HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

THE SECURITY OF RESEARCH PARTNERSHIPS BETWEEN CANADIAN UNIVERSITIES, RESEARCH INSTITUTIONS AND ENTITIES CONNECTED TO THE PEOPLE'S REPUBLIC OF CHINA

Report of the Standing Committee on Science and Research

Lloyd Longfield, Chair

MAY 2024
44th PARLIAMENT, 1st SESSION

THE SECURITY OF RESEARCH PARTNERSHIPS BETWEEN CANADIAN UNIVERSITIES, RESEARCH INSTITUTIONS AND ENTITIES CONNECTED TO THE PEOPLE'S REPUBLIC OF CHINA

Report of the Standing Committee on Science and Research

Lloyd Longfield
Chair

MAY 2024

44th PARLIAMENT, 1st SESSION

NOTICE TO READER

Reports from committees presented to the House of Commons

Presenting a report to the House is the way a committee makes public its findings and recommendations on a particular topic. Substantive reports on a subject-matter study usually contain a synopsis of the testimony heard, the recommendations made by the committee, as well as the reasons for those recommendations.

STANDING COMMITTEE ON SCIENCE AND RESEARCH

CHAIR

Lloyd Longfield

VICE-CHAIRS

Corey Tochor

Maxime Blanchette-Joncas

MEMBERS

Valerie Bradford

Richard Cannings

Lena Metlege Diab

Hon. Helena Jaczek

Arielle Kayabaga

Ben Lobb

Hon. Michelle Rempel Garner

Gerald Soroka

Ryan Turnbull

OTHER MEMBERS OF PARLIAMENT WHO PARTICIPATED

Shafqat Ali

Blaine Calkins

Chad Collins

Michael Cooper

Michael Coteau

Anju Dhillon

Stephen Ellis

Darren Fisher

Lori Idlout

Gord Johns

Marie-France Lalonde

Hon. David Lametti
Stéphane Lauzon
Ron Liepert
Wayne Long
James Maloney
Larry Maguire
Dan Mazier
Ken McDonald
Hon. John McKay
Eric Melillo
Rick Perkins
Charles Sousa

CLERKS OF THE COMMITTEE

Philip den Ouden
Hilary Smyth

LIBRARY OF PARLIAMENT

Research and Education

Kelsey Brennan, Analyst
Grégoire Gayard, Analyst

THE STANDING COMMITTEE ON SCIENCE AND RESEARCH

has the honour to present its

TENTH REPORT

Pursuant to its mandate under Standing Order 108(3)(i), the committee has studied the use of federal government research and development grants, funds, and contributions by Canadian universities and research institutions in partnerships with entities connected to the People's Republic of China and has agreed to report the following:

TABLE OF CONTENTS

SUMMARY

Scientific research is collaborative by its very nature. An increase in international exchanges and research partnerships has led to major advances for Canadian science. However, the internationalization of research is not without risk. Some foreign powers seek to take advantage of scientific research conducted in Canada. The actions of certain countries, including the People's Republic of China, constitute a threat for research security and national security in Canada.

Certain research areas are particularly sensitive, as they may have military applications. Some foreign powers seek to take advantage of research partnerships with scientists from Canada to acquire knowledge in these sensitive areas. International research partnerships may also result in intellectual property being transferred to other countries, either legally or illegally. Foreign interference within universities and on campuses is another growing threat.

While these threats do not all come from a single country, witnesses said that the People's Republic of China is the most active nation in this regard. As a result, the House of Commons Standing Committee on Science and Research carried out a study on the use of federal government research and development grants, funds, and contributions by Canadian universities and research institutions in partnerships with entities connected to the People's Republic of China.

The witnesses who appeared before the Committee provided an update on the issue of research security in Canada and on the threats faced by research stakeholders. The Committee considered measures taken by other countries, the role of universities, and initiatives taken by the federal government. In particular, the Committee examined the National Security Guidelines for Research Partnerships published in 2021 and their implementation.

The testimony on which this report is based was given before the 16 January 2024 announcement by the Government of Canada of new measures to safeguard research, including a Policy on Sensitive Technology Research and Affiliations of Concern, supported by the publication of a list of sensitive technology research areas and a list of named research organizations. However, the evidence provided by the witnesses remains very relevant. It sheds light on research security in Canada and what threatens it. The evidence also highlights the concerns of stakeholders in the research ecosystem with regard to these threats. Lastly, the evidence helps clarify the government's approach to this topic.

Based on the evidence compiled, the Committee made eight recommendations to the Government of Canada.

LIST OF RECOMMENDATIONS

As a result of their deliberations committees may make recommendations which they include in their reports for the consideration of the House of Commons or the Government. Recommendations related to this study are listed below.

HOUSE OF COMMONS
CHAMBRE DES COMMUNES
CANADA

THE SECURITY OF RESEARCH PARTNERSHIPS BETWEEN CANADIAN UNIVERSITIES, RESEARCH INSTITUTIONS AND ENTITIES CONNECTED TO THE PEOPLE'S REPUBLIC OF CHINA

INTRODUCTION

On 6 June 2023, the House of Commons Standing Committee on Science and Research (the Committee) adopted the following motion:

> That, pursuant to Standing Order 108(3)(i), the committee study the use of federal government research and development grants, funds, and contributions by Canadian universities and research institutions in partnerships with entities connected to the People's Republic of China, in areas including, but not limited to:
>
> - photonics,
> - artificial intelligence,
> - quantum theory,
> - biopharmaceuticals,
> - aerospace; and
>
> including but not limited to, intellectual property transfers and developments with Huawei Technologies and the National University of Defense Technology; that the committee hear from the director of the Canadian Security Intelligence Service, the Minister of Innovation, Science and Industry, department officials, top research officials from Canadian universities, the federal granting agencies, and any other witnesses deemed relevant to the study; that the committee allocate a minimum of four full meetings to this study; that the committee begin the study on June 20; the committee split the meetings for this study with the

> study of Long-term Impacts of Pay Gaps Experienced by Different Genders and Equity-seeking Groups Among Faculty at Canadian Universities, with this study being dedicated in the first hour; that the committee report its findings to the House; and that, pursuant to Standing Order 109, the committee request the government table a comprehensive response to the report.[1]

With contributions from both witness testimony and written briefs, the Committee's study addressed the threats that affect research security in Canada and mitigation measures. The Committee focused on knowledge and technology transfers in sensitive research areas; intellectual property transfer; and attempts to influence and interfere with the research community.

Although this study focuses on China, several witnesses said that these threats are not restricted to one nation.[2] Russia, Iran and North Korea were also mentioned by witnesses.[3] For instance, Sami Khoury, Head of the Canadian Centre for Cyber Security, said that the state-sponsored cyber-programs of China, Russia, Iran and North Korea continue to pose the greatest strategic cyber-threats to Canada.[4]

However, the Committee heard that China is the main threat in terms of research security. David Vigneault, Director of the Canadian Security Intelligence Service (CSIS), explained that the People's Republic of China (PRC) "is by far the greatest perpetrator of these activities."[5] He added that "the PRC, in the context of a threat to our economic

---

1 House of Commons Standing Committee on Science and Research (SRSR), *Minutes of Proceedings*, 6 June 2023.

2 SRSR, *Evidence*, 20 June 2023, 1110 (Jim Hinton, Intellectual Property Lawyer, As an Individual); SRSR, *Evidence*, 20 September 2023, 1635 (Cherie Wong, Executive Director, Alliance Canada Hong Kong); SRSR, *Evidence*, 4 October 2023, 1640 (Kevin Gamache, Associate Vice Chancellor and Chief Research Security Officer, Texas A&M University System Research Security Office); and SRSR, *Evidence*, 23 October 2023, 1625 (Nicole Giles, Senior Assistant Deputy Minister, Policy and Strategic Partnerships, Canadian Security Intelligence Service).

3 For example, SRSR, *Evidence*, 20 June 2023, 1105 (Christian Leuprecht, Professor, Royal Military College of Canada, As an Individual); SRSR, *Evidence*, 20 June 2023, 1120 (Jim Hinton); and SRSR, *Evidence*, 20 September 2023, 1650 (Gordon Houlden, Professor and Director Emeritus, University of Alberta – China Institute).

4 SRSR, *Evidence*, 23 October 2023, 1555 (Sami Khoury, Head, Canadian Centre for Cyber Security, Communications Security Establishment).

5 SRSR, *Evidence*, 22 November 2023, 1635 (David Vigneault, Director, Canadian Security Intelligence Service).

security and research security, is by far the most sophisticated actor that we're dealing with."[6]

As part of this study, the Committee held nine meetings between June and November 2023, during which it heard 32 witnesses. It also received eight written submissions. The Committee would like to thank those who appeared as witnesses and those who submitted briefs for their contributions to the study.

The Committee notes that all the evidence on which this report is based was given before the announcement made on 16 January 2024 by the Government of Canada on new measures to protect research.[7] These measures include implementing a new Policy on Sensitive Technology Research and Affiliations of Concern, launching the Research Security Centre, which was announced in Budget 2022, and investing close to $50 million to support post-secondary institutions through the Research Support Fund (RSF).

In support of the Policy on Sensitive Technology Research and Affiliations of Concern, the government published a list of sensitive technology research areas and a list of named research organizations.[8] Under this new policy,

> research grant and funding applications submitted by a university or affiliated research institution to the federal granting councils and the Canada Foundation for Innovation involving research that advances a sensitive technology research area will not be funded if any of the researchers involved in activities supported by the grant are affiliated with, or in receipt of funding or in-kind support, from a university, research institute or laboratory connected to military, national defence, or state security entities that could pose a risk to Canada's national security. To support this, Canada is releasing two lists that provide clear, defined, and transparent guidance so that researchers can quickly and efficiently determine if these new requirements apply to their research.[9]

These measures reinforce the National Security Guidelines for Research Partnerships, which were published in 2021 and are described later in this report.

Even though the evidence discussed in this report was given before these announcements were made, it still offers a wealth of insight. The evidence sheds light on

---

6 Ibid.

7 Government of Canada, *Statement from Minister Champagne, Minister Holland and Minister LeBlanc on new measures to protect Canadian research*, News release, 16 January 2024.

8 See: Government of Canada, *Policy on Sensitive Technology Research and Affiliations of Concern*; Government of Canada, *Sensitive Technology Research Areas*; and Government of Canada, *Named Research Organizations*.

9 Government of Canada, *Policy on Sensitive Technology Research and Affiliations of Concern*.

research security in Canada and what threatens it. The evidence also highlights the concerns of stakeholders in the research ecosystem with regard to these threats. Lastly, the evidence helps clarify the government's approach to this topic. Therefore, this report is complementary to the measures announced in January 2024. The lessons learned from the evidence can provide guidance to the government on the best way to implement research protection measures.

Based on the evidence compiled, the Committee made eight recommendations to the Government of Canada.

CHAPTER 1. CURRENT SITUATION

Although scientific research benefits from exchanges and partnerships with researchers from other countries, the evidence highlighted the importance of adequately protecting research output from strategies employed by certain countries, including China.

1.1 The Importance of International Research Partnerships

A number of witnesses mentioned the importance of international exchanges in the context of scientific research. Kevin Gamache, Associate Vice Chancellor and Chief Research Security Officer at Texas A&M University System's Research Security Office, told the Committee that research "is based on free and open collaboration and the exchange of ideas. It is based upon reciprocity. It's based upon transparency."[10] Philip Landon, Interim President and Chief Operating Officer of Universities Canada, explained as follows:

> International research collaboration is essential for Canada to remain competitive on the world stage. It fosters the exchange of ideas, talent and resources for the benefit of all concerned. Research and technology transfers work both ways, and Canadian research benefits greatly from building on progress being made elsewhere in the world.[11]

10 SRSR, *Evidence*, 4 October 2023, 1725 (Kevin Gamache).

11 SRSR, *Evidence*, 27 September 2023, 1635 (Philip Landon, Interim President and Chief Operating Officer, Universities Canada).

Several other witnesses held similar views.[12] In particular, witnesses noted that Canada can benefit from research partnerships with China.[13]

Chad Gaffield, the Chief Executive Officer of the U15 Group of Canadian Research Universities, explained that "successive federal governments had strongly encouraged Canada's universities to increase international collaboration, especially with China,"[14] for two key reasons:

> On the one hand, Canada sought to benefit from China's scientific and research expertise. On the other hand, Canada saw international collaboration as a way to tackle the world's complex challenges, such as those related to climate change and health.[15]

1.2 Threats Affecting Research Security

Although international scientific collaboration may yield benefits, witnesses highlighted that it is not without risk and that anyone engaging in such collaboration must remain vigilant.[16] According to Chad Gaffield, "globalization and internationalization can also threaten research security and, therefore, national security, by opening the door to foreign interference. Over recent years, universities have responded to a range of emerging threats."[17]

---

12 SRSR, *Evidence*, 4 October 2023, 1640 (Kevin Gamache); SRSR, *Evidence*, 25 October 2023, 1705 (Christian Baron, Vice-President, Research – Programs, Canadian Institutes of Health Research); Alliance Canada Hong Kong, *Written Submission to the Standing Committee on Science and Research (SRSR)*, September 2023, p. 6; and Government of Ontario, *Use of Federal Government Research and Development Grants, Funds, and Contributions by Canadian Universities and Research Institutions in Partnerships With Entities Connected to the People's Republic of China*, Brief submitted to the House of Commons Standing Committee on Science and Research, 6 October 2023, p. 1.

