TOP SECRET/[redacted]/CANADIAN EYES ONLY

# 2023 THREAT SUMMARY REPORT

Intelligence Assessment Branch

Canada


The Threat Summary Report (TSR) 2023 assesses national security threats as defined in the CSIS Act, including those related to espionage, foreign interference (FI), economic security and proliferation, cyber and terrorism. The TSR 2023 covers Canada's intelligence priorities, as specified by Cabinet and articulated in the Minister of Public Safety's Ministerial Direction to CSIS on Intelligence Priorities, to the year ending in March 2023. (S//CEO)



**Key Judgments**

- Hostile activities of state actors (HASA) directed at Canada are significant and likely to increase over the next year. The People's Republic of China (PRC) poses the most significant espionage, FI and cyber threats to Canada and its interests. Other state actors engage in FI activities, such as the Russian Federation, India, Iran, and others. (S//CEO)
- HASAs—linked most notably to the PRC—target and exploit economic relations with Canada, including in investment, trade and research collaboration. In 2022–23, CSIS efforts to investigate and assess these threats have translated into significant activity under the national security provisions of the Investment Canada Act (ICA), including record caseload reviews. (S//CEO)
- Canada faces multiple cyber threats. The PRC and Russian Federation (RF) pose the greatest threat—conducting aggressive cyber operations for intelligence collection and geopolitical intimidation, undeterred by repeated public exposures. Also, commercially available cyber tools are increasing the capabilities of states that previously posed little threat to Canada in the cyber domain. (S//CEO)
- An ever more diverse range of beliefs continues to motivate violent extremists, including ideologically motivated violent extremism (IMVE), religiously motivated violent extremism (RMVE) and politically motivated violent extremism (PMVE). Since the beginning of the COVID-19 pandemic, extreme anti government rhetoric and propaganda has increased, resulting in greater IMVE activity and threats to public safety.
- 

## Global Threat Picture

The international threat environment was influenced by several geopolitical developments that pose a challenge to Canada and the rules-based international order. These include Russia's war against Ukraine, which has not only undermined international peace and stability, but also challenged the resolve of the North Atlantic Treaty Organization (NATO). It has also renewed debates about the transatlantic security architecture, with formerly neutral states like Sweden and Finland seeking membership in NATO. The Indo-Pacific is one of the world's most contested maritime zones—with significant geostrategic significance—because of the deepening rivalry between the United States (US) and the PRC. The GC unveiled its own Indo-Pacific Strategy in 2022. The violent suppression of mass protests in Iran has led to new sanctions by Canada and other Western states against Tehran, which continues to advance its own nuclear ambitions and deepen its partnerships with Russia and the PRC. These, and several other threats, have contributed to a complex and extraordinary international security environment—and resulting challenges. (S//CEO)

HASAs continue to view Canada as a high-value target for espionage and FI activities. Several foreign states target critical sectors of Canada's knowledge-based economy, while their intelligence services have exploited Canada's diverse multicultural society to engage in FI in diaspora communities and the political process. The risk to Canada's democratic and electoral institutions from FI threats was a concern during the September 2021 federal election. (S//CEO)


The COVID-19 pandemic eased considerably in 2022: lockdowns, travel restrictions and related public health measures ended in Canada and the Western world, but continue to have a lingering influence. It contributed to the intensification of extreme anti-authority/anti-government rhetoric and propaganda, resulting in threats to public safety. Various IMVE actors have promoted narratives that undermine public trust and confidence in government and scientific expertise. Using the issue of mandatory vaccinations—and earlier restrictions for those who did not comply—as a key online narrative, they claimed that governments were intent on controlling populations and forcibly vaccinating everyone. This anti-public health measures movement has shifted focus, to include issues perceived to affect Canadian freedom, including government overreach and tyranny, globalization, and the protection of children. (S//CEO)

