UNCLASSIFIED

HOSTILE ACTIVITIES BY STATE ACTORS (HASA)

ISSUE

HASA encompasses any effort by foreign states (including their proxies) to undermine Canada's national interest, and those of our closest allies, with a view to advancing their own self-interest. HASA comprises of foreign interference activities that are typically short of the use of force or armed conflict yet are deceptive, coercive, corrupt, covert, threatening, or unlawful in nature. While individual activities on their own may not appear to be a threat, when combined into a pattern of malicious activities these represent a serious and destabilizing threat to Canada and its interests. HASA is distinct from normal diplomatic activities, or foreign influence, conducted by foreign actors in Canada which are legitimate and an integral part of the conduct of international relations.

POSITION

HASA constitutes a real and present threat to Canada's national interest and requires a whole of government effort, including by GAC, to detect threats, and lead Canada's involvement in international responses. Given its scope, scale and wide-ranging implications for every facet of society the Government of Canada is working closely with international partners to identify and respond to HASA appropriately.

BACKGROUND

HASA is not a new threat, and not particular to any state. However, in recent years certain countries have intensified their use of these tactics at Canada's expense. These tactics focus on undermining Canada's: democratic processes and government institutions; social cohesion; economic prosperity; international affairs and defence; and, critical infrastructure.

COUNTRY	HASA	CANADA'S RESPONSE
China	Compromise of Managed Service Providers (MSPs).	In December 2018, Canada joined partners in calling out the Chinese Ministry of State Security for the compromise. The Canadian Centre for Cyber Security within CSE reached out to MSPs in Canada to inform them of the threat and offer assistance.
	Operation Foxhunt, a global covert operation beginning in 2014 to repatriate individuals deemed corrupt, and quiet dissidents.	The Government of Canada has made several public statements noting operations are occurring in Canada, CSIS Director Vigneault most recently referenced Foxhunt publically in February 2021.
Russia	Nerve agent attack against Sergei and Yulia Skripal in Salisbury, United Kingdom.	In March 2018, Canada took action alongside allies by expelling seven Russian diplomatic personnel and denying three applications by the Russian government for additional diplomatic staff in Canada. These measures were undertaken in solidarity with the United Kingdom.

	Poisoning of Alexei Navalny, a prominent Russian political opposition figure.	In September 2020 the Minister of Foreign Affairs, expressed condemnation and demanded answers following the poisoning.
	Russia targeting Canada (and UK, US) COVID-19 vaccine research and development and hacking of international sport organizations (including the World Anti-Doping Agency and Canadian Centre for Ethics in Sport).	CSE publically released a technical advisory and cyber attribution.
Iran	Harassment and intimidation of Canada-based relatives of Flight PS752 victims from threat actors linked to proxies of Iran.	Ongoing CSIS outreach with Iranian-Canadian communities through targeted communication with various groups and community leaders.
	Harassment and intimidation of diaspora communities in Canada.	Ongoing GAC public statements expressing human rights concerns.
India	Spread of false or misleading narratives on Canada from India-based platforms (following a November 2020 statement by PM Trudeau expressing concern for Indian farmers protesting government farm reforms).	RRM Canada is tracking this issue closely. RRM Canada has observed cases of false or misleading narratives on: Canadian "vote banks" politics attempting to appeal to Sikh/Punjabi diaspora; depicting PM Trudeau as a sympathizer to Khalistani separatists; and, COVID-19 related federal spending and perceived misuse of public funds.

CHALLENGES IN COUNTERING HASA

Efforts to develop a counter-HASA plan have been ongoing, though a government wide strategy has not yet been finalized. The primary challenges have been the disjointed and complex nature of HASA and difficulty coordinating assessment as well as responses within the Canadian security and intelligence (S&I) community - including with federal, provincial, and territorial levels of government. Identifying appropriate response mechanisms for individual activities as well consistent patterns of HASA by certain states has also been difficult to coordinate between departments and agencies. A counter-HASA strategy has been delayed due to focus on specific elements of HASA, notably federal elections and concentration on protecting democratic institutions, as well efforts to address immediate concerns with foreign interference activities in Canada. Within GAC, several thematic and geographic divisions have been implicated in HASA issues, managing operational and policy responses (as well as legal considerations) independently.

