SECRET//CEO
FOR INTERNAL DISCUSSION ONLY

Canada's Strategy for Countering Hostile Activities by State Actors

Purpose

The aim of this Strategy is to protect Canada's national interest by effectively countering Hostile Activities by State Actors (HASA) through an overarching, whole-of-government framework. The Strategy provides Canada's security and intelligence community, and the Government of Canada more broadly, with a common understanding of:

- The nature of threat;
- The Government of Canada's priorities and approach to addressing HASA; and,
- Their role in this effort, within respective mandates.

Scope

Hostile Activities by State Actors (HASA) encompass any effort by a foreign state, or its proxies, to undermine Canada's national interest, and those of our closest allies, with a view to advancing its own self-interest. HASA comprises actions that are typically short of armed conflict yet are deceptive, coercive, corrupt, covert, threatening, or illegal in nature. HASA is distinct from normal diplomatic activities conducted by foreign actors in Canada, which are legitimate and an integral part of the conduct of international relations by states.

For the purposes of this Strategy, HASA include for example[1]: foreign influence[2] actions outside the traditional rules and norms of open and diplomacy that may not be illegal, but that are contrary to Canadian values and interests; foreign interference, threats or illegal activities by states against Canadian individuals or institutions, whether at home or abroad; covert or secret activities by foreign states such as espionage[3] or sabotage; and hybrid warfare, which blends conventional warfare, irregular warfare and cyberwarfare with other influencing methods.

Implicated Departments and Agencies

This Strategy directly implicates the mandates of the following departments and agencies:

- The Canada Border Services Agency;
- The Canadian Security Intelligence Service;
- The Communications Security Establishment;
- The Department of Justice;
- The Department of National Defence and the Canadian Armed Forces;

[1] Though some of these definitions differ from those found in current Canadian law, they are assessed to be commonly understood in this way in Canadian society and among our allies and are presented here for policy purposes only. The use of the term "HASA", therefore, is meant to encompass all of these activities.
[2] The CSIS Act defines foreign influence as "activities within or relating to Canada that are detrimental to the interests of Canada and are clandestine or deceptive or involve a threat to any person." The term "foreign influence" is also used in other legislation, such as the *Security of Information Act*.
[3] The CSIS Act defines the threat of espionage or sabotage as "against Canada or is detrimental to the interests of Canada or activities directed toward or in support of such espionage or sabotage."

- The Financial Transactions and Reports Analysis Centre of Canada
- Global Affairs Canada;
- Heritage Canada;
- Immigration, Refugees and Citizenship Canada;
- Innovation, Science and Economic Development;
- The Integrated Terrorism Assessment Centre;
- The Privy Council Office;
- Public Safety Canada;
- The Royal Canadian Mounted Police; and,
- Transport Canada.

This Strategy is applicable to the entirety of the Government of Canada, as foreign threat actors may target all departments and agencies, or the aspects of Canadian society that fall under their respective mandates.

The Context

The phenomenon of states and their proxies engaging in activities such as espionage, sabotage, foreign interference, foreign influence, economic coercion, and subversion against geopolitical and economic rivals is hardly new, but in recent years, certain countries have intensified their use of these tactics in order to advance their national interests. By its very nature, the targets of HASA extend beyond the realm of national security. Foreign actors seek to undermine parts of our national fabric, including Canada's sovereignty, prosperity, stability, or social cohesion for their own national objectives. They exploit or don't respect rights and freedoms that are protected by the *Canadian Charter of Rights and Freedoms*, including freedom of conscience and religion, freedom of thought and expression, freedom of the press, freedom of association, democratic rights, mobility rights, security of the person, and the rule of law. Globally, some ultimately seek to remake the rules-based international order.