# Espionage, Foreign Interference and Sabotage

## People's Republic of China (PRC)

The PRC remains the greatest espionage and FI threat to Canada and Canadian interests. Canada is likely a high-priority target because of its close ties with the United States and other Five Eyes (FVEY) countries, as well as its large Chinese diaspora. The PRC and PRC Intelligence Services (PRCIS) use sophisticated, pervasive and persistent hostile activities—both overt and covert—against civil society and all levels of government. These activities transcend party political lines, ideologies and ethnic backgrounds, and often occur over several years. (TS//CEO)

The PRC focusses on promoting its national interests and protecting the legitimacy and stability of the Chinese Communist Party (CCP). To this end, PRC foreign policy has anti-democratic effects around the world, including in Canada. For example, the CCP uses elements of its authoritarian political model to limit the ability of Canadians to speak freely about China. These efforts are part of the PRC's global endeavour to (i) undermine the rules-based international order; (ii) destabilize liberal democracy; and, (iii) shift the focus of human rights advocacy away from China. For example, in 2021, Facebook reported a cyber campaign targeting Uyghur activists, journalists and dissidents, including in Canada. Posts were designed to lure activists to sites harbouring malware that could then be used to monitor activities of unsuspecting recipients. Facebook traced the malware to two companies in China.

The PRC conducts FI activities at all levels of government, carefully targeting preferred political candidates across party lines, funnelling financial support to these candidates, and aligning community-influence groups to promote PRC political objectives. PRC officials in Canada clandestinely cultivate, sway or assist select local officials—as these PRC officials understand that municipal politicians in Canada may later move to another level of government—and nurture mutually beneficial relationships over the long term.

Reporting from a European non-governmental organization (NGO), and subsequent media reporting from September 2022, drew global attention to the existence of so-called 'Overseas Police Stations' (OPS), including in Canada. OPS very likely enable the Ministry of Public Security (MPS) to conduct repatriation activities against the Chinese diaspora. They are but one of many tools used by the CCP to conduct transnational repression (TNR) activities.

indicates *Some PRC officials have* taken specific actions to target Canadian MPs affiliated with the Canadian parliament's non-binding motion characterizing the PRC's treatment of the Uyghurs as genocide. For example, sought information on a Canadian MP's relatives who may be located in the PRC for further potential sanctions. This effort is almost certainly meant to make an example of this MP and deter others from taking anti-PRC positions. (S//CEO)

Intangible technology transfer (ITT) is a ubiquitous and yet often undetectable method used by the PRC to facilitate knowledge transfer from Canada and other Western countries. Canada is a global research leader, due to its excellent universities, public and private research organizations, and scientific talent. As a result, it has also become a prime target for ITT threat actors. The CCP-PRC party-state has established policies and strategic plans to encourage Chinese nationals, the diaspora, foreign scientists, and entrepreneurs to contribute to the development of the PRC's science and technology (S&T) sector. These policies and plans aim to exploit the collaborative, transparent and open nature of Canada's research and innovation sector to serve the PRC's economic, intelligence, and military interests. For example, in 2021, an employee of Agriculture and Agri-Food Canada (AAFC) was charged with "breach of trust by a public officer" for failing to disclose to AAFC the full extent of his relationship with Gansu Agricultural University (GAU). AAFC raised concerns that the employee was "inappropriately exchanging intellectual knowledge through his associations with GAU." (U)

### Russian Federation (RF)

The Russian Intelligence Services (RIS) rely primarily on diplomatic mission-based personnel to carry out intelligence and FI activities in Canada. The RIS continue to collect intelligence in support of the RF's geopolitical and economic objectives, with emphasis on political intelligence, Ukraine

The RIS has intensified its disinformation and influence activities in Canada via social media and pro-Russian and/or Russian-controlled websites, particularly in the lead-up to the invasion of Ukraine.

