Canadian Security Intelligence Service | Service canadien du renseignement de sécurité

TOP SECRET/ /CSIS EYES ONLY

INTELLIGENCE ASSESSMENT

CANADA TOWARDS 2028

Preamble

This Intelligence Assessment (IA) is the product of subject-matter expert input and consultation with operational desks. The IA is not a policy document or a directional statement; its primary purpose is to provide forward-looking, contextual analysis and provoke discussion. The assessment provides a thematic and country- / region-specific overview of key state-actor threats to Canadian security and related intelligence challenges facing the Service over the next five years and beyond. It offers a big-picture approach and links state-actor threats with evolving environmental variables in an effort to spur discussions on key concerns related to counterintelligence (CI) and foreign influence/interference (FI) threats from state actors, how they might evolve in the coming five years, and how we can better position ourselves to best respond to these threats.

Intelligence Assessments Branch
Direction de l'évaluation du renseignement

Canada

Key Assessments

Geopolitical Landscape

- The evolving global pandemic geopolitical environment—and the anticipated "post-pandemic" environment—suggest that key CI threat actors will continue to display flexibility in forging alliances, partnerships and proxy arrangements that are intended to bring them strategic gain. A number of hostile states will remain driven by ideological, authoritarian agendas These factors will continue to play a central role in the information / disinformation sphere, the development and pursuit (and theft) of applied technologies, all of which are likely to present increasingly complex and interrelated challenges to Canada's security and prosperity.

Key Threat Actors

- The primary CI threat actors—the People's Republic of China (PRC), Russia, Iran, India and, to a lesser extent, —will require Canada's ongoing attention. we will need to pursue a cost-benefit approach to threat activities across the CI spectrum:

- China poses threat to Canadian interests. CSIS anticipates that the PRC will present increasing challenges to Canada in coming years. PRC threat actors China will continually push the boundaries. Our investigations and reporting on the PRC threat will therefore undoubtedly have even greater political resonance for our Government of Canada (GC) clients in the near future.

- Russia—and to a lesser extent, Iran—will continue to present a significant threat to our state secrets and our advanced technology sectors, as well as our critical infrastructure. Russia's full-scale invasion of Ukraine in February 2022 is a clear reminder of the global strategic threat posed by that country. As the fallout from Russia's war against Ukraine evolves, we will require significant investments in

Technology Challenges

- Emerging disruptive technologies (EDTs) are the fast-developing new frontier that will pose increasing national security and investigative challenges over the coming decade. Hostile state actors (HSAs)

will continue to pursue development and deployment of EDTs to support their strategic

-

Evolving CI Challenges

- We should expect HSAs to continually target our advanced technologies and research sectors within a developing geopolitical and economic environment. In most cases, our leading innovative sectors (e.g., biotechnology and genomics; virology and pathology research; quantum computing; alternative energy technologies; aerospace/satellite technologies, etc.) will be the primary targets for espionage activities.
- We will need a more coherent GC strategy buttressed with economic security expertise
- Several states—most notably the PRC, Russia, Iran and Pakistan—target Canada for illicit and covert procurement, as well as technology and soft-knowledge transfer. Various actors assist in facilitating these activities: diplomats, intelligence services, researchers, insiders, state-owned enterprises (SOEs) and others acting as proxies (both witting and unwitting).
- Similarly, a more mature, less hesitant, public- and private-sector outreach strategy on CI threats will be required to better sensitize potential targets on the CI threat, including insider threat activity and communities targeted for infiltration by foreign states. This strategy would include training SMEs and IOs for sector-specific outreach. We also need to bring our Public Report more in line with other allied services that have offered far more detailed and substantive discussions of threat issues. A "taking it to the people" strategy will, for example, help support threat reduction measures (TMRs) by encouraging a general public that is more aware and by instilling a normative national security culture in the population.

