Mitigating economic and/or geopolitical risks in sensitive research projects

A TOOL FOR UNIVERSITY RESEARCHERS

December 2019

This document is meant to be adapted as needed by institutions to complement their own policies and tools.

This publication is available online at:
https://www.univcan.ca/wp-content/uploads/2020/08/mitigating-economic-and-or-geopolitical-risks-in-sensitive-research-projects-dec-2019.pdf

Authors

Guidelines and assessment tools were developed by the U15 Group of Canadian Research Universities and Universities Canada in collaboration with the Government of Canada-Universities Working Group. Although many people were involved in the publication's development, one primary contact is identified here for ease of reference.

Universities Canada
1710-350 Albert Street
Ottawa, Ontario
K1R 1B1, CANADA
Tel: 613-563-1236
Fax: 613-563-9745

Permission to Reproduce

Innovation, Science and Economic Development Canada
Cat. No. Iu37-22/2020E-PDF
ISBN 978-0-660-35965-6

Aussi offert en français sous le titre *Atténuer les risques économiques et géopolitiques associés aux projets de recherche sensibles*

Table of Contents

Introduction

The scope for research collaboration across borders and disciplines is expanding. The diffusion of data and research results is accelerating. Having a world-class university research ecosystem that can capitalize on these trends benefits Canada by creating exciting opportunities for increased societal well-being and economic growth. Around the world, other governments have recognized the strategic and economic imperative of having world-class university research and are investing at unprecedented levels – creating stronger collaborators and competitors. This is a global research ecosystem that is rich with new opportunities and new challenges.

At the core of world-class university research is academic freedom. It empowers researchers to undertake important work in sensitive areas. However, researchers need more than just the right to pursue research on these topics; they need to be equipped to safely and freely pursue research. In the current context, that means having resources to help them assess and manage risks which emerge as a result of how the research topic intersects with domestic or international economic, political and strategic interests (economic and geopolitical risks). ***Research on emerging technologies with potential military application or in areas where significant political, social or economic interests exist will often have economic or geopolitical risks.***

Managing these risks often requires knowledge in areas unrelated to the research team's expertise including cybersecurity, verifying the professional history of potential team members and assessing the economic and geopolitical context. While due diligence processes can seem daunting, there are a number of relatively easy steps researchers can take to assess and mitigate a project's exposure to these risks.

Our hope is that this guide will provide researchers and research services offices with practical advice and best practices to undertake an economic and geopolitical risk assessment and mitigate key risks.

Although this guide was developed in consultation with experts and covers many scenarios, every research project is unique. An individual project may require additional risk mitigation measures. Equally, not all elements in this guide will apply to every project.

In addition to this guide, each university will have a range of resources, policies and processes to help researchers identify and manage risk. These institutional resources also provide critical supports for a range of scenarios not covered in this guide, including partner financial due diligence, compliance with export control laws and regulations, as well as other legal or ethical requirements. For any project, especially those with significant economic or geopolitical risks, researchers should actively leverage the full range of institutional resources to help ensure a successful project.

By equipping researchers to take advantage of collaborative research opportunities while managing economic and geopolitical risks, Canada's research ecosystem will thrive. We hope this tool will be useful in this process. For your convenience, we have created an abbreviated checklist which can be found in Appendix B.

Exposure to economic and geopolitical risks

While most research projects are likely to have a low economic and/or geopolitical risk profile, taking a few minutes to proactively assess the risk profile of your project can help you decide more confidently on which, if any, risk mitigation measures are appropriate. In assessing your project's exposure to economic or geopolitical risks, you should look for external indicators of risk and consider the economic and geopolitical context of your research project.

Identifying external indicators of risk

In addition to proactively assessing your project for impacts that create economic or geopolitical risks, you should watch for external risk indicators, including:

- Offers of funding where the ultimate source of money and/or value to the funder is unclear.
- Collaborations or partnerships where you are asked not to report some/all activities to your institution or not to adhere to your institution's policies and practices. This could include offers to fund your work with cash.
- Pricing from potential suppliers that is significantly below market rate and possibly even below cost.
- You are working with items covered by Canada's Export Control List.[1]

If any of the above factors apply to you, it is important to enlist your institution's research services or partnerships office. Once you have addressed the specific indicator (e.g. by declining suspicious funding or selecting a different partner or supplier), you should invest some time in assessing whether this concern was an indicator of a larger set of economic or geopolitical risks using the process below.