Further, the COVID-19 crisis has fundamentally and irreversibly altered our world by accelerating the convergence of traditional security threats (e.g., espionage, foreign interference, military force) and non-traditional threats (e.g., economic vulnerabilities, public health). Foreign threat actors are exploiting new and unique opportunities to advance their interests at our expense. States are actively seeking to procure, or deny access to, targeted biopharmaceutical and healthcare assets, across fragile international supply chains. However, some states are seeking to acquire these assets in a manner that is harmful to our interests, and may employ hostile threat activities to do so. Hospitals, health care institutions, health-related research institutions, and other sensitive sectors are vulnerable to malicious cyber operations or intrusions attributable to foreign threat actors motivated by any number of hostile intentions. Though the pandemic may eventually subside, the new vulnerabilities it has exposed will remain, including to critical supply chains, health services and research.

Preserving Canada's status as a democratic, prosperous, open and multicultural society is a fundamental responsibility of the federal government. The past two decades have seen a significant dedication of resources in the security and intelligence community towards mitigating terrorism. However, at present, HASA should be considered the main threat to Canada's national security given its scope, scale and wide-ranging implications for society.

The National Interest

The national interest refers to Canada's sovereignty, democratic processes and institutions, security, territorial integrity, economic prosperity, social cohesion, clean environment, and resilient communities. Upholding Canada's national interest involves safeguarding the health, safety and security of Canadians, and maintaining an effective defence posture at home and abroad. Our national interest is advanced in a manner that adheres to Canada's fundamental values, especially those enshrined in the *Canadian Charter of Rights and Freedoms*.

Pursuing the national interest means having the right tools, policies and partnerships to:

- respond decisively when Canada and Canadian interests are threatened at home and abroad;
- attract investments that will foster innovation while not compromising national security;
- succeed in a more competitive global economy;
- collect intelligence to inform Canada's foreign, defence, economic and scientific policies;
- actively contribute to global security through robust foreign and defence policies;
- protect against covert or malign foreign interference against Canada's interests;
- allow Canadians to participate in our democratic processes and institutions and preserve their integrity; and
- build safe, healthy and sustainable communities.

National security and the national interest intersect, whereby protecting national security against threats posed by hostile activities by state actors or their proxies supports the protection and advancement of the national interest.

It has become clear in recent years, that Canada, and many of its allies have not kept pace with the rapidly evolving nature of HASA. New vulnerabilities and threat vectors exposed by state actors which seek to exploit the pandemic for strategic gain have widened this gap.

Recent strides to address HASA have been made in specific areas. The enactment of former Bill C-59, an *Act respecting national security matters*, which provided, among other things, modifications to the *CSIS Act* in specific areas to support its mandate to investigate and advise the government on national security threats including HASA and the Communications Security Establishment the authority to launch active and defensive cyber operations and to defend important non-federal government cyber networks, has helped bolster Canada's abilities aimed at countering HASA. Other efforts include Protecting Canada's Democracy with initiatives such as the Plan to Safeguard Canada's 2019 General Elections, as well as Budget 2019 investments in economic security, and amendments to the *Canada Elections Act*.

However, the institutions, infrastructure, economic strength, and multicultural identity that are fundamental to Canadian society are increasingly vulnerable to HASA, and more must be done, particularly in in light of the evolving post-pandemic threat environment.

Through the implementation of this Strategy, we have built a modern, nimble, proactive and sustainable whole-of-government framework that allows us to address threats across all domains

Threat Environment

Canada's approach to HASA cannot be seen in isolation from the global threat environment that poses persistent and existential challenges to the rules-based international order which has underpinned Canada's security since the end of the Second World War:

- Shifts in global power dynamics and growing tensions;
- The rise of authoritarianism, increasing political polarization and societal discord;
- Major violations of international law by state actors;
- Increased military modernization and advances in disruptive technology and weaponry that undermine the military advantage of liberal democracies and global stability.
- The growing sophistication and increasingly assertive behaviour of state and non-state threat actors;
- Increasing challenges to and manipulation of the rules-based international order by certain states; weakening and/or realignment of multilateral organizations;
- An emerging trend in inward-looking, nationalistic/protectionist policies;
- Use of cyber threats, economic coercion, and infiltration of supply chains as alternatives to traditional military levers of power;
- Sensitive and rapid technological advances that create new threat capabilities, with potential effects in the physical world, more rapidly than ever before;
- The willingness of Canada's potential adversaries to work together to advance their collective interests, often at the expense of Canadian and allied interests; and,
- The willingness of foreign states to threaten or harass dissidents, activists, and diaspora members outside their country of origin.