Foreign Interference

- The PRC is already conducting substantial sophisticated, pervasive and persistent FI activities in Canada. the Chinese Communist Party (CCP) leverage existing networks to interfere in Canada's democratic institutions and processes, thereby posing a threat to Canada The PRC has engaged in 'hostage diplomacy' and economic coercion in attempts to influence policy decisions involving the PRC-Canada bilateral relationship in its favour.

- India a primary FI threat actor in Canada; the recent launch of Canada's Indo-Pacific strategy. Despite ties between India and Canada, India influence the GC towards pro-India policies, counter perceived threats to its domestic stability emanating from Canada – such as Khalistani Extremism – and propagate pro-India narratives in Canada. Indian threat actors involved in Canadian politics (by targeting all levels of government and politicians and influence and leverage the Indo-Canadian diaspora to further their interests.

- Disinformation—and the technologies applied to it (including "deep fakes")—will present ongoing challenges. CSIS should draw more from private sector / civil organization actors (including commissioned partnerships) and other government departments (OGDs) to more effectively investigate and mitigate disinformation.

- Canada faces ongoing FI threat challenges from Pakistan, Our challenge is to investigate the depth and breadth of some of these activities (particularly those related to the electoral cycle), Although these matters are sensitive, CSIS will have to continually push for a more robust culture of FI awareness among decision makers and not shy away from "difficult" situations, including those involving elected officials or candidates.

- Recent cases involving Canadians (e.g., the "two Michaels", along with the demonstrated capability and intent of the PRC, Russia and other countries to track down perceived regime threats in various foreign countries, underscore the need for an effective whole-of-government game plan to better deal with politically charged threat events.

Cyber Threats

- China and Russia devote massive resources towards cyber espionage, cyber influence and operations targeting critical infrastructure. For both countries, these activities will facilitate intelligence gathering, but will also serve as a tool of geopolitical intimidation.

- The increasingly complex nature and widening scope of PRC, Russian and other state/non-state actor cyber operations further underscores the imperative for CSIS proactive cyber threat discovery strategy by