13 SRSR, *Evidence*, 25 October 2023, 1710 (Ted Hewitt, President, Social Sciences and Humanities Research Council); and SRSR, *Evidence*, 20 September 2023, 1650 (Gordon Houlden).

14 SRSR, *Evidence*, 27 September 2023, 1645 (Chad Gaffield, Chief Executive Officer, U15 Group of Canadian Research Universities).

15 Ibid.

16 For example, SRSR, *Evidence*, 27 September 2023, 1635 (Philip Landon); SRSR, *Evidence*, 25 October 2023, 1705 (Christian Baron); SRSR, *Evidence*, 22 November 2023, 1630 (David Vigneault); and Government of Ontario, *Use of Federal Government Research and Development Grants, Funds, and Contributions by Canadian Universities and Research Institutions in Partnerships With Entities Connected to the People's Republic of China*, Brief submitted to the House of Commons Standing Committee on Science and Research, 6 October 2023, p. 3.

17 SRSR, *Evidence*, 27 September 2023, 1645 (Chad Gaffield).

Christian Leuprecht, a professor at the Royal Military College of Canada, appearing as an individual, made the following observation:

> Tax dollars, public research funding and public universities have for years been leveraged systematically to support and enable research and to use technology that benefits hostile authoritarian states that seem to undermine Canada's democratic institutions, electoral processes, economic prosperity, national security and fundamental values, as well as international multilateral institutions and so forth.[18]

Witness testimony informed the Committee about the various types of threats that affect research.

The first threat involves sensitive research areas. Witnesses revealed that some areas of research are particularly sensitive because the technologies associated with them could have strategic importance, especially for military use. Dual-use technologies have both economic and national security value.[19] They could also be used to commit human rights violations.[20] Foreign powers want to exploit research partnerships with Canadian researchers to acquire knowledge in these sensitive areas. Some foreign powers, such as China, are also targeting Canada's data sets and big data.[21]

A second type of risk involves intellectual property. On the one hand, research partnerships between Canadian research institutes and foreign actors can result in intellectual property from research carried out in Canada being legally transferred to foreign countries.[22] In such cases, foreign companies contractually own the intellectual property resulting from research carried out with Canadian partners. On the other hand, there is a risk of intellectual property theft.[23] Sami Khoury, Head of the Canadian Centre for Cyber Security, cited the National Cyber Threat Assessment 2023–2024 report, saying:

---

18 SRSR, *Evidence*, 20 June 2023, 1105 (Christian Leuprecht).

19 SRSR, *Evidence*, 20 June 2023, 1110 (Jim Hinton).

20 SRSR, *Evidence*, 4 October 2023, 1635 (Ivana Karaskova, China Projects Lead, Association for International Affairs (AMO), As an Individual).

21 SRSR, *Evidence*, 23 October 2023, 1550 (Nicole Giles); and SRSR, *Evidence*, 20 November 2023, 1620 (Hon. François-Philippe Champagne, P.C., M.P., Minister of Innovation, Science and Industry).

22 SRSR, *Evidence*, 25 September 2023, 1620 (Margaret McCuaig-Johnston, Senior Fellow, Graduate School of Public and International Affairs and Institute of Science, Society and Policy, University of Ottawa, As an Individual); and SRSR, *Evidence*, 27 September 2023, 1630 (Jeffrey Stoff, President, Center for Research Security and Integrity).

23 SRSR, *Evidence*, 23 October 2023, 1545 (Nicole Giles); and SRSR, *Evidence*, 22 November 2023, 1630 (David Vigneault).

> [S]tate-sponsored threat actors engage in commercial espionage, targeting intellectual property and other valuable business information. They do so with the goal of sharing stolen information with state-owned enterprises or domestic industry in their home country.[24]

Another threat mentioned by witnesses was interference in universities and research institutes. These threats were described by Nicole Giles, the Senior Assistant Deputy Minister for Policy and Strategic Partnerships at the Canadian Security Intelligence Service, as follows:

> On university campuses, foreign states, including the People's Republic of China, seek to exert undue influence covertly and through proxies by harassing dissidents and suppressing academic freedoms and free speech. Foreign interference and espionage in academia can take many forms, from covertly influencing research agendas or peer-review processes to engaging in funding arrangements, where details about the source of funds are deliberately obscured or misrepresented. Common techniques can include blackmail, coercion, illicit financing, intimidation and disinformation.[25]

As mentioned above, several witnesses noted that these threats were not all from one country;[26] Russia, Iran and North Korea were also mentioned.[27]

However, the Committee heard that "the PRC, in the context of a threat to our economic security and research security, is by far the most sophisticated actor that we're dealing with."[28] When asked about how concerned Canada should be about Chinese interference in Canada's scientific research ecosystem, Gordon Houlden, Professor and Director Emeritus at the University of Alberta's China Institute, replied that, on a scale of one to 10, he would assign an eight to China.[29] Margaret McCuaig-Johnston, a Senior Fellow at the University of Ottawa's Graduate School of Public and International Affairs and Institute of Science, Society and Policy, appearing as an individual, said that, of "the

24 SRSR, *Evidence*, 23 October 2023, 1555 (Sami Khoury); and Canadian Centre for Cyber Security, *National Cyber Threat Assessment 2023–2024*.

25 SRSR, *Evidence*, 23 October 2023, 1545 (Nicole Giles).

26 SRSR, *Evidence*, 20 June 2023, 1110 (Jim Hinton); SRSR, *Evidence*, 20 September 2023, 1635 (Cherie Wong); SRSR, *Evidence*, 4 October 2023, 1640 (Kevin Gamache); and SRSR, *Evidence*, 23 October 2023, 1625 (Nicole Giles).

27 For example, SRSR, *Evidence*, 20 June 2023, 1105 (Christian Leuprecht); SRSR, *Evidence*, 20 June 2023, 1120 (Jim Hinton); and SRSR, *Evidence*, 20 September 2023, 1650 (Gordon Houlden).

28 SRSR, *Evidence*, 22 November 2023, 1635 (David Vigneault).

29 SRSR, *Evidence*, 20 September 2023, 1655 (Gordon Houlden).

countries that we know are problems," "China is certainly number one—and number two, three and four too."[30]

1.3 Strategies of the People's Republic of China

Witness testimony helped shed light on China's objectives and some of its strategies.

In a written submission, Anna Puglisi, a Senior Fellow at Georgetown University's Center for Security and Emerging Technology, explained that "Beijing has made talent development and the exploitation of overseas students, universities, and government labs a central part of its technology acquisition strategy since the country's 'opening' around 1978."[31] Ivana Karaskova, the China Projects Lead for the Association for International Affairs (AMO), appearing as an individual, said that, "as China strategically uses foreign technologies to boost its own technological base and enable domestic innovation, it increases the competitiveness of its industry and research sectors vis-à-vis foreign counterparts."[32] China's "ultimate goal" is to "substitute foreign technology with indigenous development and to achieve dominance in key sectors across the board."[33] Lastly, she added that "Chinese technology acquisition abroad is tied to the modernization of its military, as many of the technologies are of a dual-use nature."[34]

Some witnesses noted that China's ambitions are coupled with a lack of reciprocity, in that China is not giving foreign researchers the same access to Chinese science, technology and innovation sectors.[35]

According to several witnesses, this policy has become more extreme in recent years under the leadership of Xi Jinping, who has been the president of the People's Republic of China since 2013.[36] According to Christian Leuprecht, "in 2017 we had a qualitative

30 SRSR, *Evidence*, 25 September 2023, 1555 (Margaret McCuaig-Johnston).

31 Anna Puglisi, *Testimony before the House of Commons Science and Research Committee "Canadian research partnerships with entities connected to the People's Republic of China,"* Brief submitted to the House of Commons Standing Committee on Science and Research, 25 September 2023, p. 1.

32 SRSR, *Evidence*, 4 October 2023, 1635 (Ivana Karaskova).

33 Ibid.

34 Ibid.

35 Ibid.; SRSR, *Evidence*, 25 September 2023, 1600 (Margaret McCuaig-Johnston); and SRSR, *Evidence*, 25 September 2023, 1535 (Anna Puglisi, Senior Fellow, Center for Security and Emerging Technology, Georgetown University, As an Individual).

36 SRSR, *Evidence*, 20 June 2023, 1130 (Christian Leuprecht); and SRSR, *Evidence*, 25 September 2023, 1530 (Margaret McCuaig-Johnston).

and quantitative paradigm shift in the aggressive posture by China and the systematic leveraging of technology to undermine our way of life, which now poses an existential threat to Canada in a way that we did not have before."[37] Although he did not use the term "existential threat," David Vigneault said that the People's Republic of China is a "threat to the country,"[38] and he confirmed that "the PRC, under the leadership of Xi Jinping, has essentially created an environment in which all of the resources of the state have been combined under the leadership of the chairman to essentially create the tools for the PRC to succeed."[39]

1.3.1 A Holistic Approach

To achieve its objectives, China takes "a holistic approach to the development of technology," and it "blurs the lines between public, private, civilian and military."[40] In a written submission, Anna Puglisi gave the example of China's 13th five-year plan for military and civil fusion, established in 2017, which specifically calls for a "cross-pollination of military and civilian technology in areas not traditionally seen as 'national security issues,' such as quantum telecommunication and computing, neuroscience and brain-inspired research."[41] Nicole Giles said a commission chaired by Xi Jinping integrates its military and civilian technology together: "Everything they're doing, whether it's with the private sector or with our universities, is going back into a system to create dual-use applications for the military."[42]

1.3.2 Stakeholders Involved

This holistic approach also involves mobilizing all possible stakeholders. David Vigneault, the Director of CSIS, explained that "all parts of that government are involved in seeking information, either openly or surreptitiously, in order to serve the interests of the Chinese Communist Party."[43] Several laws adopted in recent years require Chinese citizens to "respond to the PRC's government or security services if they are asked for

37 SRSR, *Evidence*, 20 June 2023, 1130 (Christian Leuprecht).

38 SRSR, *Evidence*, 22 November 2023, 1635 (David Vigneault).

39 Ibid., 1640.

40 SRSR, *Evidence*, 25 September 2023, 1535 (Anna Puglisi).

41 Anna Puglisi, *Testimony before the House of Commons Science and Research Committee "Canadian research partnerships with entities connected to the People's Republic of China,"* Brief submitted to the House of Commons Standing Committee on Science and Research, 25 September 2023, p. 5.

42 SRSR, *Evidence*, 23 October 2023, 1625 (Nicole Giles).

43 SRSR, *Evidence*, 22 November 2023, 1650 (David Vigneault).

information or data."[44] According to Nicole Giles, "this summer, PRC introduced two national security laws, which have fundamentally expanded the definition of national security so that they empower PRC intelligence and law enforcement agencies to compel co-operation of firms and people."[45] This legislation means that Canadian scientists could be "partnering with civilian scientists or engineers at any university in China and not be aware that their research is going out the back door to the PLA [People's Liberation Army]."[46] David Vigneault, the Director of CSIS, said that he was "very concerned" about this matter.[47]

The regime also requires Chinese private businesses to contribute. According to Alliance Canada Hong Kong, "[u]nder the civil-military fusion strategies, Chinese private companies' investments are often driven by the CCP [Chinese Communist Party] committee within the boardrooms."[48] Margaret McCuaig-Johnston indicated that some Canadian researchers are "partnering with Chinese military and surveillance technology companies like SenseTime, Tencent, Alibaba, iFlytek and Huawei, which work with the military and which also design and sell equipment to repress the Uyghurs and others."[49]

Witnesses also mentioned that China uses concealment strategies to hide some of its activities.[50] For example, some partners hide their affiliation "in order to be able to donate money and contribute to research projects that can lead to threats to Canada's security."[51] Alliance Canada Hong Kong's written submission made the following observation:

> With opaque ties between the [People's Liberation Army] and Chinese universities, it is difficult to differentiate between collaborating with Chinese individual scholars or

44 SRSR, *Evidence*, 25 September 2023, 1535 (Anna Puglisi).

45 SRSR, *Evidence*, 23 October 2023, 1610 (Nicole Giles).

46 SRSR, *Evidence*, 25 September 2023, 1530 (Margaret McCuaig-Johnston).

47 SRSR, *Evidence*, 22 November 2023, 1715 (David Vigneault).

48 Alliance Canada Hong Kong, *Written Submission to the Standing Committee on Science and Research (SRSR)*, September 2023, p. 4.

49 SRSR, *Evidence*, 25 September 2023, 1530 (Margaret McCuaig-Johnston).

50 Anna Puglisi, *Testimony before the House of Commons Science and Research Committee "Canadian research partnerships with entities connected to the People's Republic of China,"* Brief submitted to the House of Commons Standing Committee on Science and Research, 25 September 2023, p. 6.

51 SRSR, *Evidence*, 22 November 2023, 1645 (David Vigneault). See also SRSR, *Evidence*, 25 September 2023, 1530 (Margaret McCuaig-Johnston).

> Chinese military scholars, and impossible to determine if the results of these research collaborations would benefit [the People's Liberation Army] or Chinese state actors.[52]

1.3.3 Recruitment Strategies

The Committee's attention was drawn to China's recruitment strategies and ways that researchers were vulnerable to these methods.

