans and border closures forced many foreign researchers and students to take their research home with them, providing foreign threat actors with yet further access to sensitive information.

Canadian research security: Challenges, challengers, and considerations

Contemporary research security among Western liberal democracies is threatened through a variety of legal, extralegal, and illegal means, while Canadian RS faces other domestic challenges related to OS. The following section seeks to highlight some of the

10. Alex Wilner, Harrison Luce, Eva Ouellet, Olivia Williams, and Nelson Costa, “From public health to cyber hygiene: Cybersecurity and Canada’s healthcare sector,” *International Journal* 76, no. 4 (2021): 522–543.
11. Canadian Centre for Cyber Security, “Get cyber safe,” Government of Canada, 28 August 2020; Canadian Centre for Cyber Security, “National Cyber Threat Assessment 2020.”
12. Andréanne Apablaza, “Canadian COVID-19 researchers face a growing threat of cyber-espionage,” *University Affairs* (blog), 2020.
13. Bill Marczak and John Scott-Railton, “Move fast and roll your own crypto,” Citizen Lab Research Report 126, April 2020.
most common means employed by foreign adversaries to gain access to Canadian research.

**Legal challenges.** Research security faces three legal considerations. First, as leaders in global R&D, industrialized economies attract millions of foreign researchers and students who seek to work or study at domestic research institutes. This has been an incredible benefit to host countries, who reap the academic windfall of securing top foreign talent and the budgetary gains of international student fees.\(^\text{14}\) However, the percentage of foreign students and researchers remaining within their host country upon graduation appears to be declining.\(^\text{15}\) Many return to their native countries, driven by newly emerging economic opportunities, increasing difficulties in securing work or study permits, and surging levels of suspicion against foreign researchers.\(^\text{16}\) The result is a version of brain drain, with research expertise flowing back into emerging markets and states. The trend poses a challenge to the long-term viability of some Western research institutes dependent on international students and researchers. Second, the open nature of academic publishing comes with the risk that malicious actors (and adversaries) may use research findings to advance their own goals. China has publicly stated that it will, for instance, “absorb” global scholarship to further its own domestic priorities.\(^\text{17}\) By all standards of academia, it is free to do so. The RS challenge, however, relates to dual-use technologies that have both civilian and military/security applications. Some forms of open scholarship may inadvertently invite strategic competition.\(^\text{18}\) Third, and relatedly, the open nature of the global research community allows foreign researchers to gain access to sensitive research of interest to hostile governments.\(^\text{19}\) The risk arises in partnerships and joint ventures between research organizations. By working in Western labs and institutions, foreign researchers can build expertise that can later be exploited by their home countries upon their return.\(^\text{20}\)

\(^{14}\) National Science Foundation (NSF), *Fundamental Research Security*, MITRE Corporation (Virginia: JASON, 2019).

\(^{15}\) Brendan O’Malley, “Total international student enrolment continues to fall,” University World News, 20 November 2019; Youyou Zhou, “Chinese students increasingly return home after studying abroad,” Quartz, 29 July 2018.

\(^{16}\) NSF *Fundamental Research Security* 2019; Malakoff, “Spy inquiry is taking toll on non-U.S. researchers”; Roland Hwang and Rita Pin Ahrens, “Collaborations to prevent ‘researching while Asian’ from going viral,” Asian American Policy Review 30 (January 2020): 32–37.

\(^{17}\) William Hannas and Huey-Meei Chang, “China’s Access to Foreign AI Technology,” Center for Security and Emerging Technology, 2019, 1–44.

\(^{18}\) Lev and Rager-Zisman, “Protecting public health in the age of emerging infections.”

\(^{19}\) For example, the US Department of Energy (DOE) alone welcomes 35,000 foreign nationals to work in government-supported labs each year. United States Senate, “Threats to the U.S. research enterprise: China’s talent recruitment plans,” United States Government, 2019.

\(^{20}\) National Counterintelligence and Security Center (NCSC), “Foreign economic espionage in cyberspace 2018,” Office of the Director of National Intelligence.
Alternatively, foreign researchers may inadvertently engage in the IP theft of ideas gained during a partnership.21

Extralegal challenges. Three extralegal concerns challenge contemporary RS. First, though institutional research partnerships are increasingly commonplace in academia, they can nonetheless jeopardize domestic RS. Some ostensibly civilian research institutions are, in fact, either fused or directly linked to foreign military R&D efforts.22 When Canadian researchers collaborate with these foreign institutions and/or with foreign military-linked researchers, for instance, there is a risk that the product of their collaboration will be exploited by a foreign government or military. Second, foreign talent acquisition programs are often used to access foreign research. These programs recruit individual researchers in the West to conduct research for a foreign actor, often within their own domestic facilities.23 While these collaborative programs are not usually illegal per se, the contracts of many talent recruitment programs directly designate what is to be researched (generally dual-use technologies) and provide the foreign state with access to (or outright ownership of) IP. Frequently, these contracts also contain non-disclosure agreements, forcing domestic researchers to refrain from discussing their involvement in the programs.24 As such, dual-use research conducted in the West can unknowingly be exported to foreign states. Finally, some extralegal RS challenges stem from conflicts of interest and failures to disclose. These concerns arise when principal investigators on domestically funded research projects simultaneously conduct related research for, and/or are funded by, another country. In cases where research projects are linked, it is likely that information generated by a domestic project will find its way into a foreign one; findings seamlessly flow between them.25 By failing to disclose that a researcher is receiving foreign funding in a related area of research, domestic research grants may intentionally or unintentionally be used to fund research that is ultimately provided to foreign and hostile actors.26

Illegal challenges. Illegal activities are usually the most evident and well-understood RS challenge; three types stand out. First, adversaries will exploit the access domestic