Foreign Partnerships

-

-

The Geopolitical Environment

Key Trends

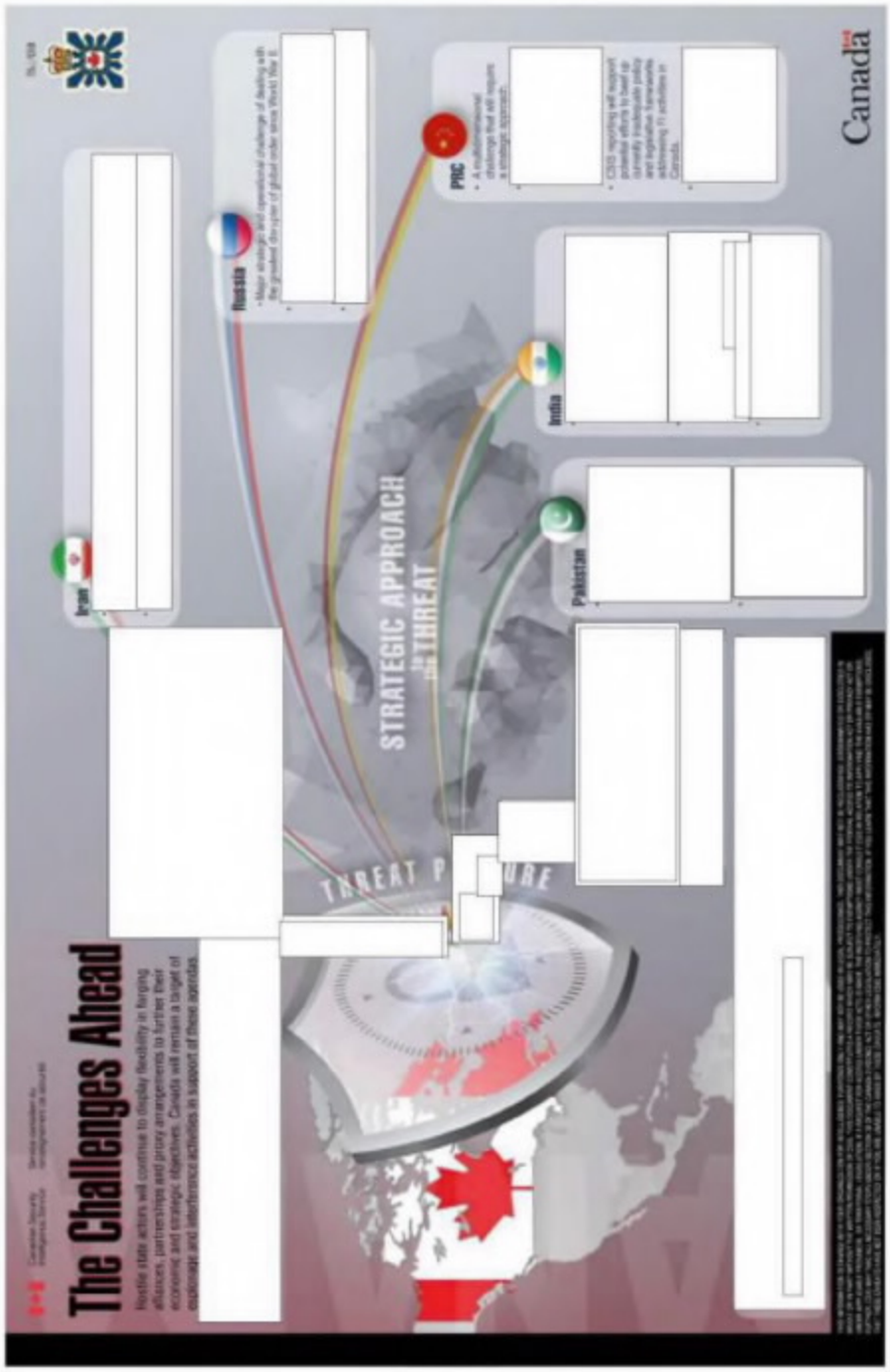
- China threat will continue to occupy centre stage.
- Russia's war against Ukraine will require a persistently resolute stance from Canada
-
-
-

1. The COVID-19 pandemic has accentuated geopolitical trends over the past decade: retrenchment of authoritarian regimes and their aggressive challenges to international institutions; the growing geopolitical ambitions of China and other states outside the framework of Western liberal democracies; increasing competition surrounding technology, resources and supply-chain management; and, ever-growing hyper-partisanship in the online space amplifying the sense of global community breakdown. All of these trends are bound to continue into the "post-pandemic" environment;

2. The COVID-19 pandemic has exposed, more than ever, the risks associated with supply-chain interdependencies and the vulnerabilities of individual national economies. As such, global strategic and economic competition will continue to intensify and the stakes involved in securing a competitive edge—and protecting national assets—will get even higher. Current and emerging key global actors will face the difficult task of protecting their assets while finding new ways to secure advantages over their competitors, even those from friendly states.

3.

4.


Canada
Russia
PRC
India
Pakistan
Iran
STRATEGIC APPROACH
THREAT
The Challenges Ahead

PRC

5.

6.

7.

8.

Russia

9. Russia's war against Ukraine will require a persistently resolute stance from Canada

10.

11.

12.

Iran

13.

14. Following the September 16, 2022, death of the young woman Mahsa Amini at the hands of Iran's morality police, mass protests erupted across Iran. As of early December 2022, more than 470 persons reportedly had been killed and 18,000 arrested as part of Iran's violent crackdown.

