UNCLASSIFIED

FOREIGN INTERFERENCE

Objective

- Underscore the importance of collaboration and reiterate Canada's commitment to strengthen our approach to countering foreign interference.

Canadian Initiatives

- The Government of Canada has taken significant action to combat foreign interference and protect our democracy in recent years. This includes important and significant updates to our national security legislation in 2017 and efforts to protect our federal elections in 2019 and 2021.
- Canada continues to review its approach to address the evolving threat environment.
- To this end, Canada recently announced a series of new measures to bolster our approach against foreign interference. This includes public consultations to guide the creation of a Foreign Influence Transparency Registry in Canada to ensure accountability from people who advocate on behalf of a foreign government.
- The Government of Canada is also making significant investments in our Counter-Foreign Interference capabilities. Budget 2023 includes $13.5 million over five years, starting in 2023-24, and $3.1 million ongoing to Public Safety Canada to establish a National Counter-Foreign Interference Office.
- This Office will provide a dedicated focus on foreign interference, enabling the Government of Canada to shift to a more proactive and coordinated approach in addressing current and emerging threats. It will also enhance partnerships between federal departments/agencies, other levels of government, and non-government partners, acting as a focal point both within the Government of Canada but also with external stakeholders.
- Budget 2023 also proposed $48.9 million over three years for the Royal Canadian Mounted Police to protect Canadians from harassment and intimidation by foreign actors, to increase its investigative capacity, and to more proactively engage with communities at greater risk of being targeted.
- Canada also works closely with its allies and like-minded partners to take a collaborative approach to counter foreign interference.
- Finally, Canada's new Indo-Pacific Strategy recognizes that China's aggressive pursuit of foreign interference and increasingly coercive treatment of other countries and economies have significant implications in that region, and puts forward how Canada intends to actively work with allies and partners to shape the future of the region.

[APG]

Background

Foreign Interference

- Foreign interference (FI) includes activities undertaken by state or non-state actors that are harmful to Canada's interests and are clandestine or deceptive or involve a threat to any person. Techniques used to conduct FI can include espionage, sabotage, illicit and corrupt financing, and other threat activities. Foreign states leverage these activities to advance their strategic interests including: domestic stability, seeking geopolitical influence, economic advancement, revision of the rules-based international order, and military advantage. These activities can be directed at Canadians, or residents of Canada, or against Canadian institutions to advance their strategic interests at the expense of our national interests and values.

- Through its mandate to investigate threats to the security of Canada, including foreign interference, the Canadian Security Intelligence Service (CSIS) has seen multiple instances of foreign states targeting Canadian institutions and communities. As well, the Royal Canadian Mounted Police (RCMP) is aware that illegal state-backed activities are committed against Canadians and Canadian interests, and investigates these activities further to its mandate. The scope of potential FI activities can be broad, encompassing a range of techniques. These include intelligence operations, the use of state-sponsored or foreign influenced media and disinformation campaigns, and the use of sophisticated cyber tools.

- Several reports have highlighted the threat of FI in Canada. For example, in its 2021 Public Report, released in April 2022, CSIS stated that foreign interference activities in Canada continue to be sophisticated, persistent, and pervasive. Espionage and foreign-influenced activities are directed at Canadian entities both inside and outside of Canada, and directly threaten Canada's national security and strategic interests. Furthermore, the 2019 Annual Report of the National Security and Intelligence Committee of Parliamentarians (NSICOP) outlined foreign interference activities, including the targeting of Canadian institutions by threat actors. The NSICOP (2019) report pointed to Russia and China as being particularly active in Canada and made a number of recommendations for Canada to bolster its response to the threat of FI.

Counter-FI Initiatives

- As the threat environment evolves, Canada is enhancing measures already in place, as well as bolstering its toolkit and legislative framework.

- In recognition of the current threat landscape, Prime Minister Trudeau announced a series of new initiatives aimed at combatting foreign interference in March 2023, including:

    - Public and stakeholder consultations to guide the creation of a Foreign Influence Transparency Registry (FITR). The online component of the

[APG]

consultations closed on May 9, 2023 and garnered submissions from a wide range of stakeholders across Canada. Preliminary analysis indicated broad support for a registry amongst online respondents and consulted stakeholders;

- A new National Counter Foreign Interference Coordinator to allow for a more proactive and coordinated approach and to enhance partnerships between federal and non-federal stakeholders; and
- Investments in the amount of $5.5 million to strengthen the capacity of civil society partners to counter disinformation.

India's Counter-FI Initiatives

India has been taking concrete steps to counter foreign interference over the past decade by strengthening its laws, regulations, and security agencies to better detect and counter foreign interference within the country. Some of these initiatives include:

- The Foreign Contribution (Regulation) Act (FCRA), which aims to better monitor foreign funding of NGOs, individuals and other organizations. This law was first enacted in 1976 and has been amended multiple times over the years.
- The multi-Agency Centre (MAC) which was established in 2009 to monitor and counter foreign interference in the country's political and economic systems.
- The Cybercrime Coordination Centre (CyCord) which was set up to detect and counter cybercrime including foreign interference on digital systems.
- The Defence Acquisition Procedure, which was introduced in 2020 and is aimed at promoting self-reliance and autonomy in defence manufacturing. Its main purpose is to reduce dependence on foreign suppliers, thus limiting exposure to foreign interference and intellectual property theft. The government has introduced new laws for foreign investment in critical sectors of the economy, such as defense and telecommunications, to protect against potential security risks. Some of the key measures that have been put in place include:
  - Increased scrutiny of foreign investment in sensitive sectors such as defense, telecoms, and critical infrastructure.
  - Introduction of a "negative list" of sectors where foreign investment is prohibited, or where foreign investment is restricted to a certain percentage.
  - India has also raised the minimum local sourcing requirement for foreign companies operating in India to promote self-reliance.

[APG]

- The government has also introduced the concept of 'golden share' which allows the government to veto any resolution that could affect the security of the country.
- Guidelines to regulate investments from countries that share a land border with India, and this is to ensure that investments from neighboring countries are not used to harm India's security

- The government is also planning on introducing a new act, the Digital India Act (DIA), to replace the current Information Technology Act, which would include provisions and regulations to moderate fake news and disinformation on social media platforms.

[APG]