With regards to countering disinformation specifically, the digital information ecosystem is a complex and rapidly evolving transnational space. Hostile actors are no longer creating original content and using bots and bot networks to amplify messages; instead, they are amplifying existing domestic content often using proxies. Hostile actors manipulate a multiplicity of platforms, not limited to social media (including websites). Attributing disinformation is increasingly difficult in this complex transnational space, where the distinction between domestic and foreign, as well as influence and interference, is often purposefully blurred. Measuring the real or potential impact of disinformation is also almost impossible,

given it is often intended to exacerbate existing social cleavages. This, in turn, challenges the principle of proportionality in state responses. Moreover, responding to disinformation as a single event misses the point, given hostile states conduct myriad activities across time and space as part of a broader campaign of foreign interference in pursuit of geopolitical objectives.

CANADA'S RESPONSE

Canada's actions are most effective when it acts in concert with allies or other likeminded states. At present, deterrence and response is exercised through a variety of issue based committees and processes. These include the Security and Intelligence Threats to Elections Task Force (SITE), the Investment Canada Act (ICA) process, the Cyber Attribution Framework, and countering HASA initiatives.

HASA takes place in the context of Canada's distinct bilateral relationships, and each relationship is complex and multifaceted. The breadth and depth of Canada's relationship with a particular country provides the framework for an array of diplomatic engagement; this can include political, economic, security, development, cultural, education, and people-to-people relations. A calibrated response thus uses different diplomatic levers, which might include messages relayed by intelligence services (i.e., intelligence diplomacy), or diplomatic tools. In addition, through its behaviour and statements, Canada is also seeking to establish or strengthen norms of state behaviour in support of a rules based international order.

When managing a calibrated response to HASA, GAC is frequently trying to simultaneously protect Canadians, deter certain types of behaviour, manage bilateral relationship, and promote specific norms of state behaviour. Responsive mechanisms are dispersed across the department and traditional diplomatic tools range from actions such as: demarches, reduction or suspension in engagement, sanctions, declaration of embassy personnel as personae non grata, or closure of consulates and/or embassies. Some of these could be applied immediately to respond to HASA, while others would require adaptation or modification, and in some case may need legislative or regulatory changes. These tools may be used on a bilateral basis or in concert with allies and like-minded partners. The effectiveness of these mechanisms are case-specific, and from a foreign policy perspective are difficult to measure immediately after their use or when used in parallel with other responsive actions. Analysis on the potential impact of tools, weighed against Canadian interests, need to be considered under the larger HASA context on a case by case basis.

To note, disinformation is ultimately an international challenge that requires an international response. With its coordination unit headquartered at GAC, Canada leads the G7 Rapid Response Mechanism (RRM), since its inception in 2018. The RRM was set up to identify and respond to foreign threats to democracies, including foreign state sponsored disinformation and it includes G7 partners plus Australia, New Zealand and the Netherlands as observers. Canada is also a member of several other counter disinformation initiatives such as

Although these initiatives are not publicly avowed, all countries are working together to share knowledge, build capabilities, and support pro-democracy messaging. We also engage across various plurilateral and multilateral fora. For example, Canada joined 32 other states in the Freedom Online

Coalition (FOC) in a statement calling on governments to refrain from conducting and sponsoring disinformation in November 2020.

FIVE EYE RESPONSES

COUNTRY	GOVERNANCE
Australia	The National Counter Foreign Interference Coordinator is responsible for leading whole of government policy coordination and private-sector engagement. This position was created in Australia's Home Affairs Department in 2018, and supported by a A$87.8M investment establishing a Counter Foreign Interference Task Force drawn from across Australia's S&I community. The National Security and Intelligence Committee of Parliamentarians (NSICOP) explicitly highlighted this office as an example for Canada to consider in their 2019 Annual Report examining HASA.
United Kingdom	The Cabinet Office leads HASA policy through its National Security Secretariat, and matrixed teams reporting to the U.K. National Security Advisor manage counter-HASA implementation and coordination.
United States	The National Counterintelligence Strategy, released in January 2020, lists "foreign influence" as a significant intelligence threat and commits the U.S. Government to lead a "whole-of-society" response. As the lead U.S. agency for investigating foreign influence operations, the Federal Bureau of Investigation (FBI) established a Foreign Influence Task Force in 2017, primarily composed of agents from FBI counterintelligence, cyber, criminal, and counterterrorism divisions.
New Zealand	New Zealand has a "foreign interference work program" established by Cabinet. A Strategic Coordinator for Foreign Interference is based in the Department of the Prime Minister and Cabinet (equivalent to PCO). The Coordinator ensures departments and agencies are aware of their responsibility for mitigating HASA risks and educates Ministers about risks as well as advocates for policy issues.

