

# National Security Concerns Require Stricter Screening of PRC Students

Sergio R. Karas

Canada is a target of espionage by the People's Republic of China, and the study permits granted to many PRC students appear to be one gateway used by the Chinese authorities to accomplish their apparent goals, taking advantage of lax security screening by Canadian visa officers and their security apparatus' ability to pressure and force collaboration by Chinese students abroad.

According to an article published by *The Walrus* on June 4, 2024, since the early 1970s, Canada has welcomed academic exchanges with the People's Republic of China (PRC), particularly encouraging Chinese students to pursue studies in science and technology at Canadian universities. This was viewed as a goodwill gesture, an opportunity to contribute to China's economic and industrial development through access to advanced knowledge and training. In return, Canadian students in China immersed themselves in language, culture, and political studies, including the study of Maoism. For decades, this mutually beneficial arrangement appeared benign. However, by the early 2000s, a strategic shift emerged. China's People's Liberation Army (PLA), amid a push for rapid military modernization, began exploiting these academic pathways to advance its goals.

The Australian Strategic Policy Institute (ASPI) explained in an article called "Picking flowers, making honey" published on October 30, 2018, that under a covert program dubbed "picking flowers in foreign lands to make honey in China,"<sup>1</sup> PLA engineers and scientists, primarily from the National University of Defense Technology (NUDT) and six other military institutions, began concealing their military affiliations to infiltrate Canadian postgraduate research programs.<sup>2</sup> This marked a turning point, transforming educational

collaboration into a potential vector for state-sponsored espionage. As the number of PRC students admitted to Canadian universities increased, and reports of industrial espionage became more widely known, there was no corresponding increase in security vetting of PRC students, and applications were approved in large numbers as students were seen as a good source of funds for Canadian educational institutions.

A 2018 paper by the International Cyber Policy Centre in Australia states that Canada is the third most targeted country by PLA military scientists, after the United States and the United Kingdom.<sup>3</sup> A study by United States intelligence company Strider Technologies, quoted by the *Globe and Mail* in January 2023, found that the Chinese military successfully targeted 50 Canadian universities.<sup>4</sup> Strider reported that the University of Waterloo had the most collaborations, whether intentional or not, with NUDT. Other Canadian universities on the list include the University of British Columbia, Simon Fraser University, the University of Victoria, McMaster University, Concordia University, and the University of Calgary. In total, researchers from the top ten Canadian universities co-authored 240 papers with Chinese military scientists over the past five years.<sup>5</sup> These worrisome reports seem to have been ignored by Immigration, Refugees and Citizenship Canada (IRCC) when reviewing visa applications.

As of October 2024, there were approximately 50,785 students from the PRC in Canada on study permits.<sup>6</sup> In December 2023, the Federal Court refused a study permit for Yuekang Li, a Chinese PhD student accepted into the University of Waterloo. The court held that his research in microfluidics, a technology with both health

<sup>1</sup> Alex Joske, "Picking flowers, making honey – The Chinese military's collaboration with foreign universities", (Oct 30, 2018), online: Australian Strategic Policy Institute

<https://www.aspi.org.au/report/picking-flowers-making-honey/> ASPI

<sup>2</sup> Jonathan Manthorpe, "Canada's Universities Are a Pipeline for Chinese Military Technology", (Jun 4, 2024), online: *The Walrus* <https://thewalrus.ca/canadas-universities-are-a-pipeline-for-chinese-military-technology/>

<sup>3</sup> Jonathan Manthorpe, *Canada's Universities Are a Pipeline for Chinese Military Technology*, *The Walrus* (2024), supra note 1.

<sup>4</sup> Robert Fife and Steven Chase "Canadian universities conducting joint research with Chinese military scientists", (Jan 30, 2023), online: *The Globe and Mail* <https://www.theglobeandmail.com/politics/article-chinese-military-scientists-canadian-universities/>

<sup>5</sup> *Ibid*

<sup>6</sup> "Number of Chinese Students in Canada: 2015-2024", online: AMCAIM <https://amcaim.ca/number-of-chinese-student-in-canada-2015-2024/>

and military uses, could pose a national security risk.<sup>7</sup> Officials said Li's ties to a university connected to China's military made it possible that he could be used by the Chinese government to gather sensitive information. This decision sounds the alarm about the risk of espionage through academic research in Canada. Still, there appears to have been no concerted effort by IRCC to increase security screening of PRC Study Permit applicants.