Threat Actors

In order to effectively protect against the threat of HASA, the Government of Canada must have a common understanding of the main threat actors we currently face, their objectives, targets and tactics.

China

China has the intent and capabilities without having to engage in open warfare, and its activities represent the most significant threat to Canada's interests for the foreseeable future. China's overall strategy is focused on the long-term objective of increasing its influence in world affairs and to ensure that the Chinese Communist Party (CCP) rule remains unchallenged. China employs a whole-of-society approach to HASA, which leverages resources from across diplomatic, informational, military and economic domains. These capabilities and assets include cultivating and using proxies (witting or unwitting), developing relationships and leveraging influence within Chinese communities, various levels of government, human and technological intelligence assets, state owned enterprises (SOEs) and state-backed or supported private entities, cyber tools and media.

Canada is an attractive target for China given its global standing, membership in the G7, NATO, and Five Eyes, and its academic research sector. China views the Five Eyes community as a threat to its ability to achieve its strategic objectives. As a core member of the Five Eyes alliance, Canada will continue to be targeted. To the detriment of Canada's national interest, hostile activities seek to foster support for Chinese international initiatives, to acquire sensitive military and security technology and expertise, to promote a pro-China narrative, and to portray China as a key partner for Canada in the areas of trade, investment, climate change and scientific cooperation.

China's persistent, long-term approach to hostile activities

For more on China's activities, see **Annex A**.

Russia

For decades, the Russian Federation has employed hostile activity tactics against Canada and its allies, former Soviet states, the former communist countries of Central and Eastern Europe, as well as in the Middle East, Africa and South America. Russia's domestic goals of maintaining territorial integrity, as well as regime stability, amid a faltering economy. Regional and global strategic goals involve reviving its standing as a great power within its perceived sphere of influence, weakening Euro-Atlantic partnerships, to change what it perceives as an unbalanced international order dominated by liberal democracies, to include what Russia considers to be its 'rightful place' on the global stage.

It seeks to attain these goals by influencing liberal democratic policy changes (e.g. economic sanctions) and fomenting divisions in a broader effort to weaken the democratic alliance by reducing citizens' trust in democratic institutions and processes. Russia sees Canada as a valuable target due to its global standing, membership in the G7, NATO and the "Five Eyes" intelligence community, and status as an Arctic nation. Canada's participation in other multilateral organizations and alliances, such as the Lima

Group and the Organization for the Prohibition of Chemical Weapons also make Canada a target for Russian hostile activity.

Russia engages in HASA across Canada's political system to influence government decision-making, sway public opinion, and undermine trust of specific elected officials. Russia conducts HASA via traditional tradecraft and by other means such as cyber, technical and SIGINT, in pursuit of its geopolitical objectives and core interests.
For more on Russia's activities, see **Annex A**.

Other Threat Actors

Other countries have and will continue to emerge as second tier threats to Canada. These include India, Pakistan,

India is a rising economic, regional and global power. In Canada, Indian officials have engaged in activities that go beyond the scope of regular diplomatic duties. They have utilized a network of contacts to engage in HASA and espionage including: collection of Canadian political information; dissident monitoring in Canada; interference with Canadian interests; influencing Canadian policy and political leaders and using clandestine sources to influence media.

While these examples stem from countries that have delicate relationships with Canada, not all states that conduct HASA against Canada's interests are considered hostile. It is also possible for foreign states to have significant positive diplomatic, economic or cultural ties to Canada, while still engaging in hostile activities against Canada's interests, adding to the complexity and nuance of this issue.

Canada's Approach

To effectively counter HASA, Canada must maintain active awareness of the evolving nature of the threats against its interests, and use a comprehensive range of actions to mitigate them while upholding Canadian values, right and sovereignty. A whole-of-society approach, which not only leverages the security and intelligence community, but also mobilizes non-traditional security and intelligence departments and other key partners within private industry, civil society, academia, other government jurisdictions, etc., is required. This approach is further bolstered by strategic and coordinated international partnerships, the use of which can amplify individual country efforts.