### India

Next to the PRC, India is the most significant FI actor in Canada. This threat requires particular attention in view of Canada's pivot toward the Indo-Pacific Strategy and engagement with India as a key partner in the emerging multipolar global order. Indian officials conduct deceptive, clandestine and coercive interference activities targeting the Indo-Canadian diaspora and elected officials at all levels of government in Canada. They aim to (i) promote a positive image of India, and pro-India decision-making in Canadian governments and (ii) counter perceived Canada-based threats to India, including those stemming from Canada-based Khalistani extremists (CBKEs). indicates, for

the Indian Ministry of External Affairs issued a travel advisory for Indian nationals in Canada, warning of a "sharp increase in hate crimes, sectarian violence and anti-India activity" in Canada. This is a clear example of disinformation that is meant to damage Canada's reputation, and was likely retaliation against Canada for hosting voting in the global Khalistan referendum. (TS/ CEO)

*Indian officials developed and built a network of contacts through whom India conducts interference activities.*

. For instance, while

media manipulation and disinformation campaigns with a nexus to Canada are

(TS/ CEO)

## Pakistan

Pakistani officials, carry out a range of FI activities in Canada. Their primary focus is supporting pro-Pakistan petitions and influence to counter anti-Pakistan and pro-India messaging in Canada.

## Iran

IIS activity. CSIS assesses that this trend will continue if the capability developed by Iran to facilitate and conduct lethal operations abroad is not disrupted or deterred. (TS CEO)

### Protests in Iran and Canadian sanctions

Following the September 16, 2022, death of Mahsa Amini while in the custody of Iran's morality police, mass protests erupted across Iran. As of February 2023, more than 500 individuals reportedly had been killed, while more than 19,000 others were arrested as part of Iran's violent crackdown. Iran's suppression of the protests has resulted in new sanctions against Iran by Canada and other Western countries. Between October 3, 2022, and March 27, 2023, within the framework of the Special Economic Measures Act (SEMA), the Government of Canada sanctioned 147 Iranian officials and 191 Iranian entities for their role in gross and systematic human rights violations. On November 14, 2022, the Minister of Public Safety designated Iran as a regime that has engaged in terrorism and systemic and gross human rights violations under the Immigration and Refugee Protection Act (IRPA), subparagraph 35(1)(b). Under this designation, those Iranians who were senior officials of the regime at any time from November 15, 2019, onwards are deemed inadmissible to Canada. (U)

CSIS assesses that leaders of anti-regime protests in Canada and the West will likely be targeted by IIS for harassment, intimidation and possibly violence, to dissuade continued involvement in anti-regime activities. (S)

## Cyber and Emerging Technologies

The Service assesses that the PRC and RF pose the greatest cyber threat to Canada. The PRC and RF conduct aggressive cyber operations for intelligence collection and geopolitical

intimidation,

PRC cyber actors continue to target numerous GC departments, agencies, politicians, academia and the private sector.

[1] Cognitive warfare integrates and leverages the latest advances in computing technologies, psychology, and neuroscience for achieving cognitive effects. CW can be specifically targeted against an individual or societal at a scale not humanly possible. A cognitive effect is not a by-product of action, but it' s very objective. (U)

[redacted] This is likely to continue as the PRC strives to modernize its military by 2035 and become a global military power by 2049. [redacted] PRC cyber actors also continue to target Canadian Members of Parliament, Senators and government employees with ties to Canadian foreign policy, demonstrating the PRC's growing determination to target foreign-based critics and collect information on Canadian decision makers. Since mid-2021, [redacted] (TS/[redacted]/CEO)

Russian cyber operations [redacted]. The diplomatic and defence sectors will likely continue to be a priority target, given Canada's membership in NATO and ongoing support to Ukraine. In early 2022, likely Russian cyber actors compromised Global Affairs Canada's (GAC's) Protected B networks, [redacted]. CSIS assesses that Russia also poses an increasing cyber-sabotage threat to Canadian critical infrastructure. [redacted] (TS/[redacted]/CEO)

The Service assesses that many Russian cybercrime groups operate with wide latitude where their activities support Russian state interests. Their threat activities are likely conducted with the implicit approval and—in some instances, at the direction of—the RIS. The RF likely believes that this relationship provides it with 'plausible deniability,' thereby reducing the risk of retaliation and/or other covert action by Western governments. Russia likely allows cybercrime, such as ransomware attacks, that advance—at least in part—Russian state interests by degrading and imposing costs on Western economies. Russia also benefits from the proceeds of cybercrime. [redacted] (TS/[redacted]/CEO)