Alliance Canada Hong Kong identified three tactics used by Chinese state-affiliated and private businesses to recruit Canadian university professors and researchers:

- collaborative grant applications through the Government of Canada and/or other Canadian funders;
- offer a lucrative research contract; and/or
- offer a lucrative consultancy contract.[53]

To attract possible Canadian partners, some Chinese entities provide generous funding. Benjamin Fung, Canada Research Chair and Professor at McGill University, speaking on behalf of Alliance Canada Hong Kong, shared his own experience in this area. He said he was offered three times his salary to become a consultant for a Chinese 5G company while remaining a professor at McGill University.[54] He added that the same company had approached several of his students.[55]

Beyond offers of funding, some researchers are enticed by other benefits promised by their Chinese partners. Ivana Karaskova mentioned the ability to use China's research infrastructure, or to carry out experiments or access data that bypasses the ethical standards in place in Canada and Europe.[56] Alliance Canada Hong Kong raised the same points in its written submission.[57]

---

52 Alliance Canada Hong Kong, *Written Submission to the Standing Committee on Science and Research (SRSR)*, September 2023, p. 5.

53 Ibid., p. 6.

54 SRSR, *Evidence*, 20 September 2023, 1630 (Benjamin Fung, Canada Research Chair and Professor, McGill University, Alliance Canada Hong Kong).

55 Ibid.

56 SRSR, *Evidence*, 4 October 2023, 1715 (Ivana Karaskova).

57 Alliance Canada Hong Kong, *Written Submission to the Standing Committee on Science and Research (SRSR)*, September 2023, p. 6.

These proposals may appeal to some researchers, particularly if they are struggling to fund their studies and research. A number of witnesses suggested that better funding for research in Canada could make researchers less susceptible to offers of funding being dangled by foreign entities.[58]

In addition, the Committee heard that there is an amount of naïveté amongst university faculty, which makes some researchers more susceptible to the recruitment efforts of foreign entities.[59] Ivana Karaskova told the Committee that some researchers "focus just on their single science area" and "basically do not see all of the geopolitical implications."[60] Margaret McCuaig-Johnston said that some researchers don't see the risk of certain partnerships:

> They say, "My friends of 25 years in China would never do anything unseemly." However, when military researchers are part of the research process, they can redirect the research to their priorities in the [People's Liberation Army], whether it's through [the National University of Defense Technology] or a civilian university partnering with the Chinese military.[61]

Therefore, the Committee recommends:

Recommendation 1

That the Government of Canada take appropriate measures to ensure that sufficient levels of research funding are being provided to post-secondary institutions, their faculty and their students, in order to discourage reliance on foreign investment that may compromise national security.

1.3.4 Influence and Intimidation on Campuses

According to Nicole Giles, "there are continual efforts by PRC institutions and individuals to try to insert themselves into our universities' research and projects."[62] These efforts include strategies to influence and intimidate.

---

58 SRSR, *Evidence*, 20 September 2023, 1705 (Benjamin Fung); SRSR, *Evidence*, 27 September 2023, 1635 (Philip Landon); and SRSR, *Evidence*, 27 September 2023, 1710 (Chad Gaffield).

59 SRSR, *Evidence*, 4 October 2023, 1710 (Kevin Gamache); and SRSR, *Evidence*, 4 October 2023, 1715 (Ivana Karaskova).

60 SRSR, *Evidence*, 4 October 2023, 1715 (Ivana Karaskova).

61 SRSR, *Evidence*, 25 September 2023, 1615 (Margaret McCuaig-Johnston).

62 SRSR, *Evidence*, 23 October 2023, 1620 (Nicole Giles).

Some of the partnerships and funding agreements proposed by entities connected to China put Canadian researchers in a vulnerable position. Benjamin Fung told the Committee about the recruitment strategy known in Chinese as "feed, trap and kill":

> They first use lucrative offers to attract their targets. Once a professor relies on their funding, they will start making unreasonable requests, including transferring IP rights, getting sensitive data or asking the professor to say something that may not be true.[63]

Students and researchers of Chinese origin who are studying or working in Canada are also targeted by these intimidation strategies. Cherie Wong, the Executive Director of Alliance Canada Hong Kong, described these practices:

> Whether they are domestic or international students, Tibetans, Uyghurs, Chinese, Taiwanese and Hong Kongers are experiencing transnational surveillance and fear of reprisal on university campuses. International students have also expressed their concerns that embassies, consulates and their home governments might revoke study permits or scholarships for unfavourable views, actions or inactions.

Anna Puglisi testified that "China intimidates and harshly silences its critics. This has only grown more prevalent in the past few years, and it increasingly includes its citizens abroad, both in Canada and the U.S."[64] According to Alliance Canada Hong Kong, "[t]here is a culture of fear and silence among the diaspora and Chinese communities."[65] In its written submission, Alliance Canada Hong Kong said that "the Chinese party-state weaponized the Chinese Students and Scholars Association globally to inject CCP [Chinese Communist Party] ideology into Chinese international students."[66]

Therefore, the Committee recommends:

Recommendation 2

That the government of Canada encourage and assist postsecondary institutions in adopting measures to protect researchers and students targeted by foreign government interference efforts on their campuses.

---

63 SRSR, *Evidence*, 20 September 2023, 1630 (Benjamin Fung).

64 SRSR, *Evidence*, 25 September 2023, 1535 (Anna Puglisi).

65 Alliance Canada Hong Kong, *Written Submission to the Standing Committee on Science and Research (SRSR)*, September 2023, p. 3.

66 Ibid., p. 8.

1.3.5 Primary Targets

According to Margaret McCuaig-Johnston, China's primary targets in the scientific field are the United States, the United Kingdom and Canada: "Canada's among the top, and the reason is that we're advanced in all of the strategic technologies that the PLA wants to get a hold of."[67]

Witnesses listed the following research areas as sensitive or targeted by China: photonics, artificial intelligence, quantum theory, biopharmaceuticals, aerospace, computer science, advanced materials manufacturing, critical minerals, polar research, genomics and neuroscience.[68]

However, Anna Puglisi noted that, "as China has become more capable, it targets earlier and earlier in the development cycle,"[69] which includes basic research.

With regard to targeted institutions in Canada, David Vigneault explained that foreign powers are no longer targeting only government actors: "With private industry and research now holding valuable intellectual property and potential for economic prosperity, threat actors have shifted to include non-government targets in their foreign interference campaigns."[70] These targets include universities and private-sector research.

Anna Puglisi also said that China's recruitment strategies are not restricted to researchers of Chinese origin, but extend to other people as well.[71]

1.4 Status of Research Partnerships

The evidence given did not reveal the exact number of research partnerships in place between Chinese partners and Canadian universities. In fact, some of these partnerships

67 SRSR, *Evidence*, 25 September 2023, 1610 (Margaret McCuaig-Johnston).

68 SRSR, *Evidence*, 20 June 2023, 1105 (Christian Leuprecht); SRSR, *Evidence*, 25 September 2023, 1530 and 1555 (Margaret McCuaig-Johnston); SRSR, *Evidence*, 4 October 2023, 1635 (Ivana Karaskova); and Anna Puglisi, *Testimony before the House of Commons Science and Research Committee "Canadian research partnerships with entities connected to the People's Republic of China,"* Brief submitted to the House of Commons Standing Committee on Science and Research, 25 September 2023, pp. 4–5.

69 SRSR, *Evidence*, 25 September 2023, 1545 (Anna Puglisi).

70 SRSR, *Evidence*, 22 November 2023, 1630 (David Vigneault).

71 Anna Puglisi, *Testimony before the House of Commons Science and Research Committee "Canadian research partnerships with entities connected to the People's Republic of China,"* Brief submitted to the House of Commons Standing Committee on Science and Research, 25 September 2023, p. 6.

that do not involve public funding are confidential.[72] Jim Hinton, an intellectual property lawyer, made the following observation:

> According to public reports, 50 Canadian universities have conducted extensive research with China's military since 2005.
>
> Huawei has partnered with over 20 of Canada's research institutions. Huawei has received intellectual property from the University of Waterloo, the University of Toronto, McGill University, the University of British Columbia, the University of Calgary, the University of Ottawa, Université Laval, Institut national de la recherche scientifique, Carleton University, Polytechnique Montréal, Western University, the University of Regina and McMaster University. … This is just the tip of the iceberg. Significant public funding, millions of dollars and resources are being used. Hundreds of patents have been generated for Huawei through these deals.[73]

The Minister of Innovation, Science and Industry, François-Philippe Champagne, said that, "since June 2021, there have been no federal grants to Huawei."[74] He also mentioned that a number of universities, including the University of Toronto, the University of Waterloo, McMaster University, Queen's University, the University of British Columbia and Western University, have "stopped any collaboration with Huawei."[75]

According to Jim Hinton, even though some Canadian universities have announced that they will no longer be collaborating with Huawei in the future, patent applications are still being submitted based on existing partnerships or agreements that recently ended.[76] He gave the example of a patent published in September 2023 that lists Huawei Technologies Canada and the governing council of the University of Toronto.[77]

CHAPTER 2. THE ROLE OF INSTITUTIONS AND RESEARCHERS

Witnesses focused on the responsibilities of research institutes and of researchers themselves, as well as on the role they could play in addressing these threats.

72 SRSR, *Evidence*, 20 June 2023, 1120 (Jim Hinton).

73 Ibid., 1110.

74 SRSR, *Evidence*, 20 November 2023, 1600 (Hon. François-Philippe Champagne).

75 Ibid.

76 SRSR, *Evidence*, 4 October 2023, 1630 (Jim Hinton).

77 Ibid., 1735.

On behalf of Universities Canada, Philip Landon stated that universities "do their due diligence on all international collaborations in this changing environment."[78] He said that "[i]t has become tighter over time."[79] Chad Gaffield, on behalf of the U15 Group, made similar comments. In his view, universities have "made huge progress, such that I think all of us today can feel very confident that our research on our campuses is being undertaken in secure ways that do not threaten us."[80]

However, not all witnesses shared their view. Jim Hinton said that there is "a failure of governance out of Canadian universities."[81] He believes that universities took action only due to public pressure:

> Back in 2018, *The Globe and Mail* reported on this issue. Only with mounting public pressure has there been reorientation. That means the universities themselves are complicit in this funnelling of IP to Huawei. They get a bit of money and they're happy about it, but it's clear to me that it's only after they've been put under the public microscope that they have had the wherewithal to remove themselves from such a bad situation. We can't trust them to make sure this doesn't happen again.[82]

In its brief, Alliance Canada Hong Kong made a connection between Canadian universities' need for funding and their actions:

> Universities and research institutions have many financial incentives to host more international students and/or foreign investments. International students pay an inflated tuition compared to domestic students. While financial inflows may offer a clear short-term benefit, a systemic failure to clearly understand longer-term institutional risks (e.g. elite capture, espionage) is again apparent.[83]

Witnesses mentioned several areas in which universities could take action to address the threats associated with research.

2.1 Increased Transparency

First, it was suggested to the Committee that universities should be more transparent. Jim Hinton made the following recommendation: "Universities receiving public funding

78 SRSR, *Evidence*, 27 September 2023, 1655 (Philip Landon).

79 Ibid.

80 SRSR, *Evidence*, 27 September 2023, 1710 (Chad Gaffield).

81 SRSR, *Evidence*, 20 June 2023, 1120 (Jim Hinton).

82 Ibid.

83 Alliance Canada Hong Kong, *Written Submission to the Standing Committee on Science and Research (SRSR)*, September 2023, p. 7.

must track and report the flow of research and development efforts with annual and concrete disclosure, including how much and whom they are working with."[84] This recommendation was supported by Anna Puglisi.[85]

2.2 Proactive Approach

Witnesses also encouraged universities to be more proactive. A number of witnesses said that universities have an important role to play in research security.[86] According to Christian Leuprecht, "universities can do a significant amount of the legwork if they are told what the sensitive research areas are and what the potentially problematic countries are, and if they are told the specific entities and actors with whom they should be avoiding collaboration."[87] In Jim Hinton's view, a proactive strategy is needed that requires universities to work with Canada's intelligence community.[88]

On this topic, David Vigneault told the Committee that the relationship between CSIS and universities has improved. Five years ago, "there was discomfort on openly engaging with CSIS, but we have come a long way from these first meetings."[89] In fact, "these institutions now proactively reach out to [CSIS] for ways to work together to protect research security and to counter foreign interference threats."[90]

2.3 Maintaining Academic Freedom and Institutional Autonomy

According to witnesses, this proactive approach from the academic sector, as well as a relationship with Canada's intelligence community, should not limit academic freedom and institutional autonomy.[91]

---

84 SRSR, *Evidence*, 20 June 2023, 1110 (Jim Hinton).

85 SRSR, *Evidence*, 25 September 2023, 1535 (Anna Puglisi).

86 For example, SRSR, *Evidence*, 20 June 2023, 1140 (Christian Leuprecht); and SRSR, *Evidence*, 4 October 2023, 1700 (Kevin Gamache).

87 SRSR, *Evidence*, 20 June 2023, 1140 (Christian Leuprecht).

88 SRSR, *Evidence*, 4 October 2023, 1630 (Jim Hinton).

89 SRSR, *Evidence*, 22 November 2023, 1630 (David Vigneault).

90 Ibid.

91 SRSR, *Evidence*, 20 November 2023, 1605 (Hon. François-Philippe Champagne); SRSR, *Evidence*, 4 October 2023, 1705 (Ivana Karaskova); and SRSR, *Evidence*, 20 November 2023, 1655 (Francis Bilodeau, Associate Deputy Minister, Department of Industry).