Though China, and to a lesser degree, Russia, currently pose the most active and persistent threats to Canada, and will likely continue to do so for the foreseeable future, Canada's approach is proactive and country agnostic to ensure that it can build resiliency and flexibility to mitigate and deter HASA from any foreign power as the threat evolves. However, actions to counter HASA will be commensurate with the threat level posed by each actor. Currently, given that China poses the greatest threat, efforts and resources will invariably be primarily directed at addressing its activities in Canada.

Five Priority Canadian Sectors

Based on assessment of Canada's national interest, and its overall vulnerability to HASA, five sectors were identified to prioritize Canada's counter HASA activities and resources: **democratic processes and government institutions; economic prosperity; international affairs and defence; social cohesion; and, critical infrastructure.**

Democratic Processes and Government Institutions

Electoral security; government infrastructure (including cyber systems) and personnel; political structures and institutions, parties and politicians

Threat actors target Canada's democratic processes and government institutions through a variety of means ranging from influence activities targeting current or potential political figures, to cyber intrusions on government infrastructure, to traditional espionage activities against government personnel. They may also seek to undermine Canadians' trust in their democratic institutions through the use of disinformation campaigns, among other tactics.

The stability and security of Canada depends on the integrity of its government bodies and electoral process, rule of law, fairness and openness of public institutions, and the protection of privacy and personal information. This underpins the government's ability to ensure and maintain the trust of its citizens, retain the credibility to protect and advance its national interests, and to project its core values abroad. Safeguarding government institutions from HASA is vital, as these institutions are the front line of the government's defences, ultimately enabling it to protect Canada's other priority sectors.

In addition, a robust overall security posture is critical to the Government of Canada's ability to fulfill its most essential functions. This includes protecting the government's secrets, such as national security operations and intelligence, trade negotiation strategies, Cabinet confidences, etc., from HASA, including insider threats and malicious cyber operations. Maintaining the integrity of government processes and systems, including cyber systems, staff, and physical facilities is crucial to Canada's sovereignty.

Economic Prosperity

Canada's economy; intellectual property and academic research in sensitive sectors; sensitive and emerging technology; supply chains; foreign direct investment; government research (including partnerships and grants) and, the Defence Industrial Base

A strong economy is itself a fundamental pillar of national security, and Canada's advanced industrial and technological capabilities, combined with expertise in certain sectors, make it an attractive target for HASA. Moreover, the extensive integration of the Canadian and US economies also creates opportunities for hostile actors to use Canada as a "backdoor" in to the US. Foreign threat actors have become increasingly adept at using licit and illicit means to obtain intellectual property and technology. This includes as the use of foreign direct investment, academic espionage, as access to exports from Canada and the shaping of international standards. Canada's Defence Industrial Base is a prime target for these efforts, and adversaries successes risk undermining an industry that contributes significantly to Canada's economic well-being, supports its strong relationship with the United States, and is critical to ensuring the Canadian Armed Forces is able to secure the capabilities it needs to defence the country; all important contributor to Canada's national interest.

Threat actors employ technical and human intelligence operations such as cyberespionage, exploitation of insider threats

HASA actors are also known to use economic ties as a strategic leveraging tool against Canada, for instance using trade restrictions in response to Canadian political activity perceived as unfavourable to foreign state interests.

Such activities undermine Canada's economic prosperity and enable foreign actors to advance their military abilities at the expense of our own, increase their intelligence collection capabilities, and leapfrog research and development. Such activities by adversaries will also diminish the willingness of allies to share intelligence and defence related technologies with Canada.