**Other cyber threat actors**

[redacted] (TS/[redacted]/CEO)

Commercially available cyber tools are increasing the capabilities of countries that previously posed little threat to Canada in the cyber domain. [redacted]

Other countries have purchased cyber tools, which could potentially be used to target Canadian interests. According to open sources, the NSO Group's Pegasus spyware conducted operations in 45 countries, including Canada; in August 2021, open-source reporting revealed a list of 50,000 potential Pegasus victims. (TS/

Emerging threats can also arise from that can purchase commercially available tools and services. Following the NSO Group's Pegasus Spyware exposure, it became apparent that (TS/

Cybercriminals who conduct ransomware attacks increasingly pose a threat to national security. (TS/ CEO)

HASAs are increasingly using AI-supported "deepfake" technology—the use of machine learning to manipulate and create realistic images, video and audio that humans and computers find hard to detect as fake—for FI activities. Deepfakes will become increasingly sophisticated and more difficult to detect over time.

Late 2022 saw the popularization of sophisticated text-generating AI programs such as ChatGPT. The ability of these tools to produce natural-sounding responses can be manipulated to facilitate malicious activity by both state and non-state actors. They can facilitate social engineering and phishing activities, or produce content for disinformation campaigns. Data manipulation is also a threat. Machine-learning tools rely on training data to generate responses to queries; if the underlying data are biased or intentionally tampered with, they will produce results that are either incorrect and/or orchestrated, and exploitable by hostile actors seeking to influence the programs' outputs. While it is unlikely that these tools will create "hackers" overnight, they can likely be used as a starting point for aspiring coders with malicious intent. More seasoned coders can also create the building blocks for malicious software. This type of technology is rapidly evolving. Hostile actors will likely develop their own versions—or seek to exploit existing ones—to help meet national objectives. (U)

## Economic Security

The international order is being reshaped by geostrategic economic competition and confrontation. Several state actors, particularly the PRC and Russia, are seeking to reshape the balance of power—defined in terms of political, economic and military capabilities—and institutions that currently underpin the existing international order by exploiting their economic relations with the West. Canada's geography, interests and values have drawn it into this competitive environment. HASAs seek to advance their strategic political, economic and military objectives by exploiting their economic relations with Canada, including investment, trade and research collaboration. (S//CEO)

HASAs continue to seek to acquire access to—or control over—sensitive

technologies, critical minerals, data and critical infrastructure to (i) advance their own military and intelligence capabilities, (ii) deprive Canada of access to economic gains, (iii) employ economic coercion against Canada, and (iv) support other intelligence operations against Canadians and Canadian interests. CSIS assesses that these activities pose a threat to Canada's national security and long-term economic prosperity, which are indivisible interests. (S/

In 2022-2023, the geo-political competition over economic and technological advantage continued to accelerate, resulting in a continual deterioration of Canada's security against economic-based threats to national security. This deterioration was characterized by both more threat activities and the introduction of previously unexamined or under-examined threats. (S//

In terms of foreign investment, over the past year,

Additionally,

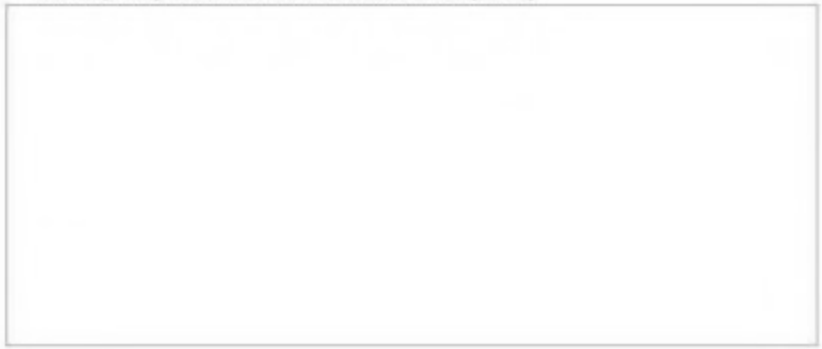
(TS/ CEO)