Some witnesses emphasized the importance of keeping science as open as possible. Minister François-Philippe Champagne made the following statement:

> [A]cademic and institutional freedom is essential in Canada. … I think the guideline we need to have is that our research must be as open as possible and as secure as necessary. That is really the framework in which we need to operate.[92]

According to Sami Khoury, it is not a matter of picking between being open and collaborative on one side, and security on the other side.[93] However, the Committee learned that it can be difficult to balance these objectives.[94]

Regarding academic freedom, a number of witnesses mentioned the responsibility of researchers themselves.[95] Jim Hinton made the following observation:

> Academic freedom requires an environment of enabled autonomy with researchers free from undue external influence. State military actors are undue influencers, whether academics like to admit it or not. There are limitations on what can and should be done in the name of academic freedom. Just as a researcher is not permitted to falsify research or plagiarise, they should not be able to aid and abet foreign military actors at the risk of Canada's national security.[96]

Alliance Canada Hong Kong stated, "Academic freedom must include students and researchers' safety, feeling educated and empowered in making informed decisions for their research."[97] This involves taking steps to "support the development of equitable research and academic advancement,"[98] where students and researchers feel protected.

2.4 Awareness and Training

According to witnesses, one responsibility that universities have is to make researchers and research officers aware of the risks of foreign influence. Benjamin Fung said, "One

92 SRSR, *Evidence*, 20 November 2023, 1605 (Hon. François-Philippe Champagne).

93 SRSR, *Evidence*, 23 October 2023, 1630 (Sami Khoury).

94 SRSR, *Evidence*, 4 October 2023, 1705 (Ivana Karaskova).

95 SRSR, *Evidence*, 25 September 2023, 1530 (Margaret McCuaig-Johnston); and SRSR, *Evidence*, 20 June 2023, 1120 (Jim Hinton).

96 SRSR, *Evidence*, 20 June 2023, 1120 (Jim Hinton).

97 Alliance Canada Hong Kong, *Written Submission to the Standing Committee on Science and Research (SRSR)*, September 2023, p. 2.

98 Ibid.

way to tackle the problem is … to educate the professors, raise awareness and let them know the potential risk."[99]

Since 2021, according to the Government of Canada's National Security Guidelines for Research Partnerships (the Guidelines),[100] which will be described in greater detail later in this report, researchers that request certain types of funding from the granting agencies—the Social Sciences and Humanities Research Council (SSHRC), the Natural Sciences and Engineering Research Council (NSERC) and the Canadian Institutes of Health Research (CIHR)—must fill out a risk assessment form. This responsibility involves being aware of the risks associated with research partnerships, sensitive research areas and foreign entities that could be problematic.

Universities have a role to play in raising awareness.[101] Chad Gaffield said that the U15 Group had developed a guide entitled *Safeguarding Research in Canada: A Guide for University Policies and Practices* for those involved in the research ecosystem.[102] Manal Bahubeshi, Vice-President of Research Partnerships at NSERC, said that universities have been increasingly engaged in raising awareness among researchers.[103] These activities go hand in hand with government awareness initiatives, which will be described later in this report.

2.5 Building Capacity

In recent years, universities have been making a concerted effort to build their capacity in order to play a more proactive role.[104] Most Canadian universities have created research security positions, with federal government support.[105] According to one

99 SRSR, *Evidence*, 20 September 2023, 1705 (Benjamin Fung).

100 Government of Canada, *National Security Guidelines for Research Partnerships*, September 2023 version.

101 SRSR, *Evidence*, 4 October 2023, 1730 (Jim Hinton).

102 SRSR, *Evidence*, 27 September 2023, 1655 (Chad Gaffield); and U15 Group of Canadian Research Universities, *Safeguarding Research in Canada: A Guide for University Policies and Practices*, 2023.

103 SRSR, *Evidence*, 25 October 2023, 1755 (Manal Bahubeshi, Vice-President, Research Partnerships, Natural Sciences and Engineering Research Council).

104 SRSR, *Evidence*, 27 September 2023, 1635 (Philip Landon).

105 SRSR, *Evidence*, 20 September 2023, 1705 (Gordon Houlden); SRSR, *Evidence*, 27 September 2023, 1635 (Philip Landon); SRSR, *Evidence*, 27 September 2023, 1655 (Chad Gaffield); and SRSR, *Evidence*, 25 October 2023, 1720 (Alejandro Adem, President, Natural Sciences and Engineering Research Council).

witness, these positions are often staffed by people with security backgrounds, including some who previously worked for CSIS.[106]

Canadian universities have also established training sessions, prepared documentation and developed internal security protocols.[107] They are also sharing best practices. In Ontario, for instance, universities have "established a province-wide community of practice to share their experiences and lessons learned and have developed and shared a best practices guide."[108]

Similar practices are also being developed outside of Canada. In the United States, Kevin Gamache gave examples of initiatives taken within the A&M University System. A research security office was created at the A&M system level to ensure "management and oversight of all … classified research, controlled unclassified programs and export-controlled research."[109] This work is done in collaboration with U.S. federal security and intelligence agencies.[110] Kevin Gamache also mentioned that A&M had created an "academic security and counter-exploitation working group, an association of university research professionals and their federal counterparts."[111] This group is actively engaged with the Canadian U15 Group.[112]

2.6 Support for Targeted Students and Researchers

The Committee's attention was also drawn to the need to better protect students and researchers who are susceptible to foreign actors' intimidation or influence.

Alliance Canada Hong Kong pointed out that Canadian university campuses often have their own security services, but that these services are not properly equipped to help

106 SRSR, *Evidence*, 20 September 2023, 1705 (Gordon Houlden).

107 SRSR, *Evidence*, 27 September 2023, 1655 (Chad Gaffield); and Government of Ontario, *Use of Federal Government Research and Development Grants, Funds, and Contributions by Canadian Universities and Research Institutions in Partnerships With Entities Connected to the People's Republic of China*, Brief submitted to the House of Commons Standing Committee on Science and Research, 6 October 2023, p. 3.

108 Government of Ontario, *Use of Federal Government Research and Development Grants, Funds, and Contributions by Canadian Universities and Research Institutions in Partnerships With Entities Connected to the People's Republic of China*, Brief submitted to the House of Commons Standing Committee on Science and Research, 6 October 2023, p. 3.

109 SRSR, *Evidence*, 4 October 2023, 1640 (Kevin Gamache).

110 Ibid.

111 Ibid.

112 Ibid.

members of the academic community deal with foreign state repression.[113] It described the situation as a "systemic and institutional failure."[114]

It proposed a number of solutions to address this issue:

- anonymous participation in class discussions and assignments if a student does not feel safe to engage without triggering transnational repression;
- strengthening universities' institutional cybersecurity measures and awareness;
- discouraging video or audio recording of class discussions without informed consent; and
- supporting international students whose study permits and scholarships are weaponized by their home governments.[115]

2.7 Need for Support

Jeffrey Stoff, President of the Center for Research Security and Integrity, said that "academic institutions typically lack the resources, subject matter knowledge or incentives to conduct robust due diligence on PRC research partners and sources of funding."[116] He added that "China's increasingly restrictive information environment … [is] making conducting robust due diligence and risk assessments too difficult and complex for individual research institutions to do themselves."[117] He further explained that these constraints raise questions about the effectiveness of policies that rely on universities conducting their own risk evaluations.[118]

Several witnesses were of the opinion that universities need government support in order to be effective in this role.[119] The Committee heard several times that members of

113 Alliance Canada Hong Kong, *Written Submission to the Standing Committee on Science and Research (SRSR)*, September 2023, p. 7.

114 Ibid.

115 Ibid.

116 SRSR, *Evidence*, 27 September 2023, 1630 (Jeffrey Stoff).

117 Ibid.

118 Ibid.

119 For example, SRSR, *Evidence*, 27 September 2023, 1725 (Chad Gaffield); and SRSR, *Evidence*, 4 October 2023, 1635 (Ivana Karaskova).

the research ecosystem were waiting for the government to release lists of problematic entities and sensitive research areas, which have since been published.[120] Minister François-Philippe Champagne also said that universities had informed the government that "it's very complex out there. They need resources. They need people."[121]

CHAPTER 3. THE ROLE OF THE FEDERAL GOVERNMENT

Witness testimony heard by the Committee highlighted the federal government's role and responsibilities in the area of research security. In recent years, the federal government has stepped up its efforts to protect research conducted in Canada, particularly by implementing the 2021 *National Security Guidelines for Research Partnerships*, and by the announcements made in January 2024.

3.1 Awareness of Issues

As mentioned above, until recently, successive federal governments had encouraged universities and researchers to establish scientific partnerships with China.[122] As a result, according to Chad Gaffield, "the Canadian research community became one of the most internationalized, thereby gaining access to the global pool of knowledge."[123]

This position began to shift as China's policy became more aggressive and as the media reported on relationships between Canadian universities and their Chinese partners.[124] Jim Hinton made the following statement:

> The federal government, through programs like … NSERC, not only has been complicit in these arrangements but has been incentivizing this behaviour. While there has been a recent shift in the approach because of the increasing public outcry, it has been entirely reactionary.[125]

120 SRSR, *Evidence*, 20 June 2023, 1105 and 1140 (Christian Leuprecht); SRSR, *Evidence*, 20 September 2023, 1635 (Gordon Houlden); SRSR, *Evidence*, 20 September 2023, 1705 (Cherie Wong); SRSR, *Evidence*, 25 September 2023, 1550 (Margaret McCuaig-Johnston); and SRSR, *Evidence*, 27 September 2023, 1650 (Chad Gaffield).

121 SRSR, *Evidence*, 20 November 2023, 1630 (Hon. François-Philippe Champagne).

122 SRSR, *Evidence*, 27 September 2023, 1645 (Chad Gaffield).

123 Ibid.

124 SRSR, *Evidence*, 4 October 2023, 1650 (Jim Hinton).

125 SRSR, *Evidence*, 20 June 2023, 1110 (Jim Hinton).

Awareness has been raised about the research community's vulnerability not only in Canada, but also around the world. Christian Leuprecht mentioned a report published by the Australian Strategic Policy Institute[126] in 2018 that was the first to reveal universities' "problematic collaborations."[127]

Witnesses identified actions taken in other countries to address the threat of interference in the academic world. Australia published a list of critical technologies: "[r]ather than restrict research in these areas, this list highlights opportunities they want to promote with other aligned nations while developing more robust risk mitigation practices."[128] Similarly, the European Union "revealed a list of 10 critical technologies, with four of them seen as more sensitive: advanced semiconductors, artificial intelligence, quantum and biotechnologies."[129]

According to Christian Leuprecht, the Canadian government has been "rather slow in picking up on this paradigmatic shift."[130] He said that other countries, such as the United States and Australia, "have been much faster out of the starting blocks and much more aggressive than the current federal government."[131] Other witnesses expressed the same opinion.[132]

Jeffrey Stoff, for his part, was of the opinion that the measures announced by Canada regarding the publication of a list of problematic entities was going a step further than the measures taken in the United States.[133] Kevin Gamache held a similar view, saying:

> I'd like to say first that I understand the strides the Canadian government has made over the last two years in particular. Some of the products you developed at the national level are very impressive, because we haven't seen that same kind of activity here in the United States. In fact, we've taken some of the documents that you developed and used them as models here.[134]

126 Alex Joske, *Picking flowers, making honey: The Chinese military's collaboration with foreign universities*, Australian Strategic Policy Institute, 30 October 2018.

127 SRSR, *Evidence*, 20 June 2023, 1125 (Christian Leuprecht).

128 SRSR, *Evidence*, 27 September 2023, 1635 (Philip Landon).

129 SRSR, *Evidence*, 4 October 2023, 1635 (Ivana Karaskova).

130 SRSR, *Evidence*, 20 June 2023, 1130 (Christian Leuprecht).

131 Ibid.

132 SRSR, *Evidence*, 20 September 2023, 1700 (Gordon Houlden); and SRSR, *Evidence*, 27 September 2023, 1635 (Philip Landon).

133 SRSR, *Evidence*, 27 September 2023, 1715 (Jeffrey Stoff).

134 SRSR, *Evidence*, 4 October 2023, 1655 (Kevin Gamache).

Witnesses discussed the policies implemented by the Canadian government in recent years.

3.2 A Whole-of-Government Approach

According to Minister François-Philippe Champagne, the government began focusing on this issue in 2018.[135] One of the first actions the government took in 2018 was to establish the Government of Canada–Universities Working Group.[136] This working group brings together members of the Government of Canada and representatives from the university community.[137] It serves as a forum to exchange information and consult stakeholders with a view to developing government policy.

The government's approach beginning in 2018 is not solely the responsibility of Innovation, Science and Economic Development Canada (ISED). It is a whole-of-government approach that relies on the efforts of other government departments and agencies as well.[138] This includes the intelligence sector, with the involvement of the Canadian Security Intelligence Service and the Canadian Centre for Cyber Security. According to ISED:

> Collectively, these federal departments and agencies offer expertise that inform the development of Canada's research security policies and programs, which balance research excellence and innovation, with national security considerations.[139]

This approach was formalized with the *National Security Guidelines for Research Partnerships*, published in 2021; efforts to raise awareness within the research ecosystem; and material support for universities through the Research Support Fund.

---

135 SRSR, *Evidence*, 20 November 2023, 1605 (Hon. François-Philippe Champagne).

136 SRSR, *Evidence*, 27 September 2023, 1645 (Chad Gaffield); and Innovation, Science and Economic Development Canada (ISED), *ISED Reply and follow up to the Minister of Innovation, Science, and Industry's Appearance before the Standing Committee on Science and Research (SRSR) on November 20, 2023*.