International Affairs and Defence

Canada's diplomatic affairs, missions and personnel abroad; foreign diplomatic activities in Canada; the Canadian Armed Forces; and, the Arctic

Canada's sovereignty at home and its presence in missions abroad, symbolizes its status as a country that contributes meaningfully to the rules-based international order. Canada constructively engages with regional, bilateral and multilateral partners in advancing positive actions and policies on global issues such as: strengthening global peace and security, promoting the rule of law, advancing inclusive approaches to trade, reducing poverty and gender inequality, and combatting climate change. Canada's assets abroad (personnel and equipment) serve as an extension of the Government of Canada's functions and are also fundamentally part of Canada's identity. Further, Canadian Armed Forces (CAF) members deployed abroad and Canada's diplomatic corps are frequently on the front lines of Canada's international approach to countering HASA. While deployed, the Canadian Armed Forces can be targeted through the use of hybrid warfare. For example, Canada's military works with allies and partners in upholding an international rules based order in highly strategic areas, including those where foreign states use hybrid tactics to achieve territorial and military expansion, such as in Ukraine, Latvia and the Asia Pacific region. Geopolitical competition and ambitions are likely to arise and test Canada's sovereignty, including in the Arctic, as global powers seek to advance their strategic, security, and natural resource interests in this region.

Social Cohesion

Canada's multicultural identity; ensuring safety of Canadians and communities from foreign interference; academic freedom; and, traditional and social media

Foreign threat actors may target any aspect of Canadian society to further their aims. In Canada, we are aware that diaspora communities may be targeted by foreign threat actors for a variety of reasons. Dissidents may be harassed or threatened, or the safety of their family abroad may be endangered because of their activism.

. Similarly, China uses its networks, along with officially sanctioned intimidation and harassment campaigns, in an effort to silence dissident members of Canada's Chinese communities and to control the wider discussion in Canada – both within Canadian civil society and at the political level – on China's human rights record, Falun Gong practitioners, the situation in Tibet and Hong Kong, and the status of China's Uyghur Muslim population. This type of activity is also present on Canadian campuses, where certain states may try to stifle academic freedom or activism that they view as contrary to their interests.

Threat actors also target Canada's social cohesion by exploiting societal wedge issues, including by pitting different civil society groups against each other. These activities can include information manipulation online to spread false narratives and amplify extreme views. This has been particularly acute during the pandemic, as both China and Russia have been deploying alternative narrative propaganda efforts questioning the origins of the virus, and criticizing the approach of liberal democracies. Canada must also be attentive to threat actors' attempts to plant fake activists in peaceful demonstrations to stir up violence and amplify divisions as this has been done elsewhere in the world.

Ensuring that all citizens have a sense of belonging and safety is fundamental to social cohesion in Canada. These hostile activities strike at the heart of Canada's values such as inclusivity, multiculturalism, and, freedom of expression, including academic freedom.

Critical Infrastructure

Energy; communications; health and transportation systems; financial services; and procurement-based threats to national security

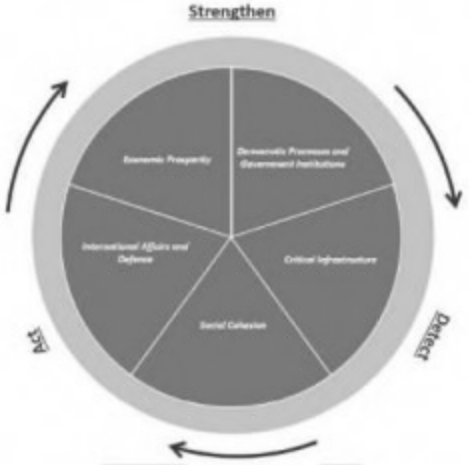
Critical infrastructure encompasses the processes, systems, assets and services that are necessary for maintaining the health, safety, security and/or economic well-being of Canadians and the effective operation of government. This includes the varied and complex energy, financial services, communications, health and transportation systems. Many of Canada's critical infrastructure systems are interconnected, both with one another, as well as across provinces, territories and other countries, particularly with the United States. While the responsibility for critical infrastructure in Canada is shared between federal; provincial and/or territorial governments; and local authorities; the majority of Canada's critical infrastructure is owned and operated by the private sector. It is for this reason that it is important to work closely with critical infrastructure owners and operators through partnership and information-sharing.

Foreign actors may target Canada's critical infrastructure systems for a number of reasons, ranging from seeking to undermine Canadians' confidence in their government's ability to protect them, to weakening Canada's military defensive posture. A failure in one mode of critical infrastructure can affect one or more of the others, and may embolden hostile actors to take advantage of a moment of vulnerability. Further, state owned enterprises have unlimited resources and use this as a competitive advantage in procurement activities in a manner that allows them to easily insert themselves into our infrastructure or our services, and compromise our security.

