THREAT ACTORS

While hostile activities by state actors (HASA) can originate from anywhere in the world and threat actors may change over time, the **People's Republic of China (PRC), Russia and India** are currently the main threat actors targeting Canada and Canadian interests. **Iran,** [redacted] **and Pakistan** are also known to engage these activities, including attempting to silence dissidents in Canada and harassing Canadians abroad.

The **PRC** is currently the most active perpetrator of HASA in Canada, due to the scope of its activities and the level of resources it expends. The party-state targets all levels of government and civil society (e.g., communities, media entities, academia) to further its interests and protect/enhance its legitimacy by influencing political decision-making, pursuing unfair advantages in trade, business and research, suppressing criticism and dissent, facilitating espionage, and inappropriately influencing Canadian communities.

Russia engages in malicious cyber activity, the theft of classified information, and influence operations to manipulate decision-makers and influence public opinion. Russia's threat activity targeting Canada has continued following the invasion of Ukraine, owing to the large Ukrainian-Canadian population, Canada's position and support of Ukraine, and its criticism of Russia.

India engages in HASA in Canada to influence Canadian politicians to take a pro-India stance and counter perceived threats to its stability. Indian [redacted] officials are actively engaged in clandestine activities in Canada; they monitor Indo-Canadians of interest and push a pro-India, pro-Hindutva agenda. India also engages in monitoring dissidents supportive of the Khalistani separatist movement to discredit the movement in Canada, including politicians that are perceived to support it.

THREAT LANDSCAPE

PRIORITY SECTORS	EXAMPLES OF THREAT ACTIVITY OBSERVED	TOOLS IN PLACE	GAPS
1. DEMOCRATIC PROCESSES AND INSTITUTIONS *Foreign states interfere with our democratic institutions (including elections systems and processes) to promote their interests,*		✓ Investigations *(CSIS Act, Criminal Code, Security of Information Act)* ✓ Foreign Intelligence Collection (s. 16 of the *CSIS Act, CSE Act)* ✓ CSE assistance to federal and non-federal partners ✓ CSIS investigates, supports and advises federal and non-federal partners	**Legislative**: Rapidly evolving technology and techniques mean that Canadian laws (in particular, the *CSIS Act, Criminal Code, Security of Information Act*) must be updated to cope with the evolving threat, including: × Gap in foreign intelligence authorities (s. 16 of the *CSIS Act*) Gap in sharing information and advice with non-federal partners *(CSIS Act)*

[APG]

PRIORITY SECTORS	EXAMPLES OF THREAT ACTIVITY OBSERVED	TOOLS IN PLACE	GAPS
counter the influence of another country, or directly undermine Canada's national interests.		✓ Cyber investigations for threats targeting the Government of Canada (GoC) or systems of importance to the GoC ✓ Critical infrastructure threat assessments ✓ Publicly available telephone and online mechanisms to report suspected threats to national security ✓ Domestic and foreign cooperation (s. 17 of the *CSIS Act*, RCMP collaboration with domestic and international law enforcement agencies) ✓ Threat reduction measures (CSIS) against threats to the security of Canada ✓ CSE foreign cyber defence operations ✓ *Immigration and Refugee Protection Act (IRPA)* provides ground for inadmissibility for national security reasons and the *Citizenship Act* contains prohibitions related to national security ✓ Public attribution of malicious cyber activity to a state actor of their proxy ✓ *Canada Elections Act* (CEA), and related investigations conducted by the Office of the Commissioner of Canada Elections with RCMP support ✓ Canada's Plan to Protect Democracy (e.g., Security and Intelligence Threats to Elections Task Force) ✓ International cooperation and coordinated messaging with like-minded partners	× Gap in providing technical and operational assistance to federal partners *(CSIS Act)* × Gap in *Criminal Code* offences (e.g., lack of aggravating factors for sentencing) × Gap in *Security of Information Act* offences (e.g., commission of an indictable offence for a foreign entity, general foreign interference offence, foreign influenced intimidation, covert interference with a democratic right or duty) × Gap in *Security of Information Act* provisions (e.g., preparatory acts, leakage of sensitive government information) × Limitations of the *Investment Canada Act* (e.g., Measures taken under the act must be tied to a specific investment, which may not address all national security threats identified during an investigation; information about residual risks cannot be shared outside the ICA community) **Information sharing:** intelligence to evidence problems cause challenges for criminal proceedings. Challenges in sharing information and advice among federal partners due to clearances, knowledge and awareness, need-to-know limitations. **Resources**: the workload of the S&I community has increased exponentially but resources have not been commensurate with rise in threat activity. **Reporting**: Members of the public have noted that they seldom receive responses after reporting instances of HASA. Reporting systems are