In 2020, the U.S. expanded its blacklist of people linked to China's NUDT by denying academic visas to those suspected of trying to steal research with military value.<sup>8</sup> A report by the Canadian Security Intelligence Service (CSIS), dated December 21, 2021, revealed that after these visa restrictions, Chinese scholarship students coming to countries like the United States, Canada, the UK, and Australia began hiding their ties to the military. They also masked the true nature of their research when applying for visas. Instead of choosing to work in fields that can be linked to the Chinese military when studying at Canadian universities, they chose areas that seem harmless but still have strong military applications.<sup>9</sup>

In a May 2025 interview, Gordon G. Chang, a senior fellow at the Gatestone Institute, warned that Chinese diplomatic and intelligence agents are operating covertly on Western campuses.<sup>10</sup> He highlighted a troubling incident at Stanford University where Chinese Communist Party (CCP) agents posed as students to gain access to sensitive research.<sup>11</sup> Chang stated that "Chinese consular officials have been coercing Chinese students to steal data," and that agents from China's Ministry of State Security are also involved in stealing intellectual property. He stressed that such covert activities are widespread, saying, "This is going on every place where there is valuable intellectual property for

China to steal." Chang called for a stronger response from Western governments, including expelling these agents, imposing serious consequences on Beijing, and addressing the long-standing negligence of Western leadership in confronting these threats.<sup>12</sup>

According to a May 2025 investigation by The Stanford Review, the CCP was running a covert intelligence-gathering campaign at Stanford University.<sup>13</sup> It shows a presumed CCP agent, under the alias "Charles Chen," posing as a student to befriend individuals and conducting research related to China. He reportedly used trusted platforms like WeChat and coached his targets on travel to China to avoid visa scrutiny. The investigation strongly suggested that Chen was linked to China's Ministry of State Security. Interviewees, including faculty and students, described a sophisticated operation involving loyalty tests, coercion, peer surveillance, and threats to students' families if they refused to comply. The investigation concluded that there was a broad pattern of espionage through academic channels, and high-tech institutions are prime targets for state-sponsored intelligence collection.<sup>14</sup> The Chinese Scholarship Council (CSC), which funds an estimated 18 percent of Chinese students<sup>15</sup> at American universities, is regarded as a primary avenue of information gathering. China experts speaking anonymously confirmed that it requires students to regularly submit "Situation Reports" to Chinese diplomatic missions about their research.<sup>16</sup> Canadian authorities seem oblivious to this issue and have apparently not taken any steps to address the potential ramifications of this problem.

Most recently, in June 2025, two Chinese nationals, Yunqing Jian and Zunyong Liu, were charged by U.S. authorities for allegedly smuggling a dangerous biological pathogen into the United States.<sup>17</sup> Liu

<sup>7</sup> "Court decision barring Chinese student sends message about espionage risk, experts say", (January 19, 2024), online: *The Mackenzie Institute* <https://mackenzieinstitute.com/2024/01/court-decision-barring-chinese-student-sends-message-about-espionage-risk-experts-say/>

<sup>8</sup> Jonathan Manthorpe, *Canada's Universities Are a Pipeline for Chinese Military Technology*, *The Walrus* (2024), supra note 1

<sup>9</sup> Ibid

<sup>10</sup> Corey Olson, "Spy Studies: Chinese Agents Pose as College Students", (May 9, 2025), online: *1190 Talk Radio – iHeart* <https://1190talkradio.iheart.com/content/2025-05-09-spy-studies-chinese-agents-pose-as-college-students/?utm>

<sup>11</sup> Ibid

<sup>12</sup> Gatestone Institute senior fellow Gordon Chang, "China 'weaponized' students attending school on US soil, expert argues", (May 31, 2025), online: *Fox News* <https://www.foxnews.com/video/6373720704112?utm>

<sup>13</sup> Garret Molloy & Elsa Johnson, "INVESTIGATION: Uncovering Chinese Academic Espionage at Stanford", (May 7, 2025), online: *The Stanford Review* <https://stanfordreview.org/investigation-uncovering-chinese-academic-espionage-at-stanford/>