Three Pillars for Countering HASA in Canada: STRENGTHEN, DETECT, and ACT

Canada's strategy seeks first and foremost to make this country a more elusive target for foreign threat actors. Having outlined the key sectors we seek to protect, Canada's whole-of-government efforts to counter HASA fall under three broad pillars: **STRENGTHEN, DETECT**, and **ACT**. This provides the frame

under which the Government of Canada can consider its actions to counter this threat. Though this section outlines actions we can currently take, any future enhancements to Canada's counter HASA capabilities would fall under these pillars.



STRENGTHEN defences and resilience in priority sectors
Desired Outcomes

Proactively ensure that Canada faces the threat of HASA from a resilient position across all priority sectors

Activities under the STRENGTHEN pillar include:

- The implementation of the HASA governance model for the Government of Canada [policy work underway[4]];
- Ensuring that our intelligence collection priorities and resource distribution are in line with our assessment of the magnitude of the threat, and the main threat actors;
- Mitigating threats against government assets by bolstering the Government of Canada's security posture (including physical security, and general risk-awareness);
- Issuing procurement guidelines, alert bulletins, working with P/Ts, briefing DSOs and CSOs to counter procurement-based threat to national security;
- Implementing a communications framework which can be used as an operational tool to proactively build resilience against and respond to HASA in Canada;
- To help amplify the government's efforts, and building upon existing efforts, such as CSIS outreach activities, engaging with a wide range of stakeholders to ensure that varied experiences and points of view are captured, that at-risk groups feel empowered and foster a sense of collective responsibility;
- Continuing to work with other levels of government and the private sector to further secure Canada's digital infrastructure and its most important cyber networks;

[4] Where such a notation is indicated, this activity will be removed should it not be approved or launched by the time the Strategy is published.

- Enhancing accountability and transparency for federal funding (i.e. standard national security wording for Request for Proposals, Grants and Contribution Agreements) [policy work in this area is being considered];
- Providing enhanced risk awareness related to the five priority sectors in other levels of government within Canada. For example, continue to provide targeted threat briefings to newly elected politicians and political parties [policy work in other areas is ongoing];
- Investing in modern military capabilities and authorities to maintain a credible deterrent [policy work in this area is being considered];
- Supporting industry and academia with guidance or advice when collaborating with foreign entities [policy work is ongoing]:
    - Emphasis on sensitive technologies of concern from a national security perspective;
    - Mitigation measures and managing residual risk when collaborating with foreign entities; and,
    - Responding to national security concerns or breaches.
- Supporting stakeholder intelligence requirements with respect to HASA, including but not limited to awareness and indicators of assets of interest, methods of operations, and tactics that could be employed against them; and,
- Working with allies through bilateral and multilateral engagement. This acts as a force multiplier, helping to build capacity by learning from countries facing similar HASA challenges.

DETECT HASA that is planned or taking place and ensure understanding of its threat to Canadian interests

Desired Outcomes

Position Canada to detect HASA using a holistic, deliberate and systematic approach to intelligence and information collection, analysis, assessment and dissemination

Activities under the DETECT pillar include:

- Using a holistic approach to collection, analysis and assessment of intelligence to identify or anticipate HASA directed against Canadians and/or Canadian interests, including the use of bolstered foreign intelligence collection capabilities and a common rigorous threat assessment methodology covering intent, capability and opportunity [policy work underway];
- Enhanced use of classified and open source intelligence to identify threat vectors and inform the development of policy options/responses;
- Continuing to deepen our already sound understanding of the scope and scale of HASA in Canada, and broadening the dissemination, at various classification levels to ensure the broadest audience, of that knowledge to help identify our vulnerabilities and strengthen defences in the five priority sectors;
- Establishing efficient and timely channels for stakeholders in the private sector, academia or P/Ts to report suspicious activity for further investigation by law enforcement or intelligence agencies [policy work underway]; and,
- Effective screening of individuals for government security clearances, admissibility to Canada, access to controlled goods, and government procurement contracts, etc.