[APG]

PRIORITY SECTORS	EXAMPLES OF THREAT ACTIVITY OBSERVED	TOOLS IN PLACE	GAPS
			decentralized, agency-specific, and may not be available in preferred language.
2. COMMUNITIES *Canadians and Canadian communities are also directly targeted through harassment, intimidation and disinformation. These activities erode confidence in government authorities and undermine social cohesion.*		✓ Investigations *(CSIS Act, Criminal Code)* ✓ Foreign Intelligence Collection (s. 16 of the *CSIS Act, CSE Act)* ✓ Publicly available telephone and online mechanisms to report suspected threats to national security ✓ Domestic and foreign cooperation (s. 17 of the *CSIS Act*, RCMP collaboration with domestic and international law enforcement agencies) ✓ Threat reduction measures (CSIS) against threats to the security of Canada, when appropriate ✓ CSE foreign cyber defence operations ✓ *IRPA* provides ground for inadmissibility for national security reasons; *Citizenship Act* contains prohibitions related to national security ✓ Engagement with civil society organizations and at-risk communities	**Legislative**: Rapidly evolving technology and techniques mean that Canadian laws (in particular, the *CSIS Act, Criminal Code, Security of Information Act*) must be updated to cope with the evolving threat, including: × Gap in foreign intelligence authorities (s. 16 of the *CSIS Act*) × Gap in sharing information and advice with non-federal partners *(CSIS Act)* × Gap in providing technical and operational assistance to federal partners *(CSIS Act)* × Gap in *Criminal Code* offences (e.g., lack of aggravating factors for sentencing) × Gap in *Security of Information Act* offences (e.g., commission of an indictable offence for a foreign entity, general foreign interference offence, foreign influenced intimidation) × Gap in *Security of Information Act* provisions (e.g., preparatory acts) **Information sharing:** intelligence to evidence problems cause challenges for criminal proceedings. Challenges in sharing information and advice among federal partners due to

[APG]

PRIORITY SECTORS	EXAMPLES OF THREAT ACTIVITY OBSERVED	TOOLS IN PLACE	GAPS
			clearances, knowledge and awareness, need-to-know limitations. **Jurisdiction:** Transnational repression activities often involve leveraging loved ones abroad, which is difficult for Canadian law enforcement to prevent/disrupt. **Resources**: the workload of the S&I community has increased exponentially but resources have not been commensurate with rise in threat activity. **Reporting**: Members of the public have noted that they seldom receive responses after reporting instances of HASA. Reporting systems are decentralized, agency-specific, and may not be available in preferred language. **Engagement**: outreach efforts are inconsistent, delivered in a piecemeal fashion by individual department/agencies
3. ECONOMIC PROSPERITY AND RESEARCH SECURITY *Foreign states use or direct investments in certain sectors for strategic goals beyond economic prosperity. Foreign states target Canadian-made research and innovation to support their economic,*		✓ Investigations *(CSIS Act, Criminal Code)* ✓ Foreign Intelligence Collection (s. 16 of the *CSIS Act, CSE Act)* ✓ Cyber investigations for threats targeting the GoC or systems of importance to the GoC ✓ Publicly available telephone and online mechanisms to report suspected threats to national security ✓ Domestic and foreign cooperation (s. 17 of the *CSIS Act*, RCMP collaboration with domestic and international law enforcement agencies)	**Legislative**: Rapidly evolving technology and techniques mean that Canadian laws (in particular, the *CSIS Act, Criminal Code, Security of Information Act*) must be updated to cope with the evolving threat, including: × Gap in foreign intelligence authorities (s. 16 of the *CSIS Act*) × Gap in sharing information and advice with non-federal partners *(CSIS Act)* × Gap in providing technical and operational assistance to federal partners *(CSIS Act)* × Review definition of "threats to the security of Canada" *(CSIS Act)*