Assessing economic and geopolitical context

Even if there are not any obvious indicators of risk, assessing the risk profile of your project is important. To assess whether your project may be of interest to a malicious actor and warrant extra mitigation measures, you should consider your research's potential to impact their economic, domestic or international political ambitions. The higher the probability and scale of these impacts, the more motivated someone might be to steal, compromise or discredit your work.

One way to quickly assess your project is to use the table on page 5, then compare your results in the color-coded risk matrix (Figure 1) to determine next steps.

Instructions:

1. For each economic or geopolitical dimension in the table on page 5, use the search terms to conduct an advanced online search. Replace "***[your research topic]***" with your actual research topic.
2. Based on the results of your search, assess whether your research could have a ***small***, ***medium or large*** impact on the economic or geo-political dimension. Indicate this in the "Size" column.
3. Based on the results of your search, assess whether the probability your research will have the above impact as being ***low***, ***medium or high***. Indicate this in the "Probability" column.

1 https://www.international.gc.ca/controls-controles/about-a_propos/expor/guide-2016.aspx?lang=eng

	Geopolitical impact of research	
	Size	**Probability**
Potential for commercial impact If you are not sure about your project's potential for commercial value, you can try an advanced online search for: *[your research topic] AND ("cost reduction" OR "revenue growth" OR "market size")*		
Potential for national security impact If you are not sure about your project's potential for significant national security impact, you can try an advanced online search for: *[your research topic] AND ("military" OR "defence" OR "security" OR 'intelligence")*		
Potential to impact domestic or international political interests If you are not sure about your project's potential impact on political interests, you can try advanced online searches for: • *[your research topic] AND ("human rights" OR "democracy" OR "authoritarian" OR "state-sponsored")* • *[your research topic] AND ("militant" OR "extremist")*		

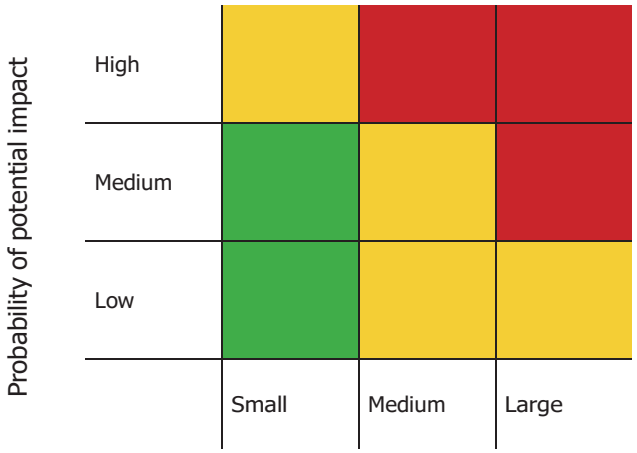
Having assessed your project's exposure in several areas of economic or geopolitical risks, you can now apply that assessment using the risk matrix to the right to help you decide on appropriate next steps.

Three possible avenues for next steps are:

- **Low risk (green):** use standard processes to protect your research.
- **Medium risk (yellow):** consider implementing additional risk assessment and mitigation measures to address risk, such as those suggested in this guide, in consultation with your research office.
- **High risk (red):** consult with your research office as a first step and seek appropriate guidance to further assess identified risks and implement significant mitigation measures.

Best practices to help you mitigate risks are the focus of the rest of this guide.

Fig. 1 Risk Matrix



Mitigating economic and geopolitical risks

Building a strong project team

The integrity of your research, particularly in sensitive areas and with international collaborators, relies heavily on knowing and trusting the people who make up your research team (researchers, fellows, graduate students, etc.). In sensitive areas, people may be more motivated to misrepresent themselves to gain access to information. Strong, trust-driven research teams set the foundation to pursue research in sensitive areas with a high degree of confidence.

Best practice checklist for sensitive projects

❒ ***Verify all team members' professional history and assess alignment with the research priorities for this project.***

Conduct appropriate reference checks and due diligence on all members of the team. Are their credentials, publications and affiliations in line with what they told you? Consider asking colleagues who may have more direct knowledge of the individual than you, and review the individual's publication history and affiliations through SCOPUS or a similar tool.

❒ ***Assess existing or potential conflicts of interest or affiliation that would impede collaboration with any team member.***

Ask yourself, "Could critics use the interests or affiliations of my team members to discredit our findings, regardless of the quality of the research itself?"