21. NSF, Fundamental Research Security, 2019.
22. Glenn Tiffert, Global Engagement: Rethinking Risk in the Research Enterprise (Stanford, CA: Hoover Institution Press, 2020).
23. Melissa Flagg and Zachary Arnold, “A new institutional approach to research security in the United States,” Center for Security and Emerging Technology, 2021.
24. Jeffrey Mervis, “NSF’s handful of foreign influence cases may be due to how it investigates them,” American Association for the Advancement of Science, 2020.
25. NSF, Fundamental Research Security, 2019.
26. Christopher Wray, “The threat posed by the Chinese government and the Chinese Communist Party to the economic and national security of the United States,” Lecture presented at Hudson Institute, July 2020.
researchers have to classified or sensitive information in order to misappropriate it. At times domestic citizens are recruited by hostile states and paid in cash for information or IP that can be relatively easily stolen.\textsuperscript{27} While this type of insider threat is particularly salient with military related research, it occurs in other avenues of research as well. Moreover, hostile states may use leverage gained over domestic researchers, monetary or otherwise, through talent acquisition programs to coerce them into providing research of interest.\textsuperscript{28} In related fashion, adversaries might also use their vast network of foreign students and researchers studying and working in the West to gain access to sensitive research. By appealing to nationalism, using bribes, or coercing through threats to an individual or their family’s safety, foreign researchers and students are encouraged to gather information and bring it back with them when they return home.\textsuperscript{29} While gathering this sort of information can take the form of regular theft, it can also involve preying on the openness of the research community and asking researchers to share their work under the guise of academic collaboration.\textsuperscript{30} Second, hostile states frequently use their intelligence services to conduct espionage operations and gain access to research. Some intelligence services will embed agents within universities to establish connections with students and researchers who have access to privileged or classified information; these contacts can later be recruited to steal information.\textsuperscript{31} Finally, due to the relatively low costs of using cyberspace to illegally gain access to domestic research, cyberattacks remain a major and growing area of RS concern.\textsuperscript{32}

**Domestic and structural challenges.** Other RS challenges stem from domestic (i.e., Canadian) considerations. First, although CSIS has explicitly warned of the rising threat to Canadian research, Canada still lacks an overarching RS policy.\textsuperscript{33} Canada’s approach largely entails raising awareness among researchers and institutions, piecemeal: Innovation, Science and Economic Development (ISED) launched the Safeguarding your Research Portal to consolidate public information about RS; Public Safety leads workshops for researchers highlighting the risks and threats to, and best

\textsuperscript{27} Poreba, “Neutralizing China’s student-spy network”; Lefebvre, “The PRC’s compromise of U.S. government information and technologies”; Strobel, et al., “US accuses China of ‘super aggressive’ spy campaign on LinkedIn.” Reuters 2018.

\textsuperscript{28} NSF, *Fundamental Research Security*, 2019.

\textsuperscript{29} Poreba, “Neutralizing China’s student-spy network.”

\textsuperscript{30} Ibid.; Wray, “The threat posed by the Chinese government and the Chinese Communist Party.”

\textsuperscript{31} Golden, “Why Russian spies really like American universities.”

\textsuperscript{32} William Barr, “Attorney General William Barr’s Keynote Address: China Initiative Conference,” Keynote Address presented at the Centre for Strategic and International Studies Headquarters, Washington DC, 6 February 2020, \url{https://www.csis.org/analysis/attorney-general-william-barrs-keynote-address-china-initiative-conference} (accessed 18 July 2022); NCSC, “Foreign economic espionage in cyberspace 2018”; Canadian Security Intelligence Service (CSIS), “CSIS Public Report 2020,” Government of Canada, 12 April 2021, \url{https://www.canada.ca/en/security-intelligence-service/corporate/publications/2020- public-report/the-threat-environment.html#toc9} (accessed 18 July 2022).

\textsuperscript{33} Catharine Tunney, “State actors have done ‘significant harm’ to Canadian companies, says head of spy agency.” CBC News, 9 February 2021; CSIS, “CSIS Public Report 2020.”
practices for conducting safe and secure research; and facing an onslaught of pandemic-related challenges, CSIS, the Communications Security Establishment (CSE), and the Public Health Agency of Canada have each become more active and vocal in highlighting threats to researchers operating in specific areas of concern. Moreover, Canada regularly updates its cybersecurity awareness resources. While many of these recent initiatives suggest an interest within the Government of Canada to approach RS in a coordinated manner, much more still needs to be done. The RS mitigation measures currently in place, for instance, are generally legacy policies spread across and between various federal departments (including members of the security and foreign policy apparatus and inward-looking departments and grant-giving agencies) most often hyper-focused on specific issues that fall within a specific organization’s mandate. While it might be difficult, if not impossible, for a single institution to address fully all RS challenges, the range of actors involved in Canada’s current approach leads to a diffuse response, replete with competing departmental interests and (at times) contradictory approaches. Moreover, Canadian research security goes well beyond the federal government. Canadian universities—which fall within provincial jurisdiction—are on the front line and have an integral role to play. But they also clearly need support: not only have Canadian universities explicitly asked for more guidance from Canadian governments, the pandemic and associated rise in the number and sophistication of cyberattacks and data thefts have strained their ability to respond effectively on their own. Canadian university RS responses are guided by each individual institution; accordingly, they manifest themselves differently. Additionally, Canadian universities do not have a formalized mechanism to review threats to research at their institutions. While a coordinated approach to university RS policy could be undertaken through collaboration with provincial governments, the framing of RS as a national security consideration has unintentionally sidelined provincial authorities from RS discussions altogether. All of this came to a head in May 2021 when the Government of Alberta took a role in managing RS within the province, taking

34. Innovation, Science and Economic Development (ISED), “Introducing the Safeguarding your Research Portal,” Government of Canada, 2020; ISED, “Research Security Policy Statement – Spring 2021,” Government of Canada, March 2021.
35. Canadian Centre for Cyber Security, “Cyber threat bulletin: Impact of COVID-19 on cyber threat activity,” 2020.
36. Despite public warnings from Canada’s intelligence community about partnering with Huawei, the Natural Sciences and Engineering Research Council (NSERC) nonetheless supplied funding to Canadian universities in partnership with Huawei. Robert Fife and Steven Chase, “Ottawa partners with Huawei to fund university research despite security concerns,” The Globe and Mail, February 2021.
37. Evan Dyer, “Experts call on Canadian universities to close off China’s access to sensitive research,” CBC News, 15 September 2020; Apablaza, “Canadian COVID-19 researchers face a growing threat of cyberespionage.”
38. For example, McGill University has resources for researchers working with protected or classified information whereas Carleton University focuses primarily on promoting ethical conduct in research. McGill University, “Guidelines, Regulations and Safety,” 2021; Carleton International, “Safeguarding Your Research,” 2020, https://carleton.ca/ci/2020/safeguarding-your-research/ (accessed 11 July 2022).
unilateral action to limit foreign university partnerships while calling on the federal government to manage better the file from Ottawa.\textsuperscript{39}

Second, contemporary Canadian RS policy faces an inherent tension with the competing priorities and principles of open science. In Canada, OS is defined as “the practice of making scientific inputs, outputs and processes freely available to all with minimal restrictions.”\textsuperscript{40} Strengthening RS may jeopardize or restrict OS and might unintentionally be self-defeating if it affects Canadian researchers’ capacity to cooperate and innovate internationally. Researchers themselves are dubious of government attempts to regulate science, highlighting the paradox that the security benefits derived from regulating knowledge-sharing might weaken national security by hindering scientific advancement.\textsuperscript{41} Yet for all the benefits of OS, failing to adequately protect Canadian research could eventually lead to increased hesitation on the part of Canadian research institutes to engage in foreign cooperation out of fear of inadvertently putting their IP at risk. This, too, would be detrimental to Canadian R&D, as foreign collaboration is increasingly integral to competitive science. Accordingly, active collaboration on RS between government stakeholders, research institutes, and scholars is a key component of developing proportional policies and strategies relevant to the current state of OS.

