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.

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 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.

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.

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 bene h ***ciary of their collaboration on your project is clear.***

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.

Best practice checklist for sensitive projects

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

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.

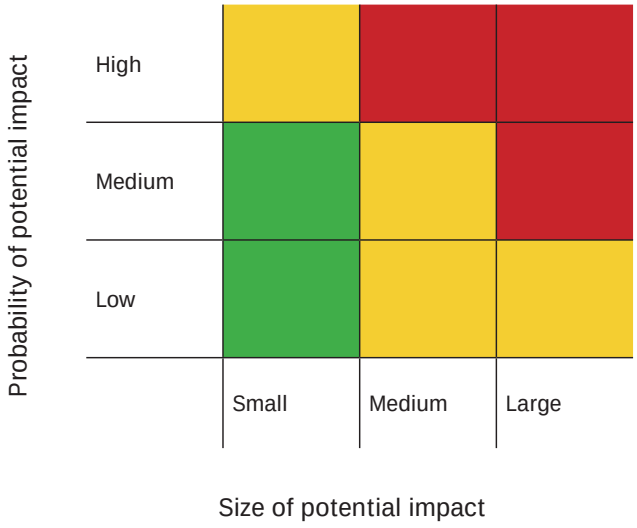
- Australian Strategic Policy Institute (ASPI) – International Cyber Policy Centre (ICPC): https://www.aspi.org.au/program/international-cyber-policy-centre
- Center for a New American Security (CNAS) – Technology & National Security program: https://www.cnas.org/research/technology-and-national-security
- 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 Tam

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 o f ce, 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 o f ce.
- **High risk (red):** consult with your research o f ce as a f rst step and seek appropriate guidance to further assess identi f ed risks and implement signi f cant 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.