TALKING POINTS

- The threat from hostile activity by state actors in all its forms represents a significant danger to Canada's prosperity and sovereignty, and remains a priority for the Government of Canada.
- Security and intelligence partners collaborate to share information in an effort to detect and counter HASA, including state-sponsored disinformation.
- However Canada cannot tackle HASA alone. Our international allies face similar threats and by working together we bring our collective resources to counter threats from foreign actors.
- The Government of Canada is committed to working with partners and allies to share the critical information necessary to understand and counter the full spectrum and threat of foreign interference.
- Canada has always stood up for a rules-based international order, one in which all countries abide by international norms. Consistent with these principles, Canada actively shares information and coordinates responses with allies through numerous multilateral bodies and relationships.

RESPONSIVE LINES

How is Canada holding HASA actors accountable?

- *In March 2018, Canada took action along with allies in response to the nerve agent attack against Sergei and Yulia Skripal in Salisbury, United Kingdom. Canada expelled seven Russian diplomatic personnel, and denied three applications by the Russian government for additional diplomatic staff in Canada. These measures were undertaken in solidarity with the United Kingdom.*
- *In December 2018, Canada again joined partners in calling out the Chinese Ministry of State Security for the compromise of Managed Service Providers (MSPs). The Cyber Center reached out to MSPs in Canada to inform them of the threat and offer assistance.*
- *In September 2020, the Minister of Foreign Affairs, expressed condemnation and demanded answers following the poisoning of Alexei Navalny, a prominent Russian political opposition figure. Navalny was poisoned by a nerve agent of the Novichok group like the one used in the poisoning in Salisbury, UK in March 2018.*
- *In October 2020, GAC and CSE expressed Canada's concern over the willingness of Russian military intelligence, GRU, to target critical infrastructure and international organizations, that demonstrated a pattern of disruptive activities and a continued disregard for the rules-based international order and international law.*
- *In the context of the COVID-19 pandemic, Canada publicly rebuked cyber actors targeting the health care sector (April 2020) and the specific attribution of Russian cyber exploitation of Canadian vaccine research organizations (July 2020).*

What measures does Canada have in place to protect the integrity of its electoral system?

- *Canada recognizes the importance of prioritizing the integrity of its electoral system. As such, in January 2019, the Government of Canada announced its plan to protect Canadian federal elections against threats to our democratic institutions.*
- *This effort includes standing up the Security and Intelligence Threats to Elections (SITE) Task Force, a collaboration between the Communications Security Establishment, the Canadian Security Intelligence Services, Global Affairs Canada (GAC) and the Royal Canadian Mounted Police.*
- *As part of SITE, GAC is mandated to:*
    - *Conduct open source research on global trends and data on threats to democracy*
    - *Partner with G7 countries to share information and coordinate responses to threats as appropriate*
    - *Provide research on disinformation campaigns targeting Canada by foreign actors*
    - *Coordinate attribution of incidents*
- *Throughout the 2019 Federal Election, the SITE Task Force raised awareness and assessed foreign interference threats, briefing members of the Government of Canada's Critical Election Incident Public Protocol (CEIPP) on any threat activities to ensure nothing affected Canada's ability to have a free and fair election.*

What measures does Canada have in place to secure its institutions from cyber attacks or breaches of information?

- *Our first priority is to defend our citizens, businesses and institutions from cyber-threats and ensure that they have all the information and guidance needed to enhance their resilience.*
- *Canada strongly condemns any malicious cyber activities, particularly irresponsible and destabilizing actions that put lives and critical infrastructure at risk. We call on all actors to ensure that cyberspace is open, secure, stable, accessible and peaceful.*
- *Canada remains steadfast in its solidarity with allies and partners in promoting a framework for responsible state behaviour in cyberspace. We also remain committed to working with partners to prevent, discourage and counter malicious cyber activity at home and around the world.*

What is Canada doing to combat Covid-19 misinformation?

- *Rapid Response Mechanism (RRM) Canada has been monitoring inauthentic and coordinated online activity related to the COVID-19 pandemic -- including coordinated amplification of the unfounded theory that 5G technology is linked to the virus.*
- *G7 RRM information sharing was tested and proven in the COVID-19 context. The mechanism quickly shifted its focus to the pandemic, supporting a real-time exchange of analysis of foreign threats that included industry and civil society organization partners, particularly with respect to evolving foreign state-sponsored information manipulation.*
- *This kind of online activity is not always the result of direct control or intervention by any particular state actor. Often, these actors create an ecosystem of distrust in government and media and amplify groups and emerging trends in the information environment that are compatible with this goal.*
- *RRM Canada continues to work with partners across the Canadian security and intelligence community to identify any malign state and non-state information operations in the online information space.*