Hostile state actors, particularly China and Russia, pose the greatest threat. In our digital era, threats can arise from anywhere, including from non-state actors. The world is increasingly competitive. Hostile states seek advantage at Canada’s expense. They look to advance their economic, technological, intelligence and military state interests. Policies and practices of Military-Civil Fusion, coercive national security laws, and state capitalism pose a growing threat. Almost all Canadian research domains face some level of risk; but the top five targets are:

- Biopharma & health
- Artificial intelligence (AI), quantum, and big data
- Semiconductors, 5G, and smart cities
- Ocean technology, including sensors
- Aerospace technology, including hypersonics

Sophisticated threat actors will exploit vulnerabilities, including via deceptive means, such as:

- Traditional espionage
- Cyber espionage
- Insider threats
- Non-traditional collectors
- Talent spotting
- Research funding
- Unsafe supply chains (equipment, services)
- Joint ventures
- Minority investments (e.g. venture capital)
- Foreign acquisitions (foreign direct investment)

Threat actors seek direct or indirect access to sensitive laboratories. Control over IP may be lost, with all gains accruing to foreign states. Researchers may knowingly or unwittingly contribute to foreign military capabilities. Leading academics and administrators may be targeted or leveraged.

Government funding may be subverted, and foreign funding may co-opt Canadian research and IP.

These threats are real; and Canada is not unique in managing these challenges and risks. Most importantly, you are not alone in facing these threats.