ACT to deter and respond to HASA with appropriate measures

Desired Outcome

Position Canada to prevent, deter or mitigate HASA events, and to take appropriate responsive action where warranted

Activities under the ACT pillar include:

- Exposing actions and motivations of threat actors in a timely manner including, non-ambiguous public attribution or revealing techniques of specific foreign actors, when appropriate, whether for the purpose of public communication, diplomatic démarches, coordination with allies, disruption, or covert response;
- Threat reduction activities (CSIS) where authorized by law;
- Cyber operations, including actions targeting the source of malicious activity;
- Reviewing of commercial activities with potential links to HASA, such as through foreign investment review under the *Investment Canada Act*, or applications for export permits for controlled goods; and,
- Criminal prosecution for HASA-related offences such as espionage, sabotage, intimidation, or unauthorized use of a computer;
- Diplomatic engagement with like-minded states, including through multilateral channels, pushing for norms/rules development (e.g. UN), as well as with countries that conduct HASA;
- Diplomatic and economic sanctions, either as part of a multilateral approach or unilaterally to specifically in defend Canadian interests;
- Military operations, such as deployments to support allies and an international rules-based order; and,
- Ensuring Canada is capable of a quick recovery in the event of a successful cyber operation(s).

Governance [Policy work ongoing to develop these options]

Canada's approach to countering HASA must be underpinned by a strong and clear governance structure. This ensures that Canada's HASA strategy, and the associated actions the government takes to counter this threat are cohesive and coordinated and comply with Canadian and international law. A counter HASA governance structure fulfills the following objectives:

Coordination of operational response and incident management

- Support the coordination of S&I and non-S&I operational activities in anticipation of and in response to HASA, including incident management and strategic communications.
- Support the inter-departmental planning of proactive HASA responses as well as coordination of risk acceptance in the context of Canadian and international law and norms.

Coordination of intelligence dissemination and situational awareness

- On an ongoing basis, promote a clear understanding of HASA threats across the Government through the preparation and/or timely dissemination of assessments informed by the Canadian intelligence community and key international allies;
- Key elements to successful assessment governance include a coordinated, all-source/all-community approach; understanding of the client needs; good access to intelligence of relevant collectors; a clear, rigorous methodology; tailored dissemination; clear accountability; and sustainability;

- Ensure stakeholders are provided with actionable intelligence with minimal delay, increasing the effectiveness of Canada's response and/or mitigation efforts; and,
- Facilitate direct lines of communication with senior decision-makers, should an issue be deemed sensitive, high-profile or necessitate risk management.

Coordination of policy analysis and development

- Coordinate and support the implementation of HASA-related policies and strategies, including those associated with non-traditional S&I partners;
- Coordinate and assess resource needs within the whole-of-government model; and,
- Build upon existing institutional expertise and resources, to enhance efficiencies and create synergies with and between current activities and capacities across the Government.

Coordination of engagement and outreach

- Coordinate strategic communications and engagement with key stakeholders—municipalities, provinces/territories, law enforcement partners, the private sector, academia, non-governmental organizations, communities, etc.—and the general public to build awareness of, and resilience through empowerment against, the threat posed by HASA; and,
- Coordinate engagement, across the GoC with Five Eyes partners, the G7, NATO and other like-minded countries to promote a coherent multilateral approach to countering HASA;

Annex A

HASA Threat Actors

China

China pursues its goals by establishing and then leveraging bilateral political and economic relationships with other states to dis-incentivize them from adopting policies with which China does not agree. Additionally, China leverages emerging technologies and societal power structures to exert totalitarian control over its citizens and overseas communities of Chinese descent. It does so to prevent potential challengers from undermining the primacy of the CCP as well as to work towards its goal of building a military that can dominate in the Asia-Pacific and project power globally. China also leverages international fora, such as the UN, to undermine liberal democratic institutions and advance its interest and embedding its ideology. Finally, China's increasingly aggressive foreign policy shows its willingness to use economic and political levers, including hostage diplomacy.