[APG]

PRIORITY SECTORS	EXAMPLES OF THREAT ACTIVITY OBSERVED	TOOLS IN PLACE	GAPS
military or strategic objectives.		✓ Threat reduction measures (CSIS) against threats to the security of Canada, when appropriate ✓ CSE foreign cyber defence operations ✓ The *Investment Canada Act (ICA)* National Security Provisions provide for the review of foreign investments of any size ✓ *IRPA* provides ground for inadmissibility for national security reasons; *Citizenship Act* contains prohibitions related to national security ✓ *Export and Import Permits Act* controls ✓ *National Security Guidelines for Research Partnerships* ✓ Engagement with at-risk sectors (e.g., *Safeguarding Science initiative)*	× Gap in *Security of Information Act* offences (e.g., commission of an indictable offence for a foreign entity) × Gaps in *Investment Canada Act* compliance and monitoring capabilities × Limitations in ICA regarding the types of investments that can be reviewed. (e.g., joint ventures and loan agreements cannot be reviewed) **Information sharing:** intelligence to evidence problems cause challenges for criminal proceedings. Challenges in sharing information and advice among federal partners due to clearances, knowledge and awareness, need-to-know limitations. National security information is also not always incorporated into economic security regulatory decision-making. There are also gaps in *the Guidelines for Research Partnerships*. **Resources**: the workload of the S&I community has increased exponentially but resources have not been commensurate with rise in threat activity. **Reporting**: Under-reporting of suspicious, threat, or criminal incidents targeting economic prosperity and research security. Reluctance of some organizations to report incidents and share information with government/law enforcement. **Engagement**: outreach efforts are inconsistent, delivered in a piecemeal fashion by individual department/agencies.

[APG]

PRIORITY SECTORS	EXAMPLES OF THREAT ACTIVITY OBSERVED	TOOLS IN PLACE	GAPS
4. INTERNATIONAL AFFAIRS AND DEFENCE *Foreign intelligence services target Canadian diplomatic and military missions abroad through a variety of means to obtain sensitive information, undermine the legitimacy of Canada's presence, or to deny Canada its foreign and defence policy goals.*		✓ Investigations *(CSIS Act, Criminal Code, Security of Information Act)* ✓ Foreign Intelligence Collection (s. 16 of the *CSIS Act, CSE Act)* ✓ Defence intelligence prepared by DND/CAF ✓ CAF and allied (North American Aerospace Defense Command) capabilities ✓ CSE assistance to federal and non-federal partners ✓ CSIS investigates, supports and advises federal and non-federal partners ✓ Cyber investigations for threats targeting the GoC or systems of importance to the GoC ✓ Domestic and foreign cooperation (s. 17 of the *CSIS Act*, RCMP collaboration with domestic and international law enforcement agencies) ✓ Threat reduction measures (CSIS) against threats to the security of Canada, when appropriate ✓ CSE foreign cyber defence operations ✓ *IRPA* provides ground for inadmissibility for national security reasons; *Citizenship Act* contains prohibitions related to national security ✓ Diplomatic levers, including bilateral and multilateral relations, international trade, consular support, development, and peace and security assistance	**Legislative**: Rapidly evolving technology and techniques mean that Canadian laws (in particular, the *CSIS Act, Criminal Code, Security of Information Act*) must be updated to cope with the evolving threat, including: × Gap in foreign intelligence authorities (s. 16 of the *CSIS Act*) × Gap in sharing information and advice with non-federal partners *(CSIS Act)* × Gap in providing technical and operational assistance to federal partners *(CSIS Act)* × Review definition of "threats to the security of Canada" *(CSIS Act)* × Gaps in the *Defence Act* **Information sharing:** intelligence to evidence problems cause challenges for criminal proceedings. Challenges in sharing information and advice among federal partners due to clearances, knowledge and awareness, need-to-know limitations. **Resources**: the workload of the S&I community has increased exponentially but resources have not been commensurate with rise in threat activity.