137 On the government side, it includes representatives from various departments (Global Affairs Canada; Innovation, Science and Economic Development Canada; Public Safety Canada); security agencies (Canadian Security Intelligence Service; Canadian Centre for Cyber Security); granting agencies (Social Sciences and Humanities Research Council; Natural Sciences and Engineering Research Council; Canadian Institutes of Health Research); the Canada Foundation for Innovation; and the National Research Council. On the university side, it includes representatives from Universities Canada and the U15 Group of Canadian Research Universities. Government of Canada, *About the Government of Canada – Universities Working Group*.

138 SRSR, *Evidence*, 22 November 2023, 1655 (Shawn Tupper, Deputy Minister, Department of Public Safety and Emergency Preparedness).

139 ISED, *ISED Reply and follow up to the Minister of Innovation, Science, and Industry's Appearance before the Standing Committee on Science and Research (SRSR) on November 20, 2023*, p. 2.

More recently, the government has established a Research Security Centre under Public Safety Canada, and on 16 January 2024 it announced new research protection measures to accompany the 2021 Guidelines.

3.3 The National Security Guidelines for Research Partnerships

The *National Security Guidelines for Research Partnerships* were published in July 2021. They are the result of consultations between the federal government and the university community, which took place within the framework of the Government of Canada–Universities Working Group.[140]

The Guidelines provide information for researchers on the risks associated with research partnerships.[141] They explain the types of risks involved and identify elements of possible national security risks that should be considered when entering into a partnership. These elements include what the research area is and who the partner is. The Guidelines also provide information on how to identify potential risks and mitigate them. For instance, the Guidelines provide information on how to develop a risk mitigation plan. Two annexes published with the Guidelines provide more detailed information about sensitive research areas and partner risks.

Once the Guidelines were published in July 2021, they were applied immediately on a pilot basis to NSERC's Alliance grants program:[142]

> Following the Guidelines, applicants seeking federal funding for research partnerships with private sector partner organizations must complete a Risk Assessment Form as an integral part of their application. This questionnaire requires applicants to consider any risks associated with the nature of their research and proposed private sector partner organizations. Applicants must also develop a tailored risk mitigation plan, commensurate with the risks identified while considering open science principles. Following the principles of the Guidelines, risk mitigation measures must never lead to discrimination against or profiling of any group or member of the research community.[143]

140 SRSR, *Evidence*, 27 September 2023, 1645 (Chad Gaffield).

141 Government of Canada, *National Security Guidelines for Research Partnerships*, September 2023 version.

142 Social Sciences and Humanities Research Council (SSHRC), *SSHRC written brief for the House of Commons Standing Committee Science and Research, Canadian Research Partnerships with Entities Connected to the People's Republic of China*, December 2023, p. 2.

143 Ibid.

Funding applications under the Alliance program that include a private partner are required to undergo a three-step risk assessment process:

> [F]irst by the applicant and their institution; then by the funding agency; and if necessary, by Canada's national security agencies.[144]

In more detail, the process is as follows: NSERC's dedicated Research Security Team reviews the risks identified and the risk mitigation measures proposed in the application.[145] If NSERC determines that additional assessments or advice are required, the application is referred to Public Safety Canada. At that point, the application is closely examined by Public Safety Canada, the Canadian Security Intelligence Service or the Communications Security Establishment. Public Safety Canada may consult Global Affairs Canada for some applications. NSERC then makes its funding decision based on the national security assessment and the merit assessment, which is carried out concurrently.[146] A witness noted that "the merit review of the research and the security review are separated so that they are not kind of conflating the quality of the research and the security risk."[147] If funding is granted, the mitigation plan must be implemented for the duration of the project.[148]

In 2023, further to feedback from participants, the form was simplified.[149] In March 2023, the scope of the risk assessment form was expanded "to include a thorough review of the integrated biomedical research fund and biosciences research infrastructure fund competition."[150]

In response to the Committee's questions, witnesses provided greater detail on certain parts of the assessment process.

---

144 Natural Sciences and Engineering Research Council (NSERC), *NSERC reply and follow-up to Dr. Alejandro Adem, President, NSERC appearance before the Standing Committee on Science and Research (SRSR) on October 25, 2023*, December 2023, p. 3. See also: Government of Canada, *Risk Assessment Review Process*.

145 NSERC, *NSERC reply and follow-up to Dr. Alejandro Adem, President, NSERC appearance before the Standing Committee on Science and Research (SRSR) on October 25, 2023*, December 2023, p. 3.

146 Government of Canada, *Risk Assessment Review Process*.

147 SRSR, *Evidence*, 20 November 2023, 1740 (Nipun Vats, Assistant Deputy Minister, Science and Research Sector, Department of Industry).

148 SRSR, *Evidence*, 25 October 2023, 1700 (Alejandro Adem).

149 SRSR, *Evidence*, 25 October 2023, 1725 (Manal Bahubeshi).

150 SRSR, *Evidence*, 25 October 2023, 1725 (Alejandro Adem).

The Committee was informed that NSERC employees responsible for assessing applications base their decisions on information available to the public on the Internet.[151] These officers have been trained "to identify where there could be security risks"[152] and they have "worked very closely with the security agencies."[153]

If an application is rejected for security reasons, feedback is provided to the researchers informing them why their application was denied.[154] According to Francis Bilodeau, Associate Deputy Minister, Department of Industry, there is no appeal process if a researcher disagrees with the decision.[155]

Alejandro Adem, NSERC President, told the Committee that the granting agencies do not look back at grants that have previously been given.[156] When asked whether there are penalties if a researcher knowingly provides misleading information in their application, Nipun Vats, Assistant Deputy Minister of the Science and Research Sector at the Department of Industry, answered that if a researcher broke the law, there would be a criminal charge.[157] Furthermore, research institutes may be given sanctions if they violate the terms of the Tri-Agency Framework: Responsible Conduct of Research, which outlines obligations for researchers and institutions receiving funding from the granting agencies.[158]

The granting agencies provided statistics on the implementation of the Guidelines. Between July 2021 and December 2023, NSERC considered nearly 2,000 Alliance grant applications submitted with a risk assessment form. Only 62 of these applications, representing less than 4%, were transferred to Public Safety Canada for an in-depth review. Of those 62 applications, 20 subsequently received funding after a positive response; 34 were denied, "following the advice that the proposed research partnership poses an unmitigable risk to Canadian national security"; two were withdrawn before the assessment was completed; and six assessments were still in progress.[159] According

151 Ibid., 1740.

152 SRSR, *Evidence*, 20 November 2023, 1640 (Nipun Vats).

153 Ibid., 1740.

154 SRSR, *Evidence*, 20 November 2023, 1705 (Francis Bilodeau).

155 Ibid., 1725.

156 SRSR, *Evidence*, 25 October 2023, 1720 (Alejandro Adem).

157 SRSR, *Evidence*, 20 November 2023, 1640 (Nipun Vats).

158 Ibid. See also: Government of Canada, *Tri-Agency Framework: Responsible Conduct of Research (2021)*.

159 NSERC, *NSERC reply and follow-up to Dr. Alejandro Adem, President, NSERC appearance before the Standing Committee on Science and Research (SRSR) on October 25, 2023*, December 2023, p. 2.

to Francis Bilodeau, of the applications that were rejected for security reasons, the participation of state-owned enterprises and the presence of sensitive technology, particularly in the digital space, were recurring patterns.[160]

The three granting agencies were asked how many funding applications have been rejected over the past 20 years because of partnerships with entities or individuals from China that were deemed risky; and how many were accepted despite partnerships with entities or individuals from China. In a written answer, NSERC told the Committee that prior to July 2021, it was "not aware of any applications being rejected due to the partnerships being deemed risky with entities or individuals from China."[161] It added that "[s]ince July 2021, one Alliance grant application has been funded with a private sector partner organization located in China, following a rigorous Risk Assessment Review Process that concluded that it did not pose a risk to Canada's national security."[162] In written answers, both SSHRC and the CIHR told the Committee that to date, they had not rejected any funding applications on the basis of security concerns, as applications submitted to these two granting agencies were not yet subject to a security risk assessment.[163]

Minister François-Philippe Champagne remarked that "since June 2021, there have been no federal grants to Huawei," explaining that the guidelines framework, as applied for the Alliance grant applications, captured partnerships with Huawei.[164]

Several witnesses commented on the use of these Guidelines.

Margaret McCuaig-Johnston said she was "very impressed" by the Guidelines, which she described as "excellent."[165] Philip Landon, speaking on behalf of Universities Canada, said that the Guidelines have been "very helpful tools" for universities.[166]

160 SRSR, *Evidence*, 20 November 2023, 1700 (Francis Bilodeau).

161 NSERC, *NSERC reply and follow-up to Dr. Alejandro Adem, President, NSERC appearance before the Standing Committee on Science and Research (SRSR) on October 25, 2023*, December 2023, p. 2.

162 Ibid., p. 3.

163 SSHRC, "Follow-up identified," Written submission to the House of Commons Standing Committee on Science and Research, December 2023; and Canadian Institutes of Health Research, "Follow-up identified," Written submission to the House of Commons Standing Committee on Science and Research, March 2024.

164 SRSR, *Evidence*, 20 November 2023, 1600 and 1630 (Hon. François-Philippe Champagne).

165 SRSR, *Evidence*, 25 September 2023, 1550 (Margaret McCuaig-Johnston).

166 SRSR, *Evidence*, 27 September 2023, 1655 (Philip Landon).

Jim Hinton expressed a more critical view. First, he believes that the Government of Canada–Universities Working Group that was tasked with developing the Guidelines "is fatally flawed."[167] He explained his perspective as follows:

> It is insular. It fails to include domain experts who understand IP, national security, data sovereignty and privacy, to name a few. In addition, the university and government working group does not include innovative Canadian firms.[168]

He also expressed doubts about the ability of universities to reform their practices, calling it a "failure of governance."[169] In his view, the patent applications filed in 2022 involving research partnerships with Huawei show that "Canadian universities are still very actively building and transferring intellectual property to Huawei. This is despite ISED's 'National Security Guidelines for Research Partnerships', which was published in 2021."[170]

The Committee therefore recommends the following:

Recommendation 3

That the Government of Canada continue to work with post-secondary institutions to promote better information-sharing and encourage them to be more transparent about partnerships with foreign entities; and that it consider broadening the Government of Canada–Universities Working Group membership to include private research stakeholders.

Questions regarding the scope of the Guidelines were also raised by several witnesses. The risk assessment process described above affects only some of the funding applications submitted to the granting agencies. Research that is not funded through the granting agencies is not subject to the Guidelines. According to Ted Hewitt, SSHRC President, the tri-council funds only about 10% of research in Canada.[171] The remaining 90% includes research funded by universities themselves, as well as research funded by the provinces, industry, private interests and foreign entities. On that point, Margaret

167 SRSR, *Evidence*, 4 October 2023, 1630 (Jim Hinton).

168 Ibid.

169 SRSR, *Evidence*, 20 June 2023, 1120 (Jim Hinton).

170 SRSR, *Evidence*, 4 October 2023, 1630 (Jim Hinton).

171 SRSR, *Evidence*, 25 October 2023, 1745 (Ted Hewitt).

McCuaig-Johnston told the Committee that Genome Canada should be added to the organizations involved in the implementation of the Guidelines.[172]

A number of witnesses noted that funding provided through the granting agencies is the government's primary lever for promoting change.[173] According to Minister François-Philippe Champagne, the government's role is in providing leadership,[174] and it is from that perspective that the federal government took action to establish requirements and a framework.[175] According to Alejandro Adem, it is a matter of establishing "best practices that apply to a whole ecosystem regardless of where the money comes from."[176] The Guidelines and other forms of government action are intended to also raise awareness across the scientific ecosystem, beyond the funding allocated by the granting agencies.[177]

Lastly, some witnesses recommended that eligibility criteria tied to federal research funding should include compliance with the guidelines and the ability to enforce penalties in cases where the rules are broken.[178]

In light of the preceding, the Committee recommends:

Recommendation 4

That the Government of Canada consider adopting enforcement measures to ensure that postsecondary institutions follow the National Security Guidelines for Research Partnerships and the Policy on Sensitive Technology Research and Affiliations of Concern to qualify for funding from the federal government.

3.4 Awareness Efforts

A key aspect of government action on the research security file involves raising awareness within the research community. In September 2020, before the Guidelines had been published, the government "released a policy statement instructing all

172 SRSR, *Evidence*, 25 September 2023, 1615 (Margaret McCuaig-Johnston).

173 Ibid., 1545; and SRSR, *Evidence*, 20 November 2023, 1720 (Francis Bilodeau).

174 SRSR, *Evidence*, 20 November 2023, 1605 (Hon. François-Philippe Champagne).

175 Ibid., 1620.

176 SRSR, *Evidence*, 25 October 2023, 1755 (Alejandro Adem).

177 SRSR, *Evidence*, 25 October 2023, 1755 (Manal Bahubeshi).

178 SRSR, *Evidence*, 20 September 2023, 1710 (Benjamin Fung); and SRSR, *Evidence*, 20 September 2023, 1710 (Cherie Wong).

organizations to remain vigilant to potential security threats. It also launched the Safeguarding Your Research portal."[179] This portal was developed by ISED to "provide researchers and universities with tools and information about how to protect research security."[180]

Furthermore, the government, through Public Safety Canada, CSIS and the granting agencies, hosts a number of information sessions with various stakeholders in the Canadian research ecosystem.