15. Between October 3 and November 29, 2022, within the framework of the *Special Economic Measures Act* (SEMA), the GC sanctioned 103 senior Iranian officials and 186 Iranian entities, including the IRGC leadership and elements of the regime's security, intelligence and economic apparatus, for their role in gross and systematic human rights violations. On November 14, 2022, the Minister of Public Safety designated the Islamic Republic of Iran as a regime that has engaged in terrorism and systemic and gross human rights violations.

India

16. In November 2022, the GC officially launched a $2.3 billion Indo-Pacific strategy, which aims to deepen Canada's engagement in the region by expanding trade, developing sustainable infrastructure and increasing its military presence.

17.

-influence activities within governments and Indian diaspora groups.

18.

Pakistan

19. As a participant in Canada's Indo-Pacific strategy, albeit to a lesser extent than India, Pakistan

and suppress narratives or policies emanating from Canada that are perceived as anti-Pakistan.

20.

21.

22.

23.

24.

25.

26.

Key Trends

-
-
-

Technology Challenges

27. EDTs and emerging technologies are the fast-developing new frontier that will pose increasing national security and investigative challenges over the coming decade. HSAs like China and Russia will continue to pursue development and deployment of EDTs to support their strategic interests.

Big Data

28.

29.

30.

31.

32.

Artificial Intelligence (IA)

33. AI is the demonstration of cognition and creative problem solving by machines rather than humans or animals—ranging from narrow AI designed to solve specific problems to artificial general intelligence, a system that, in the future, may match or exceed a human being's understanding and learning capacity. AI is currently embedded in devices we use and with which we interact daily; AI is also deepening the threats posed by cyberattacks and disinformation campaigns

34.

35.

36.

Quantum

37. Quantum information science and technology, which includes quantum computing, networking, sensing and metrology, leverages the fundamental properties of matter to generate new information technologies. Quantum-related technologies—including semiconductor microelectronics, photonics and the global positioning system—have underpinned significant parts of the national economy and defence infrastructure,

38.

39.

40.

Biotechnology

41.

42.

Evolving CI Challenges

Key Trends

-
-
-
-

PRC

43.

44.

45.

46.

47.

Russia

48.

49.

50.

Iran

51.

India

52.

53.

Economic Security Threats

54.

55.

56.

57.

58.

59.

Espionage Targets

60.

targets of foreign espionage

- Biotechnology
-
-
- Quantum computing
-
- Artificial Intelligence
-
-
-
- Aerospace technologies

Proliferation

61. Several states– –target Canada for illicit and covert procurement as well as technology transfer.

62.

63. PRC threat actors are actively targeting Canadian academic and research institutions to facilitate the transfer of critical research and expertise.

64.

65.

66.

Tackling the Threat

67.

68.

69.

Foreign Interference

Key Trends

- PRC
- Russian FI activities,
- India- Pakistan— political interference activities,
-

PRC

70. PRC FI in Canada is already sophisticated, pervasive and persistent, and the CCP leverage existing networks to interfere in Canada's democratic institutions and processes. promoting Chinese national interests and policies at every level of government and throughout civil society.

FI activity in Canada conducted through PRC officials in Canada;

71. from a FI perspective are the activities of the CCP's United Front System (UFS), including the United Front Work Department (UFWD), its associated entities and any persons who may be conducting 'united front work' in Canada. The UFS's primary role is to ensure, via its vast network, that united front work (i.e., work to strengthen a united front coalition that furthers the influence and interests of the CCP) is carried out effectively both inside and outside the PRC. United front work involves the co-optation of entities abroad—especially elites—to expand the Party's support base, while marginalizing and silencing opponents.

72. In addition, PRC FI encompasses transnational repression (TNR), which primarily targets dissidents in the Chinese diaspora communities, including in Canada. More broadly speaking, TNR represents the extraterritorial application of domestic PRC law, and signifies an attempt by the CCP to control the overseas Chinese diaspora and purportedly speak for all Chinese, everywhere. CSIS assesses that elements of the CCP's UFS, are actively engaged in TNR activities in Canada.