Third, the predominance of Chinese nationals in high-profile and public espionage cases in Canada raises legitimate concerns that some foreign researchers are being unfairly and unduly accused because of their nationality or ethnic background. Recent cases of misguided prosecution of Chinese nationals have led some to fear an emerging environment where it is a crime to be “researching while Asian.”\textsuperscript{42} These concerns are especially relevant in Canada, which has experienced a spike of anti-Asian racism and hatred since 2019.\textsuperscript{43} Targeted RS measures run the risk of wrongly affecting certain minority communities and could discredit legitimate RS policy, yet Canadian governments cannot simply avoid creating RS policies out of fear of appeasing racism; a lack of leadership might encourage disparate jurisdictions and institutions to self-regulate in an inconsistent and harmful way.\textsuperscript{44} To complicate matters, foreign states have exploited Canadian concerns over institutionalized racism in order to foster

\textsuperscript{39} Robert Fife and Steven Chase, “Alberta calls for national security rules for academics to prevent intellectual property transfer to China,” The Globe and Mail, 25 May 2021.

\textsuperscript{40} Office of the Chief Science Advisor, “Roadmap for open science - Science.gc.ca.” Government of Canada, 2020.

\textsuperscript{41} Gary Marchant and Lynda Pope, “The problems with forbidding science,” Science and Engineering Ethics 15, no. 3 (2009): 375–394.

\textsuperscript{42} Hwang and Ahrens, “Collaborations to prevent ‘researching while Asian’ from going viral.”

\textsuperscript{43} Katie Nicholson, “Racism against Asians in Canada ranges from assault to insults since start of pandemic: Report” CBC News, 23 March 2021.

\textsuperscript{44} Hwang and Ahrens, “Collaborations to prevent ‘researching while Asian’ from going viral.”
Canadian opposition to certain policies. As such, balancing a robust RS approach with the risks of stigmatizing a minority community is crucial to the effective protection of Canadian research.

Finally, international students are central to the Canadian post-secondary landscape. Pre-pandemic, international students accounted for 40 percent of all tuition fees (equivalent to $4 billion) in 2018/2019. And, as over 28 percent of international students in Canada are Chinese nationals, financial experts have warned that three of Canada’s largest universities could face a cash crunch if China was to restrict unilaterally its students from studying in Canada. In the absence of federal guidance, universities may have a disincentive to implement strict RS policies if doing so means jeopardizing their own economic viability.

International research security: Lessons from abroad

What follows are illustrative case studies of contemporary RS strategies developed by the US, Australia, Japan, and Israel. The exploration considers each country’s specific characteristics and approach to RS, allowing for a contextualized comparison useful for drawing Canadian lessons.

United States. The American position on the current state of US research security is clear: it is a widely and publicly held position by US officials, across party lines, that China poses the greatest long-term challenge to American research. This challenge is viewed as both an economic and security concern. From an economic perspective, the US estimates that Chinese IP theft leads to $600 billion in annual lost revenue. This challenge is exacerbated because the theft itself largely targets dual-use research, which may provide China an eventual military advantage. Since Washington views Beijing as a strategic competitor, any action taken by China to steal technology or information to improve its military capability translates into a direct US national security threat. Some Americans go so far as to call it an existential concern, fearing eventual Chinese

45. In 2019, China’s ambassador to Canada penned an op-ed calling Canada’s demand that China release two detained Canadians all the while itself detaining Huawei’s Meng Wanzhou a form of “white supremacy.” Lu Shaye, “Why the double standard on justice for Canadians, Chinese?” The Hill Times, 9 January 2019.
46. Statistics Canada, “International student enrolments at Canadian public colleges and universities, 2017/2018,” Government of Canada, 19 February 2020; Statistics Canada, “The Daily — International students accounted for all of the growth in postsecondary enrolments in 2018/2019,” Government of Canada, 25 November 2020.
47. The Canadian Press, “Credit agency warns big risk to Canadian schools if China pulls students,” National Post, 7 February 2019.
48. United States Senate, “Threats to the U.S. research enterprise”; Wray, “The threat posed by the Chinese government and the Chinese Communist Party”; Barr, Keynote Address 2020.
49. NSF, Fundamental Research Security, 2019.
50. Government of the United States, National Security Strategy of the United States, 2017.
technological and scientific supremacy over the US.\footnote{Rush Doshi, \textit{The Long Game: China's Grand Strategy and the Displacement of American Order} (Oxford, UK: Oxford University Press, 2021).} Appreciating these economic, security, and geostrategic concerns help explain American RS policy.

Of primary concern for the US is that its domestic research and IP might be directed or transferred, legally, illegally, or extralegally, to China, especially through talent recruitment programs. A steadily rising number of American researchers are being enrolled into Chinese talent recruitment programs to conduct research on behalf of China within American laboratories.\footnote{Tiffert, \textit{Global Engagement}.} While this contracting of research is a concern to the US in and of itself, there have also been numerous cases of researchers failing to disclose their connections to Chinese recruitment programs when applying for US government funding.\footnote{See, for example, the 180 letters sent by the NIH regarding disclosure violations, or the “hundreds of people” identified by DOE as participating in Talent Recruitment Plans. US Senate, “Threats to the U.S. research enterprise”; Mervis, “NSF’s handful of foreign influence cases.”} This adds to the risk that research and IP may accidentally be shared internationally between projects and could allow foreign actors to gain access to research they might not otherwise have had access to. Additionally, there have also been high-profile cases in which researchers have expressly used funding provided by the US government to co-fund their projects in foreign countries through talent recruitment plans.\footnote{For example, see Drs. Percival Zhang, Mingquing Xiao, and Charles Lieber, US DoJ, “Former Virginia Tech professor sentenced for grant fraud, false statements, obstructions,” 9 September 2019; US DoJ, “Harvard University professor convicted of making false statements and tax offenses,” 21 December 2021; Jeff Mervis, “US math professor found guilty in latest China initiative trial,” \textit{Science}, 5 May 2022.}

A second area of major concern is the disconnect between and among the US research community, regulators, and investigators. Historically, American responses to RS have been spread among different departments with no central authority. The result has been an empowerment of certain actors with narrow control over RS, a lack of information sharing between stakeholders, and no consensus on the efficacy of the current approach.\footnote{Flagg and Arnold, “A new institutional approach to research security in the United States”; NSF, \textit{Fundamental Research Security}, 2019; US Senate, “Threats to the U.S. research enterprise”; NRC, \textit{Beyond “Fortress America.”}} That has intensified the divide between researchers and government regulators and investigators, with the former holding negative views of the government’s efforts to regulate science and research.\footnote{Flagg and Arnold, “A new institutional approach to research security in the United States.”} Yet, paradoxically, the research community has expressed confusion regarding current RS approaches, and has called for more guidance from federal authorities, especially around disclosure and talent
recruitment programs. Other poles within the research community question the integrity and purpose of current RS practices altogether.