❒ ***Discuss and agree on a clear set of goals and measures of success for the project with all team members.***

Developing and discussing "S.M.A.R.T." goals (goals that are specific, measurable, achievable, relevant, time-bound) with your team can help ensure alignment and avoid disagreements once the project is underway. An introduction to S.M.A.R.T goals can be found at https://www.smartsheet.com/blog/essential-guide-writing-smart-goals.

❒ ***Discuss project risks internally and make a plan for their mitigation, involving external team members as appropriate.***

Brainstorm potential project risks with your team and fill out a risk register. For more information on risk registers, visit https://www.smartsheet.com/risk-register-templates.

❒ ***Assess whether the practices of your collaborator(s) and/or collaborating institution(s) are consistent with your institution's standards on ethics and research conduct.***

Ask yourself whether all aspects of the project, regardless of where the work is or was performed, would pass ethics review at your institution.

Non-academic partners

Collaboration with non-academic partners from industry or the not-for-profit sector bring significant benefits. When working with non-academic partners, it is important to ensure alignment with your research objectives. In projects where there are significant macro-risks, it is especially important to ensure non-academic partners do not have ulterior motives.

Best practice checklist for sensitive projects

- ❒ ***Ensure the motivations of all partners are clear and aligned with the goals of the research team, including any expectations about intellectual property.***

Ask the partner directly what they expect from the research team during the project and what they hope to get out of the project at the end.

- ❒ ***Assess if the partner's governance structure is transparent and whether the ultimate beneficiary of their collaboration on your project is clear.***

Looking on the partner's website, can you easily identify who leads the partner organization and any linkages to government, other organizations and/or other actors? What information gaps exist?

- ❒ ***Assess the reputational risk associated with involving the partner.***

Ask yourself, "Could critics use the involvement of the partner to discredit our findings, regardless of the quality of the research itself?"

- ❒ ***Explore if other academics have had positive experiences collaborating with this partner.***

By reaching out to researchers across your institution and at other institutions, you can gather valuable information on past experiences and solutions to address concerns.

- ❒ ***Assess whether the practices and contributions of your partner(s) are consistent with the standards on ethics and research conduct at your own institution.***

Ask yourself whether any contributions (data, background IP, etc.) are consistent with your values and would pass ethical review at your institution.

Cybersecurity and data management

The technological revolution has opened the doors to greater research collaboration by facilitating sharing of data and results in real time. When conducting research in sensitive areas, additional measures may be required to balance the need for data access with protection from unauthorized access or theft. Ensuring adequate cybersecurity and data management policies, practices and infrastructure are in place and agreed on by all research team members and partners is important to ensuring publications are not scooped, or the integrity of research is not compromised.

Best practice checklist for sensitive projects

- ❒ ***Verify that all team members have completed cyber hygiene and data management training.***

Discuss appropriate training options with your CIO or with the relevant resource person in your institution.

- ❒ ***Assess if the data management and cybersecurity measures needed to adequately protect research integrity are in place across all partners.***

Consult your institution's policies and practices. Public Safety Canada and the Canadian Centre for Cyber Security offer general and research-specific resources and best practices.

- ❒ ***Focus on addressing divergent cybersecurity and data management practices and decide on a mutually acceptable approach to securing your research project.***

When reflecting on existing divergences, ask yourself, "Given the sensitivity of the research topic and data, what is the level of risk associated with a breach and what is the probability it may occur?"

- ❒ ***If professional or personal international travel is expected during the project, agree to a protocol for device management.***

Consult with your institutional leads about the availability of temporary phone and laptops and other recommended practices. Additional guidance is available from the Australian Cyber Security Centre's Travelling Overseas with Electronic Devices guide.

Use of research findings

Publishing research findings and/or generating IP are key forms of academic currency. Industry and research partners, both in Canada and abroad, may have different interests than academics when it comes to IP ownership and publication of research results. In addition, all research partners may not enjoy the right to academic freedom, thereby potentially limiting the ability to publish results.

Best practice checklist for sensitive projects

- ❒ ***Agree to a plan of how and when you will share details about the project, including publication, conferences, teaching, mass media, social media and personal communication. This will increase effectiveness and minimize disagreement later.***

The UK's Health Foundation has a Communications in Health Care Improvement toolkit that could provide a good starting point. Keep in mind that premature disclosure can preclude certain types of IP protections.

- ❒ ***Assess the potential value of any project-related IP and what you need to do to protect it.***

Ask yourself, "What types of IP could be generated through this research project? What do we need to do to preserve the value of this IP?"