For example, Public Safety Canada delivers safeguarding science workshops, with experts from Public Safety Canada, CSIS, Global Affairs Canada, the Canadian Nuclear Safety Commission and the Public Health Agency of Canada.[181] These workshops are given to universities, private labs and other federal departments.

David Vigneault made the following statement:

> In 2022 alone, CSIS conducted 113 stakeholder engagement activities and met with representatives of academia, community organizations, civil society, advocacy associations, research and innovation institutes and Indigenous leaders, as well as representatives of provincial and municipal governments.[182]

David Vigneault emphasized the importance of building a relationship between CSIS and academia: "[t]hese relationships have proven critical to building national security literacy and resiliency in the increasingly complex threat landscape that we are facing here in Canada."[183]

CSIS also publishes an annual report available to the public in which it identifies threats and other forms of foreign interference to raise public awareness.[184] Publications on research protection are available in local languages, such as Inuktitut.[185] Lastly,

---

179 SSHRC, *SSHRC written brief for the House of Commons Standing Committee Science and Research, Canadian Research Partnerships with Entities Connected to the People's Republic of China*, December 2023, p. 3. See: Government of Canada, *Safeguarding Your Research*.

180 SRSR, *Evidence*, 27 September 2023, 1645 (Chad Gaffield).

181 SRSR, *Evidence*, 23 October 2023, 1600 (Sébastien Aubertin-Giguère, Associate Assistant Deputy Minister, National and Cyber Security, Department of Public Safety and Emergency Preparedness).

182 SRSR, *Evidence*, 22 November 2023, 1630 (David Vigneault).

183 Ibid.

184 SRSR, *Evidence*, 23 October 2023, 1550 (Nicole Giles).

185 SRSR, *Evidence*, 22 November 2023, 1700 (Nicole Giles).

David Vigneault said that CSIS also works with industry associations and specific elements of the economic sector to share practical advice.[186]

The Canadian Centre for Cyber Security provides advice and guidance for educational institutions, including small universities and technical institutes, and can look at the security of their networks at their request.[187]

3.5 Creating the Research Security Centre

In Budget 2022, Public Safety Canada received funding to establish a research security centre. Sébastien Aubertin-Giguère informed the Committee that the Centre is now "fully up and running."[188]

The Research Security Centre has two teams. The first team is a network of six regional advisors across the country who are responsible for liaising with universities and provincial governments. The second team is based in Ottawa, with six analysts who are responsible for the implementation of the Guidelines and for developing outreach products.[189]

The Centre's mandate is both to serve as a contact point for the university community across the country to provide expertise and advice; and to ensure the implementation of the Guidelines.[190]

3.6 Support for Research Institutions

The government also took steps to build the capacity of stakeholders in academia to address threats. In Budget 2022, the government announced $125 million in funding over five years for Canadian institutions through the Research Support Fund (RSF) "to help them enhance their research security capacities."[191] This funding is overseen by the Tri-agency Institutional Programs Secretariat (TIPS) on behalf of the three granting

186 SRSR, *Evidence*, 22 November 2023, 1655 (David Vigneault).

187 SRSR, *Evidence*, 23 October 2023, 1615 (Sami Khoury).

188 SRSR, *Evidence*, 23 October 2023, 1600 (Sébastien Aubertin-Giguère).

189 Ibid.

190 Ibid.; and SRSR, *Evidence*, 23 October 2023, 1625 (Lesley Soper, Director General, National Security Policy, Department of Public Safety and Emergency Preparedness).

191 SRSR, *Evidence*, 25 October 2023, 1715 (Ted Hewitt).

agencies.[192] "A first call for applications launched in December 2022, through which funding is currently being allocated to 49 universities across Canada."[193]

Minister François-Philippe Champagne explained that "[t]he money we've provided to about 50 institutions around the country is around hiring personnel, getting the software needed and making sure they can have the proper cybersecurity infrastructure in place."[194] Universities used this funding to create research security positions.[195] According to ISED, "Funding for research security is for eligible institutions receiving $2 million or more in eligible RSF direct research funding. Eligibility for research security funding is assessed against this threshold each year."[196]

However, according to Christian Leuprecht, the formula used to calculate support under the Research Support Fund is "problematic":

> Aurora College gets $256 a year, Trent gets $25,000, and the University of Toronto gets $4.3 million. This is insufficient funding for Trent to hire research officers, on the one hand, but way too much money for the University of Toronto. Second, that effort looks largely performative. The new university research officers have thus far received little guidance and are largely performing an administrative function. They require clear guidance.[197]

Philip Landon, speaking on behalf of Universities Canada, said that it is important "to ensure that smaller universities are not left out" of initiatives like this one.[198]

192 SSHRC, *SSHRC written brief for the House of Commons Standing Committee Science and Research, Canadian Research Partnerships with Entities Connected to the People's Republic of China*, December 2023, p. 3.

193 Ibid.

194 SRSR, *Evidence*, 20 November 2023, 1630 (Hon. François-Philippe Champagne).

195 SRSR, *Evidence*, 20 September 2023, 1705 (Gordon Houlden); and SRSR, *Evidence*, 20 November 2023, 1715 (Francis Bilodeau).

196 ISED, *ISED Reply and follow up to the Minister of Innovation, Science, and Industry's Appearance before the Standing Committee on Science and Research (SRSR) on November 20, 2023*, p. 18.

197 SRSR, *Evidence*, 20 June 2023, 1105 (Christian Leuprecht).

198 SRSR, *Evidence*, 27 September 2023, 1635 (Philip Landon).

The Committee therefore recommends:

Recommendation 5

That the Government of Canada review the distribution mechanism of funding for research security among postsecondary institutions through the Research Support Fund, to ensure smaller institutions are not left behind.

CHAPTER 4. STRENGTHENING RESEARCH SECURITY

On 14 February 2023, the Honourable François-Philippe Champagne, Minister of Innovation, Science and Industry; the Honourable Jean-Yves Duclos, Minister of Health; and the Honourable Marco E. L. Mendicino, Minister of Public Safety, announced that research security measures would be strengthened.[199] The witnesses, who testified before the strengthened measures were published in January 2024, shared their observations with the Committee on the update that had been announced.

4.1 Establishing Lists of Sensitive Research Areas and Entities of Concern

Witnesses explained that a general ban on research partnerships with China would be counterproductive.[200] However, a recurring request from the witnesses who appeared before the Committee was for the government to publish a list of sensitive research areas and a list of entities that pose a risk to research security.[201]

The representatives of Universities Canada and the U15 Group noted that the university sector was awaiting the publication of these lists, because the lists would enable them

199 Government of Canada, *Statement from Minister Champagne, Minister Duclos and Minister Mendicino on protecting Canada's research*, News release, 14 February 2023.

200 SRSR, *Evidence*, 20 September 2023, 1635 and 1650 (Gordon Houlden); and Anna Puglisi, *Testimony before the House of Commons Science and Research Committee "Canadian research partnerships with entities connected to the People's Republic of China,"* Brief submitted to the House of Commons Standing Committee on Science and Research, 25 September 2023, pp. 11–12.

201 SRSR, *Evidence*, 20 June 2023, 1105 (Christian Leuprecht); SRSR, *Evidence*, 20 September 2023, 1635 (Gordon Houlden); SRSR, *Evidence*, 20 September 2023, 1705 (Cherie Wong); SRSR, *Evidence*, 25 September 2023, 1550 (Margaret McCuaig-Johnston); SRSR, *Evidence*, 4 October 2023, 1635 (Ivana Karaskova); and SRSR, *Evidence*, 4 October 2023, 1710 (Kevin Gamache).

to give researchers and research institutions a clearer indication of the relevant threats.[202]

Confirming the 14 February 2023 announcement, Minister François-Philippe Champagne told the Committee that the government was in the process of drawing up these lists, adding the following:

> In short, grant applications in sensitive research areas will not be funded if any researcher supported by the grant is either affiliated with or in receipt of funding or in-kind support from a research institution connected to military, national defence or foreign state security organizations posing a risk to Canada's national security.[203]

Several questions were put to Minister François-Philippe Champagne and to the representatives of ISED and Public Safety Canada regarding the preparation of these lists and why they still had not been published by late 2023.

Sébastien Aubertin-Giguère, Associate Assistant Deputy Minister of National and Cyber Security at the Department of Public Safety and Emergency Preparedness, discussed the difficulty in compiling lists of such complexity and explained that the government needed to talk to universities and security partners.[204] The Government of Canada–Universities Working Group was involved throughout the process.[205]

Minister François-Philippe Champagne explained that the government was also consulting with representatives of the Five Eyes while developing the lists of sensitive research areas and entities of concern.[206] The Five Eyes is "an intelligence alliance composed of Australia, Canada, New Zealand, the United Kingdom and the United States."[207] According to Minister François-Philippe Champagne, "Canada will be one of the only countries in the world … to have a specific list with the names of entities."[208] He stated that he believes the list "is going to serve as a benchmark not only for Canada but

202 SRSR, *Evidence*, 27 September 2023, 1725 (Philip Landon); and SRSR, *Evidence*, 27 September 2023, 1645 (Chad Gaffield).

203 SRSR, *Evidence*, 20 November 2023, 1555 (Hon. François-Philippe Champagne).

204 SRSR, *Evidence*, 23 October 2023, 1635 (Sébastien Aubertin-Giguère).

205 SRSR, *Evidence*, 20 November 2023, 1610 (Hon. François-Philippe Champagne).

206 Ibid., 1615.

207 Government of Canada, *Five Country Ministerial*.

208 SRSR, *Evidence*, 20 November 2023, 1615 (Hon. François-Philippe Champagne).

for the Five Eyes countries."[209] On the topic of international collaboration, ISED added that:

> Notably, Canada's engagement through the Group of Seven (G7) and the Organisation for Economic Co-operation and Development (OECD) have served to advance and establish meaningful research security activities. Represented by ISED, Canada is Co-Chair of the G7's Working Group on the Security and Integrity of the Global Research Ecosystem (SIGRE). This working group was established as a result of the G7 Research Compact, signed in summer 2021, which committed all members of the G7 to advancing shared research security priorities and established the Working Group.[210]

A number of witnesses noted that the lists will have to be kept up to date to account for changes in key sectors and certain actors' attempts to conceal their identities.[211] Shawn Tupper, Deputy Minister at the Department of Public Safety and Emergency Preparedness, stated that the lists published by the government would be updated regularly.[212]

Several witnesses expressed opinions on what should be on the lists. According to Christian Leuprecht, the list of problematic entities should include "about 200 Chinese institutions and companies, but also entities in Russia and Iran."[213] In a written brief, the same witness stated that the list of entities needed to include state-owned and state-directed enterprise:

> In the PRC in particular, but in other hostile states as well, there is no clear distinction between the public and private sector. Private-sector entities are ultimately subservient to the state, and instrumentalized by the state, in the case of the PRC for the purpose of CCP regime preservation and to advance the interests of the regime. Ergo, a federal list of excluded entities issued by the Government of Canada cannot achieve its intended aim if it does not [include] state-owned and state-directed enterprise, which is quite intentionally, deliberate and strategically being leveraged by defence, security and intelligence actors. State-owned and state-directed enterprise are being used both

209 Ibid., 1625.

210 ISED, *ISED Reply and follow up to the Minister of Innovation, Science, and Industry's Appearance before the Standing Committee on Science and Research (SRSR) on November 20, 2023*, p. 3.

211 SRSR, *Evidence*, 20 September 2023, 1710 (Cherie Wong); SRSR, *Evidence*, 20 September 2023, 1705 (Gordon Houlden); and SRSR, *Evidence*, 4 October 2023, 1710 (Kevin Gamache).

212 SRSR, *Evidence*, 22 November 2023, 1720 (Shawn Tupper).

213 SRSR, *Evidence*, 20 June 2023, 1105 (Christian Leuprecht).

> to conceal the footprint of defence, security and intelligence actors, and they are being leveraged to the bidding of defence, security and intelligence actors in abroad.[214]

Margaret McCuaig-Johnston was of the same opinion and stated that Chinese military and surveillance technology companies should be added to the list.[215]

On 16 January 2024, the Government of Canada published the list of sensitive technology research areas and the list of named research organizations as part of its new Policy on Sensitive Technology Research and Affiliations of Concern.[216] The list of sensitive technology research areas includes 11 research areas. The list of named organizations comprises 102 "organizations and institutions that pose the highest risk to Canada's national security due to their direct, or indirect connections with military, national defence, and state security entities."[217] It includes 85 organizations linked to the People's Republic of China, 11 organizations linked to Iran and six organizations linked to the Russian Federation. It includes universities, research institutes and laboratories, but not private companies or state-owned enterprises.

In light of the evidence, the Committee recommends:

Recommendation 6

That the Government of Canada consider adding State-owned or State-controlled enterprises to the list of named research organizations published in support of the Policy on Sensitive Technology Research and Affiliations of Concern.

Under the Policy on Sensitive Technology Research and Affiliations of Concern, researchers and institutions that apply for funding from the granting councils or the Canada Foundation for Innovation involving research that advances a sensitive technology research area will have to check and attest that the researchers involved are not affiliated with any of the entities on the list.[218]

---

214 Royal Military College of Canada, *SRSR: Research Partnerships with Entities Connected to the PRC*, Brief submitted to the House of Commons Standing Committee on Science and Research, 8 December 2023, p. 2.