(TS/ /CEO)

With regard to research security, CSIS's support corroborated previous CSIS intelligence and assessments that threat actors continue to gain access to Canadian scientific and technological expertise through research collaborations. Such analyses have demonstrated that, in research collaboration, a national security risk may be created by either the Canadian or external partner, and in particular by the legacy of Canadian researchers working with HASA-affiliated institutions. (S//CEO)

# Violent Extremism and Terrorism

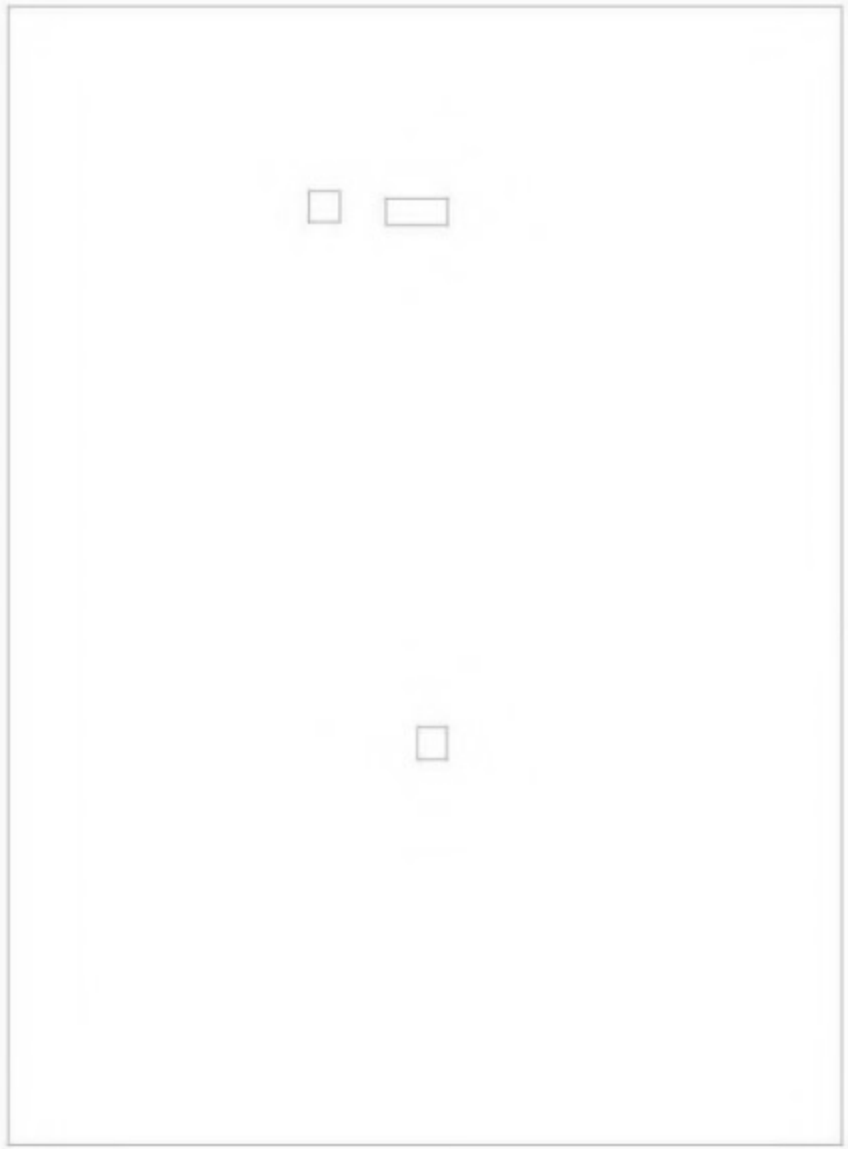
**Ideologically motivated violent extremism (IMVE)**