Although criticized for its sluggish response to emerging RS concerns, the US has recently implemented new measures that seek to strengthen its position. Washington has become increasingly aggressive in its response to recruitment programs and insider threats, including by taking steps to bar members of federal agencies from joining foreign programs. It has also empowered its federal grant-giving agencies to be more assertive in monitoring grant recipients for failures to disclose participation in foreign talent recruitment programs. The National Institutes of Health (NIH)’s use of a dedicated compliance team, for illustration, that investigates undisclosed conflicts of interest has been specifically highlighted for its efficacy in uncovering grant violations. Finally, the US has taken measures to mitigate perceived insider threats from Chinese foreign researchers and students, including by limiting the length of visas issued to researchers working with dual-use technologies, and otherwise suspending entry to the US entirely. On the latter, President Donald Trump’s Proclamation 10043 (2020)—since upheld by President Joe Biden—bars entry of Chinese researchers (on F or J visas) who have past associations with Chinese institutions that support the country’s “military-civil fusion strategy.” Through the FBI, the US has also begun focusing on RS outreach to American academic institutions. The FBI’s Office of the Private Sector has liaisons embedded within FBI field offices in each state, tasked to engage with universities, highlight RS threats, and assist in developing local solutions.

To highlight these recent (and hardline) developments on US research security, consider National Security Presidential Memorandum 33 (NSPM-33) issued under the Trump administration in January 2020. The document ordered decisive action be taken to protect American research by centralizing the authority of the Office of Science and Technology Policy in future RS policy development. Through the Office, NSPM-33 calls for closer coordination between federal agencies’ disclosure mandates, increased information sharing between departments, and raising awareness among at-risk institutions and researchers. Moreover, and of importance to Canada, it calls for further international engagement with allies on the issue of RS to coordinate best practices across borders. Although NSPM-33’s status under the Biden administration is still unclear, the president has nonetheless signalled his intention to uphold some of its key

57. Hwang and Ahrens, “Collaborations to prevent ‘researching while Asian’ from going viral”; US Senate, “Threats to the U.S. research enterprise.”
58. Eileen Guo, Jess Aloe, and Karen Hao, “The US crackdown on Chinese economic espionage is a mess,” MIT Technology Review, 2 December 2021; Eileen Guo, “All charges against China initiative defendant gang Chen have been dismissed,” MIT Technology Review, 20 January 2020.
59. Mervis, “NSF’s handful of foreign influence cases.”
60. Ibid.; National Association for Foreign Student Affairs, “Proclamation suspending entry of Chinese students and researchers connected to PRC “military-civil fusion strategy,” February 2021.
61. 45th President of the United States, “Proclamation 10043: Suspension of entry as nonimmigrants of certain students and researchers from the People’s Republic of China,” May 2020; Stuart Anderson, “Biden keeps costly Trump visa policy denying Chinese grad students,” Forbes, August 2021.
elements, including on enhanced disclosure and coordination. Accordingly, the document provides a window into the evolving nature of American RS policy.62

**Australia.** Deep cooperation between Australia and the US on civilian, dual-use, and military research has long made the former a prime target of foreign espionage. While Australia has historically interpreted research espionage and IP theft as matters of institutional oversight, today the emerging consensus is that these challenges are a matter of foreign interference and national security.63 Of specific concern to Australia, given its proximity to China, is the level of cooperation between domestic and PLA-linked universities.64 Moreover, high-profile instances of Australian researchers being recruited by Chinese acquisition programs have raised concerns that Australian-funded research risks being misappropriated by China or used in ways that contravene Australian values (notably, in relation to China’s abuse of its Uyghur minorities, which some Australian leaders, alongside French, Dutch, and Canadian parliamentarians, have called a genocide).65

Assessing Australia’s evolving RS approach must take place within its larger context, however. Since 2017, for instance, Australia’s relationship with China has soured due to a series of events unrelated to RS, that have nonetheless facilitated bipartisan support for major new RS initiatives.66 Notably, the government created the National Counter Foreign Interference Coordinator to synchronize Australia’s response to foreign interference, including in RS.67 Australia’s current focus is on better managing RS policies across stakeholders. In August 2019, it established the University Foreign Interference Taskforce (UFIT), which stakes a holistic, whole-of-government perspective on RS subsumed within the larger umbrella of foreign interference. It successfully integrated the government and university sectors within a horizontal and vertical policy response mechanism. While UFIT is led by a steering group comprised of government departments, it is supported by subject matter experts

---

62. Mitch Ambrose, “US expanding disclosure requirements for scientists,” American Institute of Physics, 7 April 2021.
63. Dennis Normile, “Australia targets foreign influence at universities,” *Science* 365, no. 6457 (2019): 965–965; Australian Security Intelligence Organisation (ASIO), “Director-General’s Annual Threat Assessment,” 14 August 2020.
64. Alex Joske, “Picking flowers, making honey,” APO Policy Brief Report no. 10, 2018.
65. Alex Joske, “The company with Aussie roots that’s helping build China’s surveillance state,” Australian Strategic Policy Institute, Aug 2019; Daniel Hurst, “Australian senator calls to recognize China’s treatment of Uighurs as genocide,” *The Guardian*, 1 March 2021.
66. For example, Labour Senator Sam Dastyari’s links to the CCP; Australian support for investigations into COVID-19 origins; Olympic Games boycotts; trade disputes; Australians detained in China. Amy Remeikis, “Sam Dastyari quits as Labor senator over China connections,” *The Guardian*, 11 December 2017; Erin Handley, “Australia-China relations continued to sour in 2021,” ABC, 21 December 2021.
67. Department of Home Affairs, “National Counter Foreign Interference Coordinator,” Australian Government, 2020.
responsible for leading further development and providing advice on cybersecurity, research and IP, foreign collaboration, and culture and communication.68 UFIT has published guidelines that provide institutions a way to account for foreign interference in their research risk frameworks, and has (re)emphasized “knowing your partner” concepts providing individual researcher RS tools and support.69 Further, UFIT engages with the Australian Research Council, a national granting agency, in updating Conflict of Interest and Confidentiality Policy guidelines for researchers.70