[APG]

PRIORITY SECTORS	EXAMPLES OF THREAT ACTIVITY OBSERVED	TOOLS IN PLACE	GAPS
		✓ Imposition of sanctions under *the Special Economic Measures Act* and the *Justice for Victims of Corrupt Foreign Officials Act*. ✓ Intelligence diplomacy	
5. CRITICAL INFRASTRUCTURE *Foreign threat actors target Canada's critical infrastructure systems to undermine Canadians' confidence in their government, disrupt the economy, access to vital services and weaken Canada's military defensive posture.*		✓ Investigations *(CSIS Act, Criminal Code, Security of Information Act)* ✓ Foreign Intelligence Collection (s. 16 of the *CSIS Act, CSE Act)* ✓ CSE assistance to federal and non-federal partners ✓ CSIS investigates, supports and advises federal and non-federal partners ✓ Cyber investigations for threats targeting the GoC or systems of importance to the GoC ✓ Critical infrastructure threat assessments ✓ Publicly available telephone and online mechanisms to report suspected threats to national security ✓ Outreach and engagement with CI owners/operators (RCMP) ✓ Domestic and foreign cooperation (s. 17 of the *CSIS Act*, RCMP collaboration with domestic and international law enforcement agencies) ✓ Threat reduction measures (CSIS) against threats to the security of Canada, when appropriate ✓ CSE foreign cyber defence operations	**Legislative**: Rapidly evolving technology and techniques mean that Canadian laws (in particular, the *CSIS Act, Criminal Code, Security of Information Act*) must be updated to cope with the evolving threat, including: × Gap in foreign intelligence authorities (s. 16 of the *CSIS Act*) × Gap in sharing information and advice with non-federal partners *(CSIS Act)* × Gap in providing technical and operational assistance to federal partners *(CSIS Act)* × Increase the efficiency of the collection and use of data *(CSIS Act)* × Gap in *Criminal Code* offences (e.g., treason, sabotage) × Gap in *Security of Information Act* offences (e.g., commission of an indictable offence for a foreign entity, general foreign interference offence, foreign influenced intimidation, covert interference with a democratic right or duty) × Gap in *Security of Information Act* provisions (e.g., preparatory acts, leakage of sensitive government information) × Limitations of the *Investment Canada Act* (e.g., Measures taken under the act must

[APG]

PRIORITY SECTORS	EXAMPLES OF THREAT ACTIVITY OBSERVED	TOOLS IN PLACE	GAPS
		✓ *ICA* National Security Provisions ✓ *IRPA* provides ground for inadmissibility for national security reasons; *Citizenship Act* contains prohibitions related to national security	be tied to a specific investment, which may not address all national security threats identified during an investigation; information about residual risks cannot be shared outside the ICA community. Certain types of investments such as joint ventures and loan agreements cannot be reviewed. **Information sharing:** intelligence to evidence problems cause challenges for criminal proceedings. Challenges in sharing information and advice among federal partners. **Resources**: the workload of the S&I community has increased exponentially but resources have not been commensurate with rise in threat activity. **Reporting**: Under-reporting of suspicious, threat, or criminal incidents due to reputational risks. Reluctance of some organizations to report incidents and share information with government/law enforcement. **Engagement**: outreach efforts are inconsistent, delivered in a piecemeal fashion by individual department/agencies.

[APG]