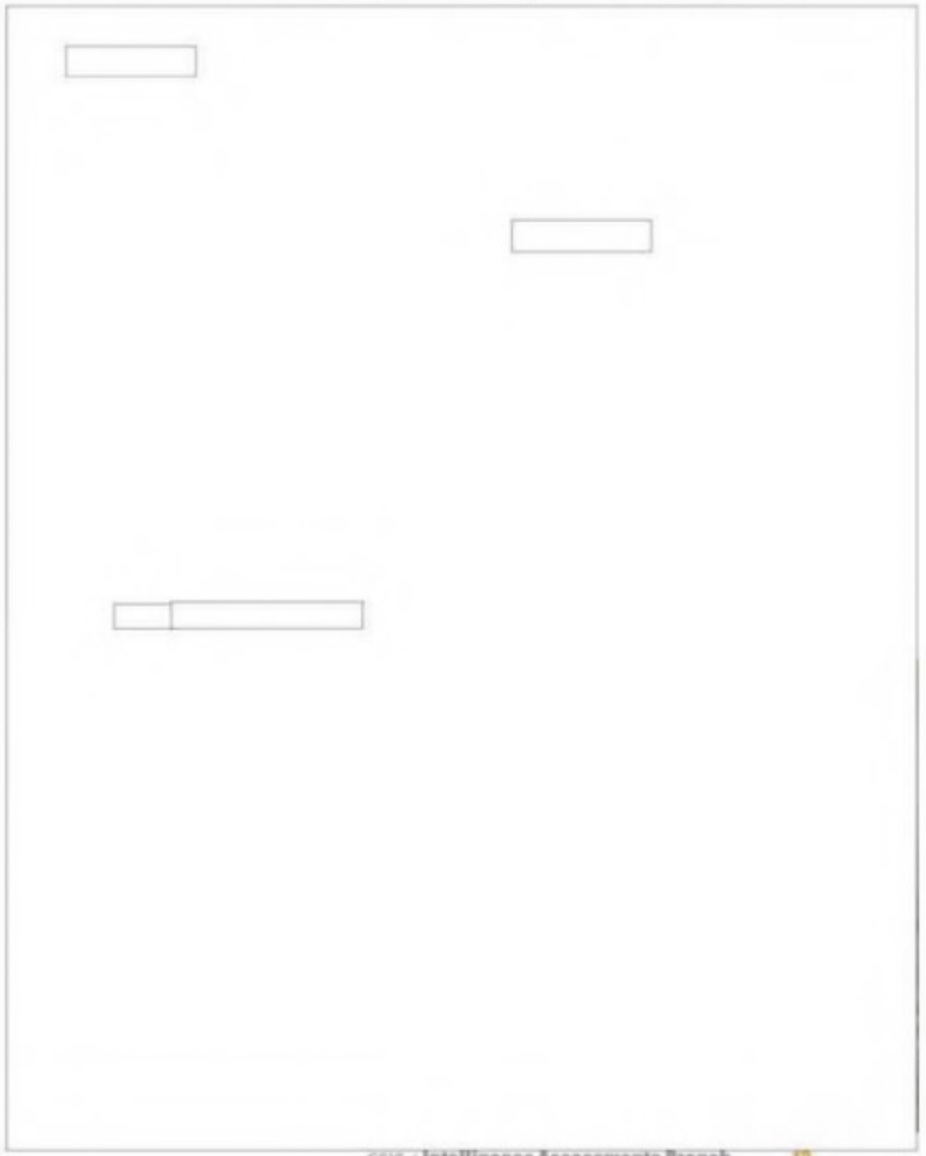


TSR

TOP SECRET/ /CANADIAN EYES ONLY

## Religiously motivated violent extremism (RMVE)





**Politically motivated violent extremism (PMVE):**

**Outlook**

Canada will continue to face a broad range of threats related to FI, espionage, cyber, economic security, proliferation and terrorism. CSIS assesses that the PRC will continue to pose the greatest FI, espionage, cyber and economic security threat to Canada for the foreseeable future. Various pressures to the rules-based international order supported by Canada—like Russia's war against Ukraine and Iran's incremental development of an indigenous nuclear program—will likely compound this threat. The proliferation of Canadian technology and expertise remains of high importance.