Besides UFIT, the Australian government has itself taken other steps to protect its domestic research. It has sought to better coordinate cybersecurity with states, territories, and the private sector, including by providing A$1.6 million over ten years to enhance university cybersecurity, develop threat intelligence-sharing networks and sector-wide threat modelling, and a national cybersecurity forum.71 And, in adopting Australia’s Foreign Relations (State and Territory Arrangements) Act, the government established a general legislative scheme for all arrangements between Australian public actors and foreign governments, providing the minister for foreign affairs a veto on arrangements between public universities, local councils, state governments, and foreign entities, ensuring they are “not inconsistent with Australia’s foreign policy.”72

The Act was criticized for increasing the burden of compliance and jeopardizing collaborative opportunities, and because it regulates agreements negotiated by public institutions but not those pursued by private universities. Nor is there currently a process for appealing vetoed deals.73 As in the US and elsewhere, researchers have likewise criticized the heavy-handedness of Australia’s emerging RS approach, juxtaposing it against the virtues of open science; university administrators regularly dismiss public concerns as fearmongering.74 And, as in Canada, Australian universities’ budgets rely on Chinese foreign student fees.75 Following pressure from the

68. Department of Education, “Development of University Foreign Interference Taskforce - Guiding framework,” Australian Government, 2019.
69. University Foreign Interference Taskforce, Guidelines to Counter Foreign Interference in the Australian University Sector,” Australian Government, 2020.
70. Australian Research Council, “ARC Conflict of Interest and Confidentiality Policy version 2020.1,” 2020.
71. Australian Government, “Cyber Security Strategy,” 2020; David Mussington, Brent J. Arnold, Benoît Dupont, Scott Hilts, Timothy Grayson, Christian Leuprecht, Lian Nevill, Brian O’Higgins, and Josh Tupler, “Governing cyber security in Canada, Australia and the United States,” Centre for International Governance Innovation (CIGI), 4 April 2018, https://www.cigionline.org/publications/governing-cybersecurity-canada-australia-and-united-states (accessed 18 July 2022).
72. Australian Government, “Australia’s Foreign Relations (State and Territory Arrangements) Bill 2020,” 2020.
73. Rob Bolton, “Foreign relations bill adds to ‘government overreach,’” Australian Financial Review, December 2020.
74. Melissa Tyler and Siew F. La, “Australia’s universities need to be free to engage globally,” Pursuit, 27 November 2020.
75. Alex Joske found that the international tuition fees of Chinese students make up 25 to 30 percent of the overall income at some top Australian universities. Joske, “Picking flowers, making honey.”
education sector, an amendment was added to the Act specifying that university-to-university arrangements will only require notification if the foreign institution in question does not have “institutional autonomy,” defined as governance, research, and/or teaching independence from foreign government control.

Japan. Japanese RS is marked by two interesting (and interrelated) characteristics: it is almost exclusively focused on China and shadows the American approach. Geopolitical and regional factors play an oversized role in framing Japanese RS. Japan has identified particular areas of research China is known and/or suspected of having sought access to—including dual-use research in quantum computing, AI, and semiconductor manufacturing—through illegal technological transfers and espionage. Japan’s response, though unhurried, measured, and piecemeal in nature, is modelled after the American one. While Japan traditionally approached RS as a matter of economic security, like the US (and Australia), it is increasingly applying a national security lens to the topic. Tokyo’s primary concern is that a failure to mitigate threats to research will create a perception among Japan’s core ally (the US), other international security partners (within the G7, Quadrilateral Security Dialogue, and NATO, for instance), and key trading partners (including Canada, Australia, and the EU) that it is a weak link in regard to RS, leaving it isolated from Western partnerships. The state minister of foreign affairs warned, for instance, that if Japan does not strengthen its counterintelligence capabilities, close partners will be reluctant to work with it. As such, Japanese RS is as much about reassuring friends as it is about countering threats.

Japan’s focus on China stems from its oversized role in domestic higher education. Japanese universities heavily engage with Chinese universities, including forty-five partnerships with PLA-linked institutions in areas of dual-use technology. Additionally, Japanese universities, like those in Australia, are dependent on Chinese students, who represent 40 percent of all foreign students. And it is estimated that the Chinese government operates forty-six talent recruitment stations in Japan. The Australian Strategic Policy Institute (ASPI) has warned that some Chinese institutions

76. National Institute for Defense Studies, “NIDS China Security Report 2021,” Ministry of Defense, 2020; Smriti Mallapaty, “Japan considers tougher rules on research interference amid US-China tensions,” Nature, 4 August 2020.
77. Ayumi Tereoka, “When international students pose a very real risk,” The Japan Times, 20 September 2020; Tomohiro Osaki, “Japan boosts checks on Chinese students amid fears of campus spying,” The Japan Times, 15 October 2020.
78. Yusuke Takeuchi, “Japan to establish intel unit to counter economic espionage,” Nikkei Asia, 27 August 2020.
79. Gao Feng and Gigi Lee, “Japanese universities’ ties to China’s military-linked schools sparks concern,” Radio Free Asia, 11 November 2020.
80. Osaki, “Japan boosts checks on Chinese students amid fears of campus spying.”
81. Joske, “Hunting the Phoenix,” The Australian Strategic Policy Institute, 2020.
leverage their privileged access to acquire sensitive Japanese information and technology, which they then relay to the Ministry of State Security.\textsuperscript{82}

Japan’s response has been two-pronged: fostering better communication and coordination among government agencies and creating stricter visa requirements. In response to China’s growing economic regional power, for instance, the government established an Economic Statecraft Division within its National Security Secretariat in April 2020, with a mandate that includes protecting Japanese technologies.\textsuperscript{83} The move corrects a perceived shortfall of Japan’s previous RS strategy which was restrained to specific ministries controlling specific responses, leading to a generally disjointed approach.\textsuperscript{84} Japan also amended its Foreign Exchange and Foreign Trade Act to include regulations on foreign investments, curbing research espionage in sectors critical to Japan’s national security.\textsuperscript{85}