<sup>14</sup> Ibid

<sup>15</sup> Ryan Fedasiuk, "The China Scholarship Council: An Overview", (July 2020), online: *Center for Security and Emerging Technology*, (July 2020), online: CSET Issue Brief <https://cset.georgetown.edu/wp-content/uploads/China-Scholarship-Council-Overview.pdf?ref=stanfordreview.org>

<sup>16</sup> Garret Molloy & Elsa Johnson, "INVESTIGATION: Uncovering Chinese Academic Espionage at Stanford", online: *The Stanford Review*, supra note 14

<sup>17</sup> Taylor Romline, Andy Rose & Josh Campbell "2 Chinese researchers are charged with smuggling biological pathogen to study at University of Michigan lab", (June 4, 2025), online: *CNN* <https://www.cnn.com/2025/06/04/us/chinese-researchers-smuggle-pathogen-university-of-michigan>

attempted to bring the pathogen through Detroit Metro Airport in July 2024, and Jian, who was affiliated with the University of Michigan and funded by the Chinese government, intended to conduct unauthorized research using the university's lab. Both individuals are facing serious charges, including conspiracy, smuggling, visa fraud, and making false statements. This case has raised serious concerns about foreign researchers misusing access to sensitive scientific facilities.<sup>18</sup> The PRC has enacted legislation that allows its government to require Chinese citizens living in other countries to help with intelligence gathering and operations. Under the 2017 National Intelligence Law, all Chinese citizens and organizations must support and cooperate with China's intelligence agencies if asked and keep any related information secret. This applies no matter where the person lives.<sup>19</sup> Other legislation, including the Data Security Law (2021) and Counterespionage Law (2023), also extends these duties to citizens and companies abroad. This gives the Chinese authorities the power to demand information or assistance from Chinese nationals overseas and even punish them for actions taken outside China.<sup>20</sup> According to an independent, nonprofit research and analysis organization, CNA, the Chinese authorities can go to great lengths enforcing their requests for cooperation, even pressuring Chinese citizens living abroad by threatening their family members still in China.<sup>21</sup>

This broad extraterritorial reach of Chinese intelligence laws casts a troubling light on the growing presence of Chinese companies like Huawei in Canadian research institutions. Whether the sponsorship of research at Canadian universities by Huawei Technologies qualifies as a military incursion is a matter of interpretation. The company's investment, in 2019, of close to \$60 million in research in Canadian laboratories, was seen as a major security issue. In the previous five years, Huawei had established research relationships with seventeen Canadian universities. The money

involved in each deal ranged from tens of thousands of dollars to many millions. The University of Waterloo alone received over \$15 million from Huawei over the previous five years to fund sixteen projects. In addition to using Canadian laboratories and researchers to develop new technologies, for which the company kept the patents, Huawei had sold network equipment to wireless carriers like Bell and Telus.<sup>22</sup> These forays into Canadian academia by the PRC's military and electronic espionage agents may not have occurred if the Canadian government had issued clear warnings about the threat they pose to the country's security.<sup>23</sup> It is difficult to understand why Canada has not increased security screening of PRC students, given these concerns.

Australia, the United States, and the United Kingdom have implemented significant measures to safeguard their research ecosystems and technology sectors in response to concerns over foreign influence and acquisition of sensitive technology, particularly by China. Australia's Foreign Relations Act 2020<sup>24</sup> gives its government the power to review or terminate university agreements with certain foreign entities to safeguard the national interest; the United States has imposed visa restrictions on students from organizations linked to China<sup>25</sup>, and the United Kingdom's National Security and Investment Act<sup>26</sup> lets the government block or reverse sensitive tech and research investments on security grounds. These efforts illustrate an international move towards increased transparency and targeted risk management, aiming to protect national security while upholding academic freedom, human rights, and due process.

Canada has recently begun to follow suit by adopting a suite of new legislation and policies aimed at strengthening research security and transparency; however, that does not impact the selection of PRC students abroad. In June 2024, Parliament passed Bill C-70, the Foreign Influence Transparency and Accountability Act (FITAA)<sup>27</sup>, requiring individuals and

<sup>18</sup> Ibid

<sup>19</sup> "China's National Security Laws: Implications Beyond Borders", (2023), online: CNA <https://www.cna.org/quick-looks/2023/China-national-security-laws-implications-beyond-borders.pdf>

<sup>20</sup> Ibid

<sup>21</sup> Ibid

<sup>22</sup> Jonathan Manthorpe, *Canada's Universities Are a Pipeline for Chinese Military Technology*, *The Walrus* (2024), supra note 1

