

SECRET//CEO**Security and Intelligence Threats to Elections Task Force (SITE TF) – Lessons Learned Summary**

(U) In August 2018, the Government of Canada created the Security and Intelligence Threats to Elections Task Force (SITE TF) – an operationally-focused body – to address threats of foreign interference in the 2019 Canadian federal election. SITE TF membership:

- Communications Security Establishment (SIGINT)
- Canadian Security and Intelligence Service (HUMINT)
- Global Affairs Canada (International Affairs)
- Royal Canadian Mounted Police (Law Enforcement)

(U) The four pillars of SITE's mandate were:

1. Provide government partners engaged in elections-related work with a clear point of engagement within the security and intelligence (S&I) community.
2. Conduct a review of existing intelligence collection efforts across SITE TF agencies, ensuring our collective posture is focused on the threat of foreign interference.
3. Increase the situational awareness of Cabinet, government and non-government partners, and senior public servants.
4. Promote the use of intelligence, assessment, and open-source information analysis in the protection of electoral processes through sharing with other government partners or, when mandates permit, taking direct action.

Pre-election (starting 12 months before the election)

- Held weekly meetings to share intelligence and coordinate activities
- Conducted baseline threat assessment and review of intelligence coverage to prioritize threat actors, identify gaps and steer collection efforts
- Established an analytic body to support SITE TF
- Conducted interdepartmental Table Top Exercises (TTXs) and established internal communications protocols
- Used TTX to inform creation of Response Options document
- Provided regular threat briefs to Ministers and various government stakeholders – including regular engagement with Elections Canada
- Engaged with allies for lessons learned on their experiences

Support during the election (starting 4 weeks before the election)

- Provided SECRET-level briefings to cleared members of political parties
- Daily secure SITE TF calls to review intelligence/actions/follow-up
- Issued Daily SITREPs to senior government officials, informing of threats/activities
- 24/7 on-call, and co-location of SITE TF reps with CCCS on surge floor during election

Post-election

- 24/7 on-call for one-week post-election
- Prepared After Action Report which included summary of SITE TF activities, assessment of threats and recommendations on future efforts

SECRET//CEO**Lessons Learned**

- Clarity of mission, clear terms of reference and an appropriate scope of work provided focus to SITE
- Multidisciplinary teaming facilitated access to a broad range of expertise, collection sources and authorities in order to identify, assess and mitigate threats
- TTXs and testing off-hours protocols were essential to resolving issues and reinforcing the principles of communications ahead of formal surge posture
- Early engagement with partners was essential to building trust, increasing confidence, and establishing a common language and understanding of the threat
- A single point for coordinating media queries ensured consistency of messaging
- Clear and frequent communications with senior government officials during the writ provided reassurance and a common and timely understanding of the threat picture

Challenges

- Measuring the impact of foreign interference on elections remains difficult
- Increasingly difficult to distinguish between 'foreign' and 'domestic' interference
- Multidisciplinary teaming highlighted differences in analytic methodologies
- There is a need to balance the protection of highly sensitive intelligence and appropriate dissemination of this intelligence to enable assessment/action
- Strategic communications plans need to be established early on (determining desired level of engagement with the public)
- Counter foreign interference efforts need to be prioritized over the long-term; re-orienting collection assets and training analysts takes time