215 SRSR, *Evidence*, 25 September 2023, 1530 (Margaret McCuaig-Johnston).

216 Government of Canada, *Sensitive Technology Research Areas*; and Government of Canada, *Named Research Organizations*.

217 Government of Canada, *Named Research Organizations*.

218 Government of Canada, *Policy on Sensitive Technology Research and Affiliations of Concern*.

The lists published in January 2024 will also be used to implement the 2021 Guidelines, which still apply.[219] The findings and impact of the Guidelines are also expected to be presented in an annual report: "[t]his publication will include information on the results of the implementation of the Guidelines and highlights other initiatives that are underway to safeguard Canadian science, data, and research."[220] In November 2023, after the Committee had heard from all the witnesses in this study, the government published its first progress report on the implementation of the Guidelines.[221]

Therefore, the Committee recommends:

Recommendation 7

That the Minister of Innovation, Science and Industry report to the House of Commons Standing Committee on Science and Research within a year on the implementation of the Policy on Sensitive Technology Research and Affiliations of Concern, including the following points:

- **any updates to the list of sensitive technology research areas and the list of named research organizations;**
- **the validation process to evaluate whether funding applications to the granting councils and the Canadian Foundation for Innovation are compliant with the policy;**
- **funding for research security for postsecondary institutions through the Research Support Fund; and**
- **awareness-raising efforts by the Government of Canada towards the research community.**

219 Ibid.

220 SSHRC, *SSHRC written brief for the House of Commons Standing Committee Science and Research, Canadian Research Partnerships with Entities Connected to the People's Republic of China*, December 2023, p. 4.

221 Government of Canada, *Progress Report on the Implementation of Canada's National Security Guidelines for Research Partnerships and Supporting Research Security Efforts*.

4.2 A Country-Agnostic Approach

During discussions with the witnesses, the issue of whether Canada should opt for a country-agnostic approach or take measures that specifically target China came up more than once.

The approach that the government took with the 2021 Guidelines does not target any country in particular. It was described as a "threat basis" approach.[222] That approach is "[n]ot to box ourselves into individual organizations and individual countries.... It's recognizing [that] those threats evolve and that to be able to respond, we need an ecosystem that is more capable and educated."[223]

Some witnesses expressed reservations about this type of approach. Gordon Houlden argued that "focusing on the most immediate problems is rational" and suggested concentrating on the countries that pose the most risk.[224] Margaret McCuaig-Johnston and Jeffrey Stoff expressed similar opinions.[225]

Conversely, several stakeholders suggested maintaining an approach that does not focus on one country in particular.[226] The Committee heard that focusing on China "singles out Chinese students who went to public institutions in China. This affects how the issue is portrayed in the media and may unintentionally exacerbate discrimination against students of Chinese origin."[227] This point was raised on several different occasions.[228] Alliance Canada Hong Kong noted that, "[s]ince the start of the COVID-19 pandemic along with growing geopolitical tensions with the [People's Republic of China], Asian and ethnic Chinese Canadians have experienced a surge in violence and hate crimes."[229]

---

222 SRSR, *Evidence*, 20 November 2023, 1715 (Francis Bilodeau).

223 Ibid.

224 SRSR, *Evidence*, 20 September 2023, 1650 (Gordon Houlden).

225 SRSR, *Evidence*, 25 September 2023, 1555 (Margaret McCuaig-Johnston).

226 SRSR, *Evidence*, 20 June 2023, 1105 (Christian Leuprecht); SRSR, *Evidence*, 20 September 2023, 1635 (Cherie Wong); SRSR, *Evidence*, 20 September 2023, 1710 (Benjamin Fung); SRSR, *Evidence*, 27 September 2023, 1635 (Philip Landon); SRSR, *Evidence*, 4 October 2023, 1700 (Ivana Karaskova); and SRSR, *Evidence*, 4 October 2023, 1710 (Kevin Gamache).

227 SRSR, *Evidence*, 27 September 2023, 1635 (Philip Landon).

228 SRSR, *Evidence*, 4 October 2023, 1720 (Kevin Gamache); and SRSR, *Evidence*, 20 November 2023, 1655 (Nipun Vats).

229 Alliance Canada Hong Kong, *Written Submission to the Standing Committee on Science and Research (SRSR)*, September 2023, p. 3.

Several witnesses stressed the importance of ensuring that the enhanced security measures do not have unintended negative consequences, such as discrimination or racism on campuses.[230] Christian Leuprecht argued that, on the contrary, it is in fact the government's inaction that could lead to these kinds of consequences by creating widespread uncertainty.[231] According to Minister François-Philippe Champagne:

> [b]y adopting a country-agnostic approach paired with a case-by-case risk assessment process, the government is mitigating the possibility of racial profiling within the research community while at the same time bolstering Canada's research security policies to account for the threats that originate from anywhere in the world.[232]

The Policy on Sensitive Technology Research and Affiliations of Concern that was announced in January 2024 states that it "remain[s] country-agnostic."[233] As noted above, the list of named entities unveiled by the government includes organizations with ties to China, Iran and Russia.

Therefore, the Committee recommends:

Recommendation 8

That the Government of Canada adopt measures to ensure that research security policies do not unintentionally exacerbate prejudice and discrimination against students and researchers of Asian origin on campuses and in the way research funding is distributed.

230 SRSR, *Evidence*, 27 September 2023, 1645 (Chad Gaffield); and SRSR, *Evidence*, 25 October 2023, 1715 (Ted Hewitt).

231 SRSR, *Evidence*, 20 June 2023, 1105 (Christian Leuprecht).

232 SRSR, *Evidence*, 20 November 2023, 1555 (Hon. François-Philippe Champagne).

233 Government of Canada, *Policy on Sensitive Technology Research and Affiliations of Concern*; Government of Canada.

4.3 Collaboration with Provinces

The testimony showed that research security requires a collaborative approach involving the federal government, the provinces and research sector stakeholders.[234]

Although the provinces are not part of the Government of Canada–Universities Working Group, witnesses explained that the federal government is in contact with the provinces to discuss and provide updates on the measures it is taking.[235]

Margaret McCuaig-Johnston stated that she would like the provinces to be at the table every step of the way and to be part of the decision making in terms of what is communicated to universities. However, she stated the following:

> All through this, the provinces have been inclined to say that this is national security and that national security is not their business—that's the federal government's business—but the federal government has their act together, is getting their act together now, and can help the provinces convey the message to their universities.[236]

According to ISED:

> In order to build a whole-of-government approach to research security, the federal government strongly encourages the provinces and territories to incorporate research security considerations into their own processes. This has been done through a series of Ministerial Letters that are sent to provincial and territorial government representatives. These documents offer updates and guidance on how federal research security policies can be implemented or adapted into provincial and territorial research funding practices. In addition, ISED's Science and Research Assistant Deputy Minister participates in a working group that includes senior provincial and territorial executives. This group continues to meet on a quarterly basis to discuss general updates and how multiple levels of government can work to align their evolving research security practices and policies.

---

234 SRSR, *Evidence*, 20 June 2023, 1105 (Christian Leuprecht); SRSR, *Evidence*, 20 September 2023, 1705 (Gordon Houlden); SRSR, *Evidence*, 25 September 2023, 1605 (Margaret McCuaig-Johnston); SRSR, *Evidence*, 4 October 2023, 1730 (Jim Hinton); SRSR, *Evidence*, 20 November 2023, 1605 (Hon. François-Philippe Champagne); SRSR, *Evidence*, 20 November 2023, 1700 (Nipun Vats); and Government of Ontario, *Use of Federal Government Research and Development Grants, Funds, and Contributions by Canadian Universities and Research Institutions in Partnerships With Entities Connected to the People's Republic of China*, Brief submitted to the House of Commons Standing Committee on Science and Research, 6 October 2023, p. 3.

235 SRSR, *Evidence*, 23 October 2023, 1605 (Sébastien Aubertin-Giguère); SRSR, *Evidence*, 25 October 2023, 1725 (Alejandro Adem); and SRSR, *Evidence*, 20 November 2023, 1720 (Nipun Vats).

236 SRSR, *Evidence*, 25 September 2023, 1550 (Margaret McCuaig-Johnston).

> […]
>
> The new National Counter Foreign Interference Coordinator will work on expanding briefing mechanisms with provincial/territorial, municipal, and Indigenous officials. The Protecting Democracy Unit within the Privy Council Office will expand its work with provinces and territories.[237]

The provincial governments have come up with their own research security initiatives. In a written brief, the Government of Ontario described the steps it had taken:

> Ontario, in partnership with colleges and universities in our province, began implementing a country-agnostic, risk-based security review for our competitive research programs in 2019.
>
> Any applicants who want to receive funding through our province's competitive research programs, must complete an Economic and Geopolitical Risk Checklist and disclose their foreign affiliations and sources of funding. Each application also undergoes a comprehensive scientific review, followed by a security review that is conducted by a dedicated security office within the Ministry of the Solicitor General. Each security review includes an analysis of the nature of the research, as well as the research team's collaborations with international partners. This comprehensive security review leverages both open-source websites and public information. Following the implementation of this approach in 2019, no research projects identified as 'high-risk' have received funding from the Ontario government.[238]

The Government of Ontario announced new measures in the fall of 2023, including the following:

- a new attestation and risk reduction/mitigation initiative that provides institutions and researchers the opportunity to address identified risks before funding decisions are made. This ultimately will help reduce the number of projects that are not funded due to security concerns;
- spot audits to confirm compliance with the agreed upon risk reduction and mitigation measures over the course of the projects; and

---

237 ISED, *ISED Reply and follow up to the Minister of Innovation, Science, and Industry's Appearance before the Standing Committee on Science and Research (SRSR) on November 20, 2023*, p. 8 and 11.

238 Government of Ontario, *Use of Federal Government Research and Development Grants, Funds, and Contributions by Canadian Universities and Research Institutions in Partnerships With Entities Connected to the People's Republic of China*, Brief submitted to the House of Commons Standing Committee on Science and Research, 6 October 2023, p. 2.

- annual disclosure of the institution's foreign relationships.[239]

In a written submission to the Committee, ISED also presented some measures adopted by the governments of Quebec, Alberta and Saskatchewan:

> In September 2021, the Quebec Government enacted Bill 64, now Law 25, which includes strengthened privacy rights for individuals and several controller requirements, such as privacy policies, risk assessments, and data breach notifications. Moreover, this Act created new obligations with which public bodies, including Quebec universities, must comply with. […] While Law 25 does not speak directly to research security due diligence, the protection of data can help ensure the confidentiality, integrity, and accessibility of data while research is being conducted.
>
> […]
>
> In May 2022, the Alberta Government provided an update to Comprehensive Academic and Research Universities, with the following directions:
>
> - Institutions are permitted to resume low-risk agreements with China, limited to undergraduate student mobility and transferability and corporate training opportunities.
> - Institutions are to pause agreements [with China] that involve:
>   - Graduate student research at the doctoral or post-doctoral level, and participation in programs of study/research that are related to areas of national and economic security for Canada and Alberta.
>   - Visiting researchers and post-doctoral fellows.
>   - Research commercialization, technology transfer, and intellectual property.
>
> […]
>
> In March 2022, the Government of Saskatchewan published a document titled "International Research Partnership Framework". This guidance offers institutions in the province with a proactive approach for mitigating risks related to research partnerships and innovation.

239 Ibid., pp. 2–3.

- This framework aligns closely with the federal government's *National Security Guidelines for Research Partnerships*, as well as Saskatchewan's post-secondary institution principles.

- In Saskatchewan, as in other provinces, post-secondary institutions have instituted a variety of policies and practices to ensure oversight and accountability in their research projects. These policies detail the expectations and processes researchers are expected to follow to ensure safe and ethical research practices.[240]

A number of witnesses highlighted the importance of federal leadership in creating a clear framework that the provinces can follow, particularly since the provinces may not have the necessary resources to analyze international security risks.[241]

240 ISED, *ISED Reply and follow up to the Minister of Innovation, Science, and Industry's Appearance before the Standing Committee on Science and Research (SRSR) on November 20, 2023*, p. 10-11.

241 SRSR, *Evidence*, 20 September 2023, 1715 (Gordon Houlden); SRSR, *Evidence*, 25 September 2023, 1605 (Margaret McCuaig-Johnston); SRSR, *Evidence*, 20 November 2023, 1620 (Hon. François-Philippe Champagne); and SRSR, *Evidence*, 20 November 2023, 1720 (Nipun Vats).

APPENDIX A:
LIST OF WITNESSES

The following table lists the witnesses who appeared before the committee at its meetings related to this report. Transcripts of all public meetings related to this report are available on the committee's webpage for this study.