- ❒ ***Ensure all collaborators and partners have agreed on how IP will be handled.***

Your institution's research services office can help you understand your institution's policies with regard to IP, as well as how policies, laws and enforcement might vary across relevant institutions and countries.

- ❒ ***Discuss how restrictions on academic freedom or commercial interests may impact the research project and the communication of research results.***

Ask yourself, "Do the restrictions imposed on communicating results have potentially harmful impacts on the integrity of our research or our ability to publish results?"

- ❒ ***Ensure all collaborators and partners are comfortable with the likely uses of any research results.***

Brainstorm with your team the likely uses of the results of the project, then ask members if they remain comfortable proceeding with the project.

- ❒ ***Ensure mechanisms exist that guarantee that any graduate students involved in the project are able to use the results to complete their studies.***

Verify with your research or partnership office what measures exist at your institution and make all partners and collaborators aware of this requirement.

International travel

Today, researchers travel so frequently that we assume it is low risk. However, when working on a project with economic and/or geopolitical risks, international travel requires greater attention than normal. Once you are in another country, the legal protections and norms you are accustomed to in Canada may not apply. In addition, you are in less familiar surroundings with a less robust support network. Malicious actors can and do use these realities to their benefit.

Best practice checklist for sensitive projects

❒ ***Review government travel advisories and register travel to any countries associated with the research project.***

The Government of Canada's travel advisories provide relevant security information for regions around the world and enable you to register your travel before leaving.

❒ ***Assess any potential risks to team members in regards to human rights, particularly minority rights, in any country where travel is required for the project.***

Consult Government of Canada's travel.gc.ca website, including the Travel Health and Safety webpage and the Lesbian, gay, bisexual, transgender, queer and two-spirit Canadians abroad webpage to identify potential risks. The Travel Advice and Advisories webpage also offers region-specific information regarding ethnic tensions and other threats to members of other minority groups.

❒ ***Review your cyber hygiene before travel.***

Review the Canadian Centre for Cyber Security's guidance on mobile devices and business travellers as part of your preparations. Additional guidance is available from the Australian Cyber Security Centre's guide on travelling overseas with electronic devices.

❒ ***Review the Travel security guide for university researchers and staff.***

The guide provides a checklist of security steps that can be taken before, during and after travel.

Appendix A: Recommended resources

Additional resources that may be helpful in understanding the current context, particularly the intersection between geopolitical issues and technological innovation and risk, are listed below.

- Australian Strategic Policy Institute (ASPI) – International Cyber Policy Centre (ICPC): https://www.aspi.org.au/program/international-cyber-policy-centre
- Center for a New American Security (CNAS) – Technology & National Security program: https://www.cnas.org/research/technology-and-national-security
- Center for protection of national infrastructure (CPNI) - Trusted research guidance for academics: https://www.cpni.gov.uk/trusted-research
- Center for Strategic & International Studies (CSIS) – Technology Policy Program: https://www.csis.org/programs/technology-policy-program
- Georgetown University – Center for Security and Emerging Technology (CSET): https://cset.georgetown.edu
- Stockholm International Peace Research Institute (SIPRI) – Dual-use and arms control: https://www.sipri.org/research/armament-and-disarmament/dual-use-and-arms-trade-control
- U.S. Department of Homeland Security (DHS) – 2018 Public-Private Analytic Exchange Program report entitled *Emerging Technology and National Security: Findings and recommendations to develop and deploy advanced technologies through effective partnerships that promote economic, technological, and national security competitiveness*. Available at: https://www.dhs.gov/sites/default/files/publications/2018_AEP_Emerging_Technology_and_National_Security.pdf

Appendix B: Research partnership worksheets

When determining how to manage a research project, assessing the project's risk profile is important. While most research projects are likely to have a low economic and/or geopolitical risk profile, taking a few minutes to proactively assess the risk profile of your project can help you more confidently decide on appropriate risk mitigation measures.

Step 1: Preliminary risk analysis

a. Assess whether there are any indicators of risk (IoR).

	Yes	No
There is an offer of funding where the ultimate source of the money and/or value to the funder is unclear.		
You have been asked not to report some/all activities to your institution and/or not to adhere to your institution's policies and practices. This could include offers to fund your work with cash.		
Pricing from potential suppliers is significantly below the market rate and possibly even below cost.		
You are working with items covered by Canada's Export Control List.[2]		

If you answered "Yes" to any of indicators of risk, it is important to enlist your institution's research services or partnerships office. Once you have addressed the specific indicator, you should proceed with the broader risk assessment below.

