UNCLASSIFIED

2 AUGUST 2019

SITE TF BULLETIN

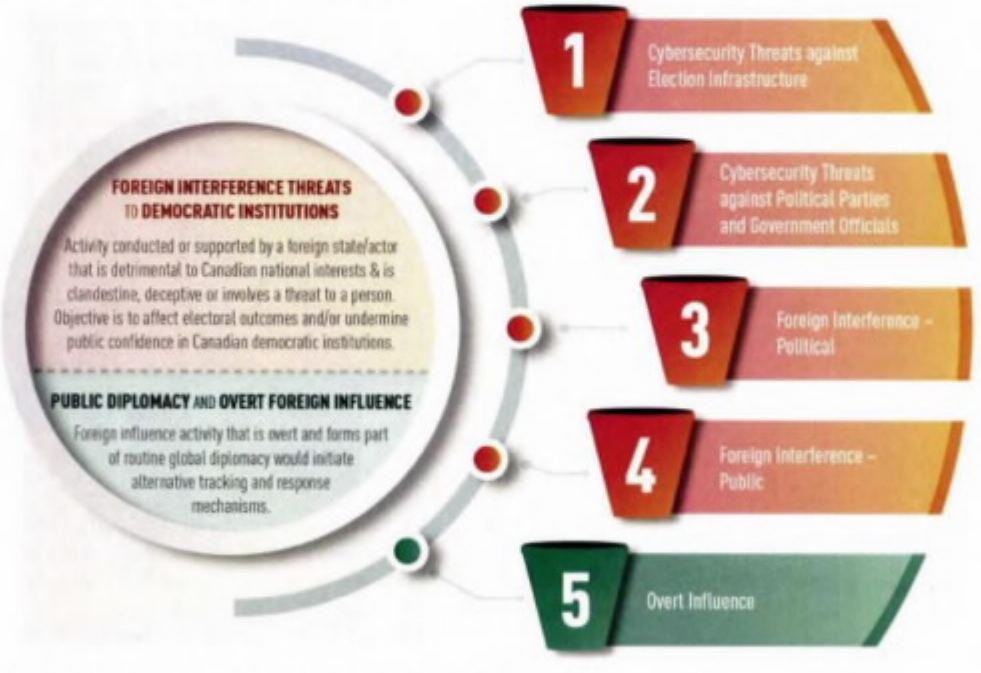
UNDERSTANDING FOREIGN INTERFERENCE

This is a product of the Security and Intelligence Threats to Elections (SITE) Task Force (TF). It has been produced to improve situational awareness, and provide interested stakeholders with a better understanding of foreign interference.

SITE TF Overview:

Recognizing the complexity of foreign interference activity facing Canada, SITE has developed a playbook for understanding what is meant by the terms 'foreign interference' and 'foreign influence', and the different spheres these activities can impact. SITE defines foreign interference as activity that is conducted by, or at the behest of, a foreign state/actor, is detrimental to Canadian national interests and is clandestine, deceptive or coercive. Foreign interference can have many objectives but this bulletin will focus on that which is designed to impact electoral outcomes and/or undermine public confidence in Canadian democratic systems or processes. Foreign influence activity is overt and forms a part of routine global diplomatic engagement. It is important to note the distinction between 'influence' and 'interference' as they initiate different tracking and response mechanisms.

Based on these definitions, SITE has identified four categories of foreign interference activity and one category of foreign influence activity (see diagram below):



- **Bin 1: Cybersecurity threats against election infrastructure**
  - Threats that are malicious and deliberate attempts directed, subsidized or undertaken by – or on behalf of – a foreign state/actor targeting Canadian election infrastructure.
  - Threats to Canada's elections infrastructure targeting information technology (IT) systems supporting the election; the owners and operators of electoral IT systems; individuals accountable for the election (i.e. electoral officials); and, the vendors of hardware and/or software that is used within the elections infrastructure.

UNCLASSIFIED

- **Bin 2: Cybersecurity threats against government officials, political parties or electoral candidates.**
  - Malicious and deliberate attempts directed, subsidized or undertaken by – or on behalf of – a foreign state/actor that targets Canadian government officials, Canadian political parties or electoral candidates.
  - In these instances, the IT systems of a Canadian political party, candidate or government official would be threatened.

Depending on the context of the threat, for example a foreign-nexus vs. a domestic-nexus, either (or both) CSE's or CSIS' authorities could be leveraged in response to a threat within Bin 1 or 2.

- **Bin 3: Foreign Interference – Political**
  - Foreign interference activity that targets Canadian government officials, political organizations or electoral candidates with the goal of impacting electoral outcomes, and/or undermining their policies, positions and opinions.
  - This threat activity is conducted in a clandestine, deceptive or coercive manner and is directed, subsidized, or undertaken by – or on behalf of – a foreign state/actor.
- **Bin 4: Foreign Interference – Public**
  - Foreign interference activity that targets the Canadian public and/or discrete populations, such as local diaspora communities.
  - The objective of this type of activity is to impact electoral outcomes, sow societal discord, sway public sentiment within Canada to undermine Canadians' confidence in the electoral system and processes and/or support the foreign state's/actor's own national interests and agenda.

Given the clandestine, deceptive or coercive nature of these threats, CSE and CSIS are able to provide SITE with intelligence reporting on threats within Bins 3 and 4, and are in a position to respond where their mandates and capabilities allow. Moreover, should the threat aim to undermine public trust in elected officials and/or governance structures, or target socially divisive issues to increase social tensions using social media, in addition to CSE and CSIS, GAC may also be engaged via their Rapid Response Mechanism with Bins 3 and 4 to provide SITE with an analysis and assessment of the threat activity. For Bins 1 through 4, should the threat in question meet the threshold of criminality, the RCMP may also choose to pursue a criminal investigation.

- **Bin 5: Overt Influence**
  - Overt influence refers to the use of public diplomacy and other means whereby a foreign state openly attempts to influence Canadian policy, the political landscape and/or electoral processes. Similar to the other Bins, one goal of overt influence activity can be to affect electoral outcomes within Canada but because it is overt and transparent, it initiates alternative diplomacy response mechanisms.
  - Given the overt and often political nature of this activity, GAC is best positioned to respond to concerns within Bin 5.

Using these bins to frame how a threat affects Canada's democratic institutions and electoral process allows SITE to identify which agency is best positioned to address the threat at hand. Such a framework will allow SITE to rapidly understand incoming threats, and coordinate amongst the TF members appropriately. Moving forward, SITE will ensure that its definitions of foreign interference and foreign influence, as well as the 5 Bins, remain adaptable to changes in the threat landscape.