Organizations and Individuals	Date	Meeting
As an individual	2023/06/20	51
Jim Hinton, Intellectual Property Lawyer		
Christian Leuprecht, Professor, Royal Military College of Canada		
Alliance Canada Hong Kong	2023/09/20	53
Benjamin Fung, Canada Research Chair and Professor, McGill University		
Cherie Wong, Executive Director		
University of Alberta - China Institute	2023/09/20	53
Gordon Houlden, Professor and Director Emeritus		
As an individual	2023/09/25	54
Margaret McCuaig-Johnston, Senior Fellow, Graduate School of Public and International Affairs and Institute of Science, Society and Policy, University of Ottawa		
Anna Puglisi, Senior Fellow, Center for Security and Emerging Technology, Georgetown University		
Center for Research Security and Integrity	2023/09/27	55
Jeffrey Stoff, President		
U15 Group of Canadian Research Universities	2023/09/27	55
Chad Gaffield, Chief Executive Officer		
Universities Canada	2023/09/27	55
Philip Landon, Interim President and Chief Operating Officer		

Organizations and Individuals	Date	Meeting
As an individual	2023/10/04	56
Jim Hinton, Intellectual Property Lawyer		
Ivana Karaskova, China Projects Lead, Association for International Affairs (AMO)		
Texas A and M University System Research Security Office	2023/10/04	56
Kevin Gamache, Associate Vice Chancellor and Chief Research Security Officer		
Canadian Security Intelligence Service	2023/10/23	59
Nicole Giles, Senior Assistant Deputy Minister, Policy and Strategic Partnerships		
René Ouellette, Director General, Academic Outreach and Stakeholder Engagement		
Communications Security Establishment	2023/10/23	59
Sami Khoury, Head, Canadian Centre for Cyber Security		
Samantha McDonald, Assistant Deputy Minister, Innovative Business Strategy and Research Development		
Department of Public Safety and Emergency Preparedness	2023/10/23	59
Sébastien Aubertin-Giguère, Associate Assistant Deputy Minister, National and Cyber Security		
Lesley Soper, Director General, National Security Policy		
Canadian Institutes of Health Research	2023/10/25	60
Christian Baron, Vice-President, Research - Programs		
Natural Sciences and Engineering Research Council	2023/10/25	60
Alejandro Adem, President		
Manal Bahubeshi, Vice-President, Research Partnerships		
Social Sciences and Humanities Research Council	2023/10/25	60
Ted Hewitt, President		
Valérie La Traverse, Vice-President, Corporate Affairs		
Valérie Laflamme, Associate Vice-President, TIPS		

Organizations and Individuals	Date	Meeting
Department of Industry	2023/11/20	65
Francis Bilodeau, Associate Deputy Minister		
Hon. François-Philippe Champagne, P.C., M.P., Minister of Innovation, Science and Industry		
Nipun Vats, Assistant Deputy Minister, Science and Research Sector		
Canadian Security Intelligence Service	2023/11/22	66
Nicole Giles, Senior Assistant Deputy Minister, Policy and Strategic Partnerships		
David Vigneault, Director		
Department of Public Safety and Emergency Preparedness	2023/11/22	66
Sébastien Aubertin-Giguère, Associate Assistant Deputy Minister, National and Cyber Security		
Shawn Tupper, Deputy Minister		

APPENDIX B:
LIST OF BRIEFS

The following is an alphabetical list of organizations and individuals who submitted briefs to the committee related to this report. For more information, please consult the committee's webpage for this study.

Alliance Canada Hong Kong

Canadian Institutes of Health Research

Center for Research Security and Integrity

Government of Ontario

Natural Sciences and Engineering Research Council

Puglisi, Anna

Royal Military College of Canada

Social Sciences and Humanities Research Council

REQUEST FOR GOVERNMENT RESPONSE

Pursuant to Standing Order 109, the committee requests that the government table a comprehensive response to this Report.

A copy of the relevant *Minutes of Proceedings* (Meetings Nos. 51, 53, 54, 55, 56, 59, 60, 65, 66, 77 and 79) is tabled.

Respectfully submitted,

Lloyd Longfield
Chair

Dissenting Report of His Majesty's Official Opposition

The Conservative Party of Canada

MP Corey Tochor - Saskatoon—University

MP Gerald Soroka - Yellowhead

MP Ben Lobb - Huron—Bruce

Hon. Michelle Rempel Garner, PC, MP - Calgary Nose Hill

Introduction

Canada should be a leader on the international stage in ensuring our Intellectual Property (IP) is protected and our research partnerships are beneficial and secure. The testimony we heard from this study made it clear that this is not the current state of our research partnerships in Canada and that the Government of Canada must do more to bolster national security in the context of the research partnerships that Canadian institutions can pursue. However this Liberal government's repeated delays on releasing the long needed guidance on these partnerships until after testimony for this report was essentially complete have undermined the committee's ability to properly investigate and recommend decisions going forward.

This dissenting report provides clarity on several key points that were not addressed or adequately captured by the report and additional recommendations to address the issue of Canadian research partnerships with entities connected to the People's Republic of China (PRC).

1. Canada urgently needs a foreign influence registry

Witness after witness made clear that Canada needs to act on a foreign influence registry. Benjamin Fung, a Canada Research Chair and Professor at McGill University who is also with the Alliance Canada Hong Kong stated "Yes, definitely. A foreign registry would help."[1] The Alliance Canada Hong Kong also made reference to "a registry of foreign principals and their proxies" in

[1] SRSR, Sept 20, 2023, 1640, https://www.ourcommons.ca/DocumentViewer/en/44-1/SRSR/meeting-53/evidence

their briefing submission[2]. Dr. Christian Leuprecht, a Professor at the Royal Military College of Canada, noted that there had been a number of significant changes in Australia on this issue, and included reference to a foreign influence registry in Australia in his comments as well[3]. After continuous calls from the Conservative Opposition, the Liberal government said they would table a bill on a foreign influence registry. But despite closing consultations in the previous spring they continue to delay.[4]

The longer the government waits, the worse off our country will be in terms of research security. We call on the government to act on this important matter with the below recommendation, which was not included in the Committee's report

Recommendation 1: The federal government immediately establish a foreign influence registry, as called for by the Conservative opposition.

2. **Universities do not currently have the capacity to make proper decisions on safe partnerships and the committee has not had the opportunity to adequately scrutinize new guidelines due to the government's delays in releasing them.**

We heard very clear testimony that universities do not have the capacity to screen for national security threats before they engage in research partnerships. As Mr. Hinton, an IP lawyer stated, "I don't think universities are capable of screening national security issues. They're not resourced. They don't have the wherewithal and they're not experts."[5]

This is something the government needs to acknowledge and take action on, to ensure the safety of our research partnerships. Months ago, the Conservative Opposition made clear that Canadian universities should be banned from doing research projects in alliance with foreign

[2] SRSR, Alliance Canada Hong Kong, page 10, Brief, https://www.ourcommons.ca/Content/Committee/441/SRSR/Brief/BR12599027/br-external/AllianceCanadaHongKong-e.pdf

[3] SRSR, June 20, 2023, 1130, https://www.ourcommons.ca/DocumentViewer/en/44-1/SRSR/meeting-51/evidence

[4] "Consultation on a foreign influence transparency registry" Public Safety Canada, https://www.canada.ca/en/services/defence/nationalsecurity/consultation-foreign-influence-transparency.html

[5] SRSR, June 20, 2023, 1120, https://www.ourcommons.ca/DocumentViewer/en/44-1/SRSR/meeting-51/evidence

dictatorships[6]. The Conservative Opposition recommended, months ago, that the government issue a ministerial order to advise provinces and Canadian universities to ban research partnerships with the PRC[7]. As evidenced clearly by the testimony we heard from Dr. Chad Gaffield, the CEO of U15 Group of Canadian Research Universities, "The national intelligence services obviously have great capacity that we don't have on our campuses."[8] The government must recognize this capacity gap and act.

We heard much testimony that a list of entities which institutions should not conduct research with is in the works[9]. However, we did not have the opportunity to see such a list and what it would include prior to the closing of witness testimony for this report. We clearly heard from witnesses that the list needs to be evergreen, including from witnesses such as Dr. Chad Gaffield[10]. Dr. Christian Leuprecht also aptly noted that "The government must muster the courage to list problematic entities, which includes about 200 Chinese institutions and companies, but also entities in Russia and Iran, for instance. Researchers must have clarity about which affiliations are problematic."[11] Unfortunately the list which the government ultimately released lacked the courage that Canada needs. Furthermore, although the government finally released a Policy on Sensitive Technology Research and Affiliations of Concern in 2024 we would reiterate that the decision to delay release of the list until 2024 means that it was delayed until after the passing of an additional grant funding cycle, essentially choosing to "kick the can down the road" for another year. The excuses from the government, including Minister Champagne, for why it took them so long to release the list ring hollow given, as established in this report, that there has been a decisive shift in Canada-People's Republic of China relations since 2017, the government has had many years to recognize and rectify what has been occurring since they took office, and have repeatedly chosen to delay action.

These delays have imposed unacceptable pressures on Canadian academic bodies who have been left without the guidance from government that they required and have put Canadian interests at risk. The Liberal delays in putting forward their guidelines have not only effectively delayed the impact of these guidelines for another year but have also effectively undermined this study, given that the guidelines were only released after the committee received testimony.

---

[6] Global News, Feb 15, 2023, https://globalnews.ca/news/9488207/canada-china-research-crackdown/

[7] Globe and Mail, Jan 30, 2023, Ottawa urged to issue directive to universities halting joint research with Chinese military scientists - The Globe and Mail

[8] SRSR, Sept 27, 2023, 1715, https://www.ourcommons.ca/DocumentViewer/en/44-1/SRSR/meeting-55/evidence

[9] SRSR, Sept 27, 2023, 1710, https://www.ourcommons.ca/DocumentViewer/en/44-1/SRSR/meeting-55/evidence

[10] SRSR, Sept 27, 2023, 1650, https://www.ourcommons.ca/DocumentViewer/en/44-1/SRSR/meeting-55/evidence

[11] SRSR, June 20, 2023, 1105, https://www.ourcommons.ca/DocumentViewer/en/44-1/SRSR/meeting-51/evidence

Clearly the report needs to be revised so that the committee can receive new testimony on the long delayed list, and any adjustments that will be needed to ensure that Canadian research remains safe.

The failure to specifically proscribe organizations such as Huawei represents a terrible blow to the credibility of the latest Liberal policies. Contrary to Liberal claims this is clearly an ongoing issue as can be seen in the recent decision by the Openmind Research Institute in Alberta to partner with Huawei on research in the critical field of artificial intelligence.[12] Given the dangers posed by the risk of advanced artificial intelligence falling into the wrong hands it remains shocking that the Liberals refuse to specifically name Huawei.

As David Vigneault, the director of the Canadian Security Intelligence Service has publicly warned, the risks posed by the People's Republic of China have advanced to such a level that "Everything that they're doing in our universities and in new technology, it's going back into a system very organized to create dual-use applications for the military" and, given that this committee has received expert testimony characterizing this as an "existential threat" the dangers of advanced AI falling into the wrong hands, and the public warnings from the Director of CSIS that "Everything that they're doing in our universities and in new technology, it's going back into a system very organized to create dual-use applications for the military" and, given that this committee has further received expert testimony characterizing this as an "existential threat" to Canada, the failure of this government to adequately protect Canadian research remains unacceptable.

This has been made increasingly clear as for example in how the Liberals and their coalition partners in the NDP have sought to supress investigation into the Winnipeg Lab leaks.[13] Even going so far as to take a Liberal Speaker to court in a shocking violation of parliamentary privilege in an attempt to suppress that information. [14] Ultimately their record shows that they will do anything to hide their repeated failures and their refusal to release the new guidelines until it was too late for this committee to properly scrutinize them is unfortunately a part of this pattern.

Recommendation 2: The government should issue a ministerial order to advise provinces and Canadian universities to ban research partnerships with the PRC and foreign dictatorships, which should include an evergreen list of entities which research should not be conducted with.

[12] Globe and Mail, Top AI researcher launches new Alberta lab with Huawei funds after Ottawa restrictions November 24, 2023

[13] National Post, March 26, 2024, Second time is the charm: Conservatives succeed in launching probe into Winnipeg lab documents

[14] Globe and Mail, August 17, 2021, https://www.theglobeandmail.com/politics/article-speaker-anthony-rota-cites-afghan-detainee-matter-in-court-dispute/

Recommendation 3: The Science and Research Committee should receive further witness testimony, including from the responsible minister, in order to ensure that we can properly study the government's long delayed policy and issue appropriate recommendations in an up to date report.

Conclusion

The Liberal government has failed to adequately prioritize protecting our research, our valuable intellectual property and our research institutions from dangerous relationships with regimes such as the PRC. We cannot allow this to go on any longer. As this dissenting report clearly explains, the government must act. We cannot allow the NDP-Liberal Government to stall on this any longer.

Supplementary Report From a Member of the Bloc Québécois

The Bloc Québécois member of the Standing Committee of Science and Research would like to thank the staff of the Library of Parliament, the clerks, and the interpreters for all the work made during this study. He would also like to acknowledge the essential contribution of the witnesses for their enlightening presentations.

This supplementary report aims to highlight the fourth recommendation of this report, which restricts scientific freedom, and likely violates the areas of jurisdiction of Quebec.

> "That the Government of Canada consider adopting enforcement measures to ensure that postsecondary institutions follow the National Security Guidelines for Research Partnerships and the Policy on Sensitive Technology Research and Affiliations of Concern to qualify for funding from the federal government."

While the three federal granting agencies fund only about 10% of research in Canada, universities are responsible for finding the remaining 90%, funded by provinces, industry, private actors and foreign states.

Putting additional conditions on this financing, which is already difficult to access and therefore few, is not necessary, especially since it is the main lever of the federal government.

At this stage, it is also undesirable to see that the federal government could use funds as a weapon to enforce and adopt conduct, moreover, in the field of education, which is the exclusive responsibility of Quebec.

Therefore, it is preferable to withdraw this recommendation, and leave the implementation of such measures to the provinces and Quebec.