To counter espionage in higher education in particular, since 2019 Japan has launched a number of distinct measures. It strengthened visa processes; the Japanese foreign ministry requested ¥220 million to expand student visa evaluations with an emphasis on preventing technology theft. Japan also tightened restrictions on Japanese researchers who are identified to be under “strong influence of foreign governments.” Controversially, the label carries with it a requirement to gain a Ministry of Economy, Trade and Industry license to work with dual-use technologies.\textsuperscript{86} The government likewise approved an innovation strategy which obliges government agencies and research institutes to strengthen their guidelines around research integrity and conflicts of interest in order to prevent the outflow of technologies linked to national security. This is in conjunction with the planned increase of export controls on suspicious foreign research. The government also considered a proposal, also controversial, that would allow them to withhold funding to universities that fail to declare conflicts of interests and foreign partnerships.\textsuperscript{87} Finally, the Ministry of Economy, Trade and Industry established a project with a budget equivalent to C$17 million to help equip universities and small businesses with stronger frameworks better able to prevent the transfers of sensitive research and technology.\textsuperscript{88}

\textbf{Israel.} Israel’s approach to RS is an outlier among the four examples explored. Though a global leader in research—spending the highest proportion of GDP on R&D—it has staked a starkly different approach to RS than the US, Australia, and Japan.\textsuperscript{89} Israeli

\begin{itemize}
  \item \textsuperscript{82} Joske, “The company with Aussie roots that’s helping build China’s surveillance state.”
  \item \textsuperscript{83} Peter Fraioli, “Japan’s economic statecraft,” \textit{Strategic Comments} 26, no. 4 (2020): iv–vi.
  \item \textsuperscript{84} Mallapaty, “Japan considers tougher rules on research interference amid US-China tensions.”
  \item \textsuperscript{85} Devin Stewart, “China’s influence in Japan,” Center for Strategic & International Studies, July 2020.
  \item \textsuperscript{86} Suvendrini Kakuchi and Yojana Sharma, “Research security tightened with China threat in mind,” \textit{University World News}, June 2021.
  \item \textsuperscript{87} Mallapaty, “Japan considers tougher rules on research interference amid US-China tensions.”
  \item \textsuperscript{88} Osaki, “Japan boosts checks on Chinese students amid fears of campus spying.”
  \item \textsuperscript{89} World Economic Forum, “These countries spend the most on research and development,” 16 November 2020.
\end{itemize}
R&D is both a matter of existential national security and economic interest. Israel’s perception of geostrategic vulnerability has compelled it to invest massively in developing military, cyber, and defence capabilities that ensure national security. To that end, government and public entities are some the primary funders of R&D, providing financial support for well over half of the country’s research activities in advanced electronics, cybersecurity, pharmaceuticals, and medicine. Additionally, given its small size and domestic market, technological exports, which accounted for nearly 60 percent of Israeli manufactured exports in 2019, help ensure its economic prosperity.

Because research is paramount in Israel, it has favoured policies that encourage open science that pose few restrictions. Indeed, Israel has not adopted RS terminology; nor has it taken any extensive effort to safeguard its domestic research, other than in certain niches (like biosecurity). For the most part, the perceived economic benefits of OS have limited Israeli calls for the creation of a RS framework. And Israel does not openly perceive China as a significant threat to its research. Israel-China ties significantly expanded in 2013 when Prime Minister Benjamin Netanyahu welcomed and encouraged Chinese investment in the hopes of increasing economic and diplomatic ties between the two countries. Government resolutions, directives, and incentives were provided to various Israeli ministries to increase collaboration with Chinese entities. It is estimated that Chinese investments in Israel’s technology sector, including in dual-use technologies like AI and satellite communications, amounted to US$5.7 billion between 2011 and 2018. Additionally, Israel-China academic partnerships have expanded with new exchange programs and scholarships. Although Israeli and American national security organizations occasionally raise concerns about Israel’s encouragement of open collaboration, the government has, to date, largely avoided regulating its research sector in ways that might mitigate perceived Chinese challenges. Instead, the focus of Israeli RS is squarely placed on biosecurity and cybersecurity.

On biosecurity, Israel created the Regulation of Research into Biological Disease Agents Law (2008), with an eye on preventing biological terrorism and controlling dangerous pathogens. The framework is praised in RS literature as an effective tool to

90. Israel Ministry of Foreign Affairs, “SCIENCE AND TECHNOLOGY: Research and Development,” Government of Israel, 2013.
91. World Bank, “Medium and high-tech exports (% manufactured exports) – Israel,” accessed January 2022; Jarunee Wonglimpiyarat, “Government policies towards Israel’s high-tech powerhouse,” Technovation 52–52 (2016): 8–27.
92. Yoram Evron, “Between Beijin and Washington: Israel’s technology transfers to China,” Journal of East Asian Studies 13, no. 3 (2013): 503–528; Yossi Melman, “China is spying on Israel to steal U.S. secrets,” Foreign Policy, 24 March 2019.
93. Ivan Levingston, “U.S. scrutiny of Israel’s China ties expands to universities,” Bloomberg, 18 May 2020.
94. Shira Efron, Karen Schwindt, and Emily Haskel, Chinese Investment in Israeli Technology and Infrastructure: Security Implications for Israel and the United States (Santa Monica, CA: RAND Corporation, 2020).
mitigate challenges associated with research involving dual-use goods. This is due to the overarching centralization of relevant stakeholders to establish clear policy guidelines, as well as extensive engagement and oversight mechanisms within universities.\textsuperscript{95} The law requires that institutions using dangerous pathogens obtain approval from a council regulating research on disease pathogens, which may dictate terms to be respected throughout the research project. Approved projects must be reported to the General Manager of the Health Ministry, and researchers and institutions who do not follow the law may be subject to imprisonment and fines.\textsuperscript{96}

On cybersecurity, Israel has developed a vertically integrated cyber strategy which helps mitigate the impacts of cyberattacks, including those linked to IP theft and RS. The Ministry of Science and Technology cites the introduction of science and its accessibility to the research community as one of its primary goals.\textsuperscript{97} To achieve this objective, cybersecurity training is integrated into school and university curricula. Further, the government’s Nation Cyber Security Research Center Program established six cybersecurity research centres within universities, with a goal of ensuring multidisciplinary research.\textsuperscript{98} The Israel National Cyber Directorate (INCD) provides guidance, creates policies, and publishes reports and statements specific to cybersecurity. These reports are rather specific: they discuss trends in cyberattacks, name actors as potential threats, and provide detailed unclassified information about cyberattack methods. Furthermore, within the INCD, the Israeli Cyber Emergency Response Team (CERT) is staffed at all times to help civilians and organizations deal with cyber incidents. The CERT also raises awareness around preventive practices, ensures information sharing, issues public alerts, and develops new mechanisms for dealing with emerging threats. To carry out these various functions, it maintains working relationships with private companies, academia, other government organizations, as well as CERT sub-centres which provide support on sector-specific threats.\textsuperscript{99}