The Chinese state supplements its use of traditional tools of statecraft (e.g., intelligence agencies, officials in Canada, military forces, government institutions) with non-traditional actors that have been co-opted to act in the interests of the state. China considers all ethnic Chinese, regardless of citizenship, and all Chinese companies to be intelligence assets capable of providing information/intelligence for the benefit of the People's Republic of China (PRC) and expects them to fulfill their duty to advance the PRC's interests. This is enshrined in Article 7 of China's National Intelligence Law of 2017, which requires Chinese organizations and citizens to "support, assist and cooperate with state intelligence work".

The United Front Work Department (UFWD), active in all Chinese embassies abroad, is at the forefront of China's efforts to conduct foreign interference globally. Under President Xi,

China often relies on the exploitation of bilateral Canada-China economic ties to pursue its economic objectives through: . Using these means, China targets specific areas including:

- Emerging technology
- Early stage research in science, technology, engineering, mathematics (STEM) fields;
-
- Small, medium and large enterprises; and
- Critical infrastructure (transportation, telecommunications, energy, health, agriculture, and government).

The biopharmaceutical and healthcare sectors have been and will continue to be at a high risk during the pandemic. As states continue to accelerate their COVID-19 research and development to support the pandemic response, China is seeking to exploit the aforementioned threat vectors and global economic downturn to invest in companies with sensitive technologies or asset of interest, which may be in financial distress. Other at risk sectors include advanced manufacturing (e.g. semiconductors), artificial intelligence, quantum, big data analytics, and 5G.

This recent cyber threat activity by China continues its long history of gaining access to information in other countries via its large and highly capable cyber expertise.

As the pandemic continues to unfold, Canada finds itself among like-minded democracies as a target of China's disinformation campaigns or alternative narrative propaganda efforts questioning the origins of the virus, praising the regime's success in containing it and criticizing the approach of liberal democracies. Spreading disinformation on social media including Twitter, a platform largely inaccessible to domestic Chinese users, shows that the CCP is further seeking to control its messaging beyond China's borders. In addition to deflecting blame, it is also likely an effort to demonstrate to international and domestic Chinese observers that the Chinese government will protect its people.

Russia

Russia leverages numerous government and non-government entities to support its influence efforts. In addition to the highly capable intelligence services, Russia utilizes current and former senior political figures, diaspora and compatriot groups, cultural and economic entities, the media, and its diplomatic staff to carry out interference and espionage activities. Oligarchs, organized crime, and the Russian state also have a symbiotic relationship, often cooperating for mutual benefit. For example, seemingly legitimate businesses or commercial activity may in fact be a guise for criminal activity that has the potential to cause significant harm to Canada's national security. The introduction of illicit funding into the Canadian economy is a national security risk due to its impact on the integrity of the financial system and economy.

Russia is an active and highly sophisticated cyber threat actor that uses cyber threat activity to support its economic and security intelligence priorities, including domestic surveillance, cyber espionage, and aggressive online foreign influence operations. In addition, Russian targeting of global telecommunications infrastructure . Russia is willing to leverage disruptive and destructive cyber threat activities as a means of coercion against countries within Russia's perceived sphere of influence, particularly Ukraine. Although to a much lesser extent, Russia targets critical infrastructure in Canada and other Western states, in a similar manner, In mid-July 2020, CSE released a joint statement alongside the United States and the United Kingdom attributing a recent malicious cyber campaign to Russian intelligence. These cyber activities conducted by proxies of Russia were very likely aimed at

stealing information and intellectual property related to the development and testing of COVID-19 vaccines.

During the pandemic, Russia has increased its information operations, spreading disinformation and exploiting wedge issues in liberal democratic countries. For example, the Canadian-led NATO battle group in Latvia was the target of pandemic-related disinformation attributed to Russia. The Russians sought to spread false rumours in Baltic and Eastern European media outlets that camps housing foreign troops had high numbers of infections, posing health risks to nearby communities.

Additionally, Russia seeks to modernize its military and improve its intelligence capabilities via clandestine procurement.

Additionally, China and Russia are known to cooperate with each other on issues of shared interest,