<sup>23</sup> Ibid

<sup>24</sup> Australia's Foreign Relations (State And Territory Arrangements) Act 2020 "Fact Sheet 1 – Overview", (2021), online: Australian Government — Foreign Arrangements Scheme / Department of

Foreign Affairs and Trade

<https://www.foreignarrangements.gov.au/sites/default/files/2021-02/Fact%20Sheet%201%20-%20Overview%20.pdf>

<sup>25</sup> "Marco Rubio says U.S. to begin revoking visas of some Chinese students", (May 28, 2025), online: CBC News

<https://www.cbc.ca/news/world/us-student-visas-china-1.7546589>

<sup>26</sup> "National Security and Investment Act – 2021, online: UK

Government <https://www.gov.uk/government/collections/national-security-and-investment-act#:~:text=The%20NSI%20Act%20gives%20the,do%20business%20in%20the%20UK.>

<sup>27</sup> <https://lois.justice.gc.ca/eng/acts/F-29.2/FullText.html>

organizations to register arrangements with foreign principals that involve political or public communication activities<sup>28</sup>. This legislation imposes strict timelines and penalties for non-compliance. Alongside this, the May 2024 Policy on Sensitive Technology Research and Affiliations of Concern<sup>29</sup> prohibits federally funded research collaborations with entities affiliated with foreign military or national security bodies, particularly in areas such as AI, quantum computing, and aerospace. These efforts are supported by the National Security Guidelines for Research Partnerships (NSGRP)<sup>30</sup>, which mandate risk assessments for high-risk collaborations and encourage intelligence sharing between the federal government and academic institutions. These frameworks signal Canada's growing recognition of the need to protect its innovation and academic sectors from covert foreign influence, but it is difficult to explain why IRCC has not increased vetting of PRC students to ensure that they have no ties to state organizations involved with the Chinese military or suspected of espionage, or why it has not required universities to restrict access to PRC students wishing to enter fields of research that may have military use, or may involve sensitive intellectual property.

Canada immigration is not currently implementing sufficient safeguards to prevent foreign students from using study permits as cover for nefarious activities or from being forced to spy for foreign governments. To ensure national security while maintaining openness to international students, several important steps should be taken. Security screening by Immigration, Refugees and Citizenship Canada (IRCC) should increase and deepen background checks, especially for students applying to sensitive programs that can have military applications, like engineering, computer science, and advanced technologies. Applicants who show signs of risk, such as ties to military or government organizations, or work in sensitive research, or have family connections to state entities, should undergo enhanced security screening. The use of predictive analysis and algorithms can help flag such cases. A case-by-case assessment approach should remain in place to ensure accuracy and fairness in decision-making. Educational institutions must comply with mandatory reporting requirements, confirming that

students are actively enrolled and meeting the conditions of their study permits, and ensuring that their facilities are not used to conduct unauthorized research. While there are no official country-specific restrictions, it is important to apply heightened scrutiny to applicants from high-risk countries and strategic adversaries like China, due to growing concerns over intellectual property theft, espionage, and national security.

---

Sergio R. Karas, principal of Karas Immigration Law Professional Corporation, is a certified specialist in Canadian Citizenship and Immigration Law by the Law Society of Ontario. He is Division Chair of the ABA International Law Section, past chair of the Ontario Bar Association Citizenship and Immigration Section, past chair of the International Bar Association Immigration and Nationality Committee, and a fellow of the American Bar Foundation. He can be reached at [karas@karas.ca](mailto:karas@karas.ca). The author is grateful for the contribution to this article by Jhanvi Katariya, student-at-law.

<sup>28</sup> Ethan Barkley, "Canadian universities raise concerns over foreign influence registry", (June 27, 2024), online: *The Martlet* <https://martlet.ca/canadian-universities-raise-concerns-over-foreign-influence-registry/>

<sup>29</sup> "Policy – Sensitive Technology Research and Affiliations of Concern", online: Government of Canada — Science & Innovation

(Science.gc.ca) <https://science.gc.ca/site/science/en/safeguarding-your-research/guidelines-and-tools-implement-research-security/sensitive-technology-research-and-affiliations-concern/policy-sensitive-technology-research-and-affiliations-concern>

<sup>30</sup> Ibid