On China, as mentioned, Israel takes a notably laissez-faire approach. Policymakers have been primarily interested in the economic benefits Israel receives from partnering with China, rather than on the threats, and have largely disregarded warnings from the national security community. However, following extensive American pressure, increased criticism from Israeli intelligence, and the identification of Chinese

\textsuperscript{95} Lev and Rager-Zisman, “Protecting public health in the age of emerging infections.”
\textsuperscript{96} Ori Lev, “Regulating dual-use research: Lessons from Israel and the United States,” Journal of Biosafety and Biosecurity 1, no. 2 (2019): 80–85.
\textsuperscript{97} Ministry of Science and Technology, “About Ministry of Science and Technology,” Government of Israel, 25 July 2018, https://www.gov.il/en/departments/about/ministry_of_science_and_technology_about (accessed 18 July 2022).
\textsuperscript{98} Israel National Cyber Directorate, “Israel National Cyber Directorate,” Government of Israel, n.d., https://www.gov.il/en/departments/israel_national_cyber_directorate (accessed 11 July 2022).
\textsuperscript{99} Israel National Cyber Directorate, “The Israel National Cyber Directorate: Iran is a main cyber threat on the Middle East,” Government of Israel, 26 June 2019.
involvement in areas essential to Israeli national security, including in the energy, military, and transport sectors, the situation has recently garnered more attention. As a result, Israel announced the creation of a new mechanism for screening foreign investments, an advisory committee that assesses the national security implications of foreign involvement in certain sectors. Yet, the committee’s decisions are non-binding; they only assist regulators and provide opinions. Considering the extent of investment and involvement of China in different spheres of Israeli R&D, domestic RS strategies and policies—if and when they are developed or strengthened—will likely have to strike a careful balance between appeasing the US and not aggravating China.

Conclusion: The future of Canadian research security

By way of conclusion, this section draws a series of comparative lessons from the empirical analysis that might help inform Canada’s evolving and emerging approach to RS. International concern for and contemporary responses to RS among a subset of liberal democracies can be distilled into four key themes: centralization, collaboration, controls, and cybersecurity. What follows is an exploration of each theme as applied to the Canadian context.

Centralization. Without a designated authority for policy centralization, RS responses have traditionally been diffuse, disconnected, and inconsistently applied between various government departments and related stakeholders. In response, a process of RS centralization is currently taking place across each case. Although Israel does not interpret RS in the same way as the US, Australia, and Japan, its council for the regulation of research with disease pathogens has, nonetheless, been in use for years, offering an example of bringing together relevant departments over specific issues of concern. Centralization is built into that process. Similarly, Australia created the National Counter Foreign Interference Coordinator to oversee the government departments involved in RS policy development and response. And the US and Japan have also begun establishing centralized RS authorities tasked with policy harmonization, interdepartmental communication, and coordination, though they are still nascent.

Improving communication between government departments alone is not enough, however. The cases suggest a need for clear and effective communication with other non-government RS stakeholders. As discussed above, some Canadian universities have already voiced concern over confusing and conflicting RS requirements, calling for more government support and precise information on emerging threats and proper responses. To this end, the case studies reveal a concerted effort to foster better relationships with, and provide more direct guidance to, RS stakeholders. One model from the US entails integrating FBI liaisons at the local level, each tasked with working

100. Melman, “China is spying on Israel to steal U.S. secrets”; Efron et al., Chinese Investment in Israeli Technology and Infrastructure.
with specific institutions to identify threats and responses. Lessons therein are then fed back into the national strategy. Other models from Japan and Australia focus on providing federal training to institutes on preventing espionage and tech transfers and countering foreign influence. In all cases, when communicating with stakeholders, governments should clearly reiterate their commitment to the principles of OS and RS. By championing OS, governments help reinforce RS by securing academic and institutional buy-in, easing tensions with particular research communities, and improving relationships between researchers and authorities. Publicly expressing these ideas also demonstrates commitment to democratic values and OS at the international level, allowing countries to benefit from the continued flow of scientific cooperation, collaboration, and discovery. Finally, defining the guiding principles of OS will further ensure that regulators have a concrete reference point for RS policy development, ensuring that they, too, avoid over-securitizing research.

For Canada, next steps entail concretely centralizing its RS policy leadership within a designated authority—existing or newly established—allowing for better communication and outreach with stakeholders. This could include working with universities at the local level to address challenges specific to their institutions, as well as challenges facing universities and researchers writ large. This authority can likewise publicly outline Canada’s commitment to open science and to foreign researchers, positioning these commitments within the larger context of research security.

Collaboration. While overwhelmingly beneficial to the global scientific community, collaboration with foreign researchers, students, and research institutes has nonetheless emerged as a chief RS concern. Illustrations from the four cases abound, with particular attention paid to PLA-linked universities and talent recruitment programs. While some countries have reacted to this particular challenge with hardline (and even aggressive) responses, it is nonetheless important that Canada first debates and then finds the right balance between addressing the challenges of foreign collaboration and deriving benefit from it, which includes supporting OS, countering racism and stigmatization in research, and fostering innovation, excellence, and economic opportunities. From the case studies, we find a range of responses regarding foreign collaboration. America’s assertive approach includes better vetting of foreigners, changes to visa policies, cracking down on talent recruitment plans through the use of conflict-of-interest clauses, threats of sanctions, and entry bans. By contrast, Australia has been working with its universities to better recognize PLA-affiliated entities, while developing a culture of awareness about the potential risk of foreign collaboration. Japan’s approach, still under development, sits somewhere between these two poles. Only Israel stands as

101. Any centralized Canadian process will have to consider that Canadian university research is conducted in both official languages, and might, as a result, stem from two international academic communities involving different research partners from vastly different countries. RS solutions might need to be tailored to the particularities of these two communities. The authors thank an anonymous reviewer for this insight.
the outlier: it actively pursues collaboration with China despite American (and some domestic) protest.