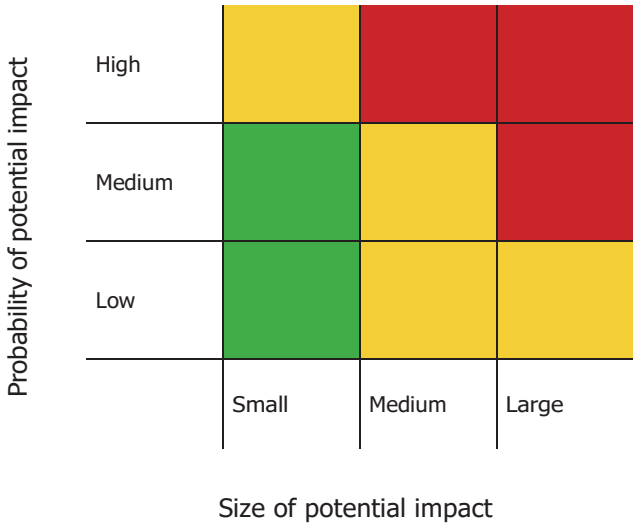
2 https://www.international.gc.ca/controls-controles/about-a_propos/expor/guide-2016.aspx?lang=eng

b. Assess the level of interest a malicious actor may have in your research. Consider the scale of potential economic and geopolitical impacts from your research and the probability of those impacts occurring. Compare your results with the risk matrix and determine what mitigation steps are required (e.g. none, the mitigation measures contained in this guide, engaging your institutions research office, etc.).

	Geopolitical impact of research	
	Size	Probability
Potential for commercial impact		
Potential for national security impact		
Potential to impact domestic or international political interests		

- **Low risk (green):** use standard processes to protect your research.
- **Medium risk (yellow):** consider implementing additional risk assessment and mitigation measures to address risk, such as those suggested in this guide, in consultation with your research office.
- **High risk (red):** consult with your research office as a first step and seek appropriate guidance to further assess identified risks and implement significant mitigation measures.

Fig. 1 Risk Matrix



Step 2: Mitigating economic and geopolitical risk checklist

Build a strong project team

- ❒ Verify all team members' professional history and assess alignment with the research priorities for this project.
- ❒ Assess existing or potential conflicts of interest or affiliation that would impede collaboration with any team member.
- ❒ Discuss and agree on clear goals and measures of success for the project.
- ❒ Discuss project risks internally and make a plan for their mitigation, involving external team members as appropriate.
- ❒ Assess whether the practices of your collaborator(s) and/or collaborating institution(s) are consistent with your institutions' standards on ethics and research conduct.

Assess non-academic partners

- ❒ Ensure the motivations of all partners are clear and aligned with the goals of the research team, including any expectations about intellectual property.
- ❒ Assess if the partner's governance structure is transparent and whether the ultimate beneficiary of their collaboration on your project is clear.
- ❒ Assess the reputational risk associated with involving the partner.
- ❒ Explore if other academics have had positive experiences collaborating with this partner.
- ❒ Assess whether the practices and contributions of your partner(s) are consistent with the standards on ethics and research conduct at your own institution.

Cybersecurity and data management

- ❒ Verify all team members have completed cyber hygiene and data management training.
- ❒ Assess if data management and cybersecurity measures needed to adequately protect research integrity are in place across all partners.
- ❒ Focus on addressing divergent cybersecurity and data management practices and decide on a mutually acceptable approach to securing your research project.
- ❒ If professional or personal international travel is expected during the project, agree to a protocol for device management.

Review use of research findings

- ❒ Agree to a plan regarding how and when project details will be shared including through publications, conferences, teaching, mass media, social media and personal communications.
- ❒ Assess the potential value of any project-related IP and how to protect it.
- ❒ Ensure all collaborators and partners have agreed on how to handle IP.
- ❒ Discuss how restrictions on academic freedom or commercial interests may impact the research project and the communication of research results.
- ❒ Ensure all collaborators and partners are comfortable with the likely uses of any research results.
- ❒ Ensure mechanisms exist that guarantee that any graduate students involved in the project are able to use the results to complete their studies.

International travel

- ❒ Review government travel advisories and register travel to any countries associated with the research project.
- ❒ Assess any potential risks to team members in regards to human rights, particularly minority rights, in any country where travel is required for the project.
- ❒ Review your cyber hygiene before travel.
- ❒ Review the Travel security guide for university researchers and staff.