73. For example, the Overseas Police Stations (OPS) in Canada illustrate the threat posed by TNR. OPS in Canada to conduct repatriation activities that target the Chinese-Canadian diaspora. Such activities are a manifestation of TNR activities by the PRC's state security apparatus that have been ongoing for many years. The establishment of OPS in Canada demonstrates the CCP's desire to control individuals of Chinese descent outside of PRC borders.

74. PRC threat actors are increasingly using the online space—including social media platforms like Twitter and Facebook—to spread propaganda and disinformation on issues of importance to the Party (e.g., Hong Kong, Xinjiang) and target dissidents. These activities can include the use of proxies and bots, as well as state officials (e.g., diplomats and journalists). Certain social media platforms, notably Twitter, Facebook and YouTube, have already taken action to address PRC online interference efforts, for example by closing accounts linked to suspected PRC-linked inauthentic activity (e.g., use of bots). we expect that the current lack of adequate policy and legislative frameworks to address this problem will continue to encourage China to push the limits of activities that operate, at best, in a legal and normative 'grey zone'.

India

75. Notwithstanding strengthened ties between India and Canada, as an expected ramification of Canada's Indo-Pacific strategy, India a primary FI actor in Canada. India influence the government of Canada towards pro-India policies to counter perceived threats to its domestic stability emanating from Canada – such as Canada-based Khalistani

extremism (CBKE) – and to propagate pro-India narratives in Canada. Indian FI activities in Canadian democratic institutions and Indo-Canadian diaspora and community groups

76. seeking to cultivate Canadian politicians to advance Indian interests in all levels of government within Canada.

77. on promoting a pro-India narrative in Canadian public discourse (e.g., in media, social media and political discussions), use of disinformation as a key FI tactic against Canada,

78. swaying Canadian governments towards pro-India policy positions

79. to exert influence and leverage the Indo-Canadian diaspora and community groups to further its interests,

Russia

80. Russian disinformation activities have escalated during the Russia-Ukraine war, as expected. They are pervasive, but continues to focus on sowing doubt and entrenching the Kremlin narrative among the Russian population.

A Note on Disinformation

Disinformation—and the technologies applied to it, including "deep fakes"—will present ongoing challenges, particularly from Russia and China.

- We need to invest more resources into media and social media monitoring
- draw from private sector / civil organization actors as well as other government departments to more effectively investigate and mitigate disinformation.
- look towards more commissioned partnerships with organizations that have the expertise to carry out specific research.

81. Russia use new developments in social media and other tools to propagate disinformation,

82.

Government and private-sector exposure of Russian disinformation, while not a perfect solution, will be a useful tool moving forward.

Pakistan

83. Pakistan's FI activities within Canada are primarily aimed at portraying a positive image of Pakistan

influence GC policies and political figures towards pro-Pakistan initiatives,

84.

85.

86.

87.

88.

89.

Cyber Threats

Key Trends

- tangible integration of cyber-HUMINT expertise and investigations
- China, Russia and Iran
-
-
-

HUMINT and Cyber

90. we cannot disassociate hostile state cyber activities from their (in many cases) parallel intelligence gathering conducted through HUMINT.

INTELLIGENCE ASSESSMENT

PRC

91.

92.

93.

1)

2)

3)

4)

5)

94.

95.

96.

Canada

Russia

97.

98.

99.

100.

101.

Cyber Investigations

The Canadian S&I community must shift from need-to-know to need-to-share for reporting related to cyber activity with a national security nexus. Domestic victim engagement must be executed in a manner that supports collection and reporting requirements of all stakeholders.

Iran

102.

103.

104.

105.

106.

107.

108.

109.

110.

111.

112.

113.

114.

115.

A Note on Foreign Partnerships

Key Trends

-
-
-

116.

117.

118.

119.

INTELLIGENCE ASSESSMENT

CSIS_PUBLICATIONS / SCRS_ PUBLICATIONS