Our research also illustrates the importance of competing considerations in developing an RS policy response to foreign collaboration. Of greatest importance, open science generates international collaboration which feeds scientific innovation. This is a good, in and of itself. Further, many universities are reliant on international tuition fees paid by foreign (mostly Chinese) students. Should vetting make it more difficult for foreign students to study abroad—a trend already taking shape—the effects will be largely felt on universities’ budgets and domestic tuition fees. And finally, RS responses must consider the real and/or perceived nature of racial bias unduly and unfairly targeting certain nationals. US Presidential Proclamation 10043, for illustration, has been strongly rebuked for its effect on Chinese students and researchers.102

Taken together, Canada must look to its own visa policies and processes to ensure they remain effective at deterring contemporary research theft. Canada should mitigate risks from foreign institutions with direct military ties by establishing lists of particular institutions of concern—as some Canadian allies have already done—and working with domestic stakeholders in developing a more nuanced review process when exploring collaborative opportunities with researchers who have active links to these institutions. And finally, Canada might draw from American and Australian efforts to foster a know-your-collaborator culture among domestic researchers, mitigating RS challenges at the frontline of collaboration.

Controls. Traditionally, export controls have entailed safeguarding the foreign transfer of goods that could be used in military settings, including weapons, dual-use technologies, nuclear capabilities, and other related goods. More recently, however, countries like Japan and the US have taken measures to broaden their export controls to protect economic interests or to altogether reframe them as national security concerns. But while these countries move towards securitizing their economies, civil society actors and researchers alike have become wary of this approach because it risks undermining OS, international collaboration, and the free flow of scientific information. Moreover, focusing on export controls may not be the most effective way to mitigate threats to research; ASPI has found that export control lists are not updated frequently enough to adapt to evolving technological developments. Furthermore, only rarely do countries deny export control applications; in 2019, for instance, Canada denied just 0.02 percent of applications.103 Export controls can, however, be used to regulate the transfer of goods, services, and technologies regardless of their means of delivery, including the electronic transfer of information. But the low rate of denial and the high

102. Kevin Bryan, “Chinese international students urge Penn to back their rebuke of Trump era visa suspensions,” The Daily Pennsylvanian, June 2021.
103. Canada denied one of the 6,260 applications in 2019. A total of five were denied that year, including applications carried over from previous years. Global Affairs Canada, “2019 Annual Report to Parliament on the Administration of the Export and Imports Permits Act,” Government of Canada, 2020.
volume of electronic transfers of information, especially in the context of COVID-19 research, demonstrates that it is unlikely that all researchers are applying for export control permits, even though they may be required to do so under evolving considerations. These issues are of particular concern when conducting research with dual-use technologies and goods. The definition of dual-use is generally too broad to be of much operational utility. Israel’s case highlights, for example, a blurring between technology that is of purely civilian use and technology that may have military or security applications. Given the flexible and evolving definition and scope of dual-use, researchers may be working with these technologies without being aware of it.

While export controls should not function as the primary mechanism for contemporary RS, they can and do have a supporting role. Accordingly, Canada should conduct an analysis regarding the impacts of broadening its export controls to other sectors considered integral to Canada’s economic security. Additionally, the creation of a standing committee with relevant technological expertise, perhaps built along the lines of Israel’s lauded council for the regulation of research with disease pathogens, could be established to support the evolving decision-making process as to what goods and technologies should be included in export controls. The committee could likewise assist in the development of clear guidelines for researchers working with dual-use technologies. Finally, Canada might consider further emulating Israel’s council by establishing a centralized body and requiring universities to create institutional committees which regularly review projects in military and dual-use areas. This will ensure better regulation of dual-use technology and support universities and researchers.

**Cybersecurity.** Many governments, Canada’s included, have taken recent measures to raise public awareness about the linkages between cybersecurity and RS. However, researchers’ interest in, and concern for, cybersecurity remain thin; British studies have found that hackers were able to obtain high-value data from university researchers with just 2 hours of effort, and that human error remains a key determinant of data breaches.\(^{104}\) For contemporary RS, ensuring relevant stakeholders buy into cybersecurity is critical. Crafting an effective cybersecurity strategy to protect research will require a flexible and engaging approach in which researchers are compelled to better ensure the protection of their information. The Israeli case study provides interesting insights on this theme, as it promotes a whole-of-society resilience to cyberattacks. The vertically integrated strategy wherein the government continuously reiterates its commitment to cybersecurity contributes to increased public awareness and ensures that the general population—including targeted researchers—has a high level of technological literacy. The CERT provides direct support to civilians who are suspected to have been the victim of a cyberattack. It also provides tools and resources to civilians to help them address potential cyber threats directly.

\(^{104}\) Sean Coughlan, “Hackers beat university cyber-defences in 2 hours,” BBC, 4 April 2019; Michael Hill, “90% of UK data breaches due to human error in 2019,” *InfoSecurity*, 6 February 2020.
Canada should continue to work with universities to develop cybersecurity training that resonates with researchers; universities might consider making cybersecurity training mandatory for all publicly funded researchers, as they already do with other forms of training (e.g., research ethics, physical safety, and mental health). Researchers working on subjects that are particularly threatened by RS should be tested frequently on their knowledge and compliance with cybersecurity best practices. Canada’s Cyber Centre might likewise increase the support it provides directly to researchers (and civilians more broadly) who have been, or suspect they have been, the victim of a cyberattack. Moreover, the government as a whole could provide direct cybersecurity support to universities and research institutions, including by circulating timely and tailored information about specific threat actors, the means they employ, and the targets they may be after, in order to better augment RS and cybersecurity awareness among researchers. Finally, Canada should conduct continual network penetration operations, similar to those conducted in the UK, to identify weaknesses in cyber infrastructure and raise awareness among at-risk actors.

Declaration of conflicting interests
The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding
The author(s) received no financial support for the research, authorship, and/or publication of this article.

ORCID iD
Alex Wilner https://orcid.org/0000-0003-2087-252X

Author Biographies
Dr. Alex Wilner is an associate professor at the Norman Paterson School of International Affairs (NPSIA), Carleton University, Canada. His books include Deterring Rational Fanatics (University of Pennsylvania Press, 2015), Deterring Terrorism: Theory and Practice (editor; Stanford University Press, 2012), and Deterrence by Denial: Theory and Practice (editor; Cambria Press, 2021).

Ms. Sarah Beach-Vaive is a graduate of the Norman Paterson School of International Affairs’ MA program. She was part of the 2021 Capstone cluster that helped produce the article.

Ms. Catherine Carbonneau is a graduate of the Norman Paterson School of International Affairs’ MA program. She was part of the 2021 Capstone cluster that helped produce the article.
Mr. Graeme Hopkins is a graduate of the Norman Paterson School of International Affairs’ MA program. He was part of the 2021 Capstone cluster that helped produce the article.

Mr. Félix Leblanc is a graduate of the Norman Paterson School of International Affairs’ MA program. He was part of the 2021 Capstone cluster that helped produce the article.