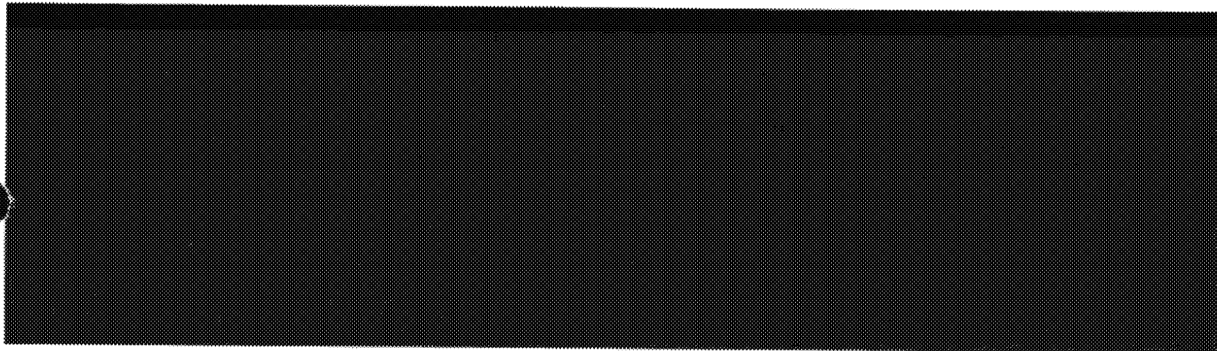


- # Security and Intelligence Threats to Elections Task Force After Action Report (2019 Federal Election)

- AUGUST 2020

HIGHEST CLASSIFICATION OF THIS DOCUMENT: TS/ /CEO



SITE TF AAR

Highest Classification:
TOP SECRET//CEO

Contents

1.0	(U) EXECUTIVE SUMMARY	2
2.0	(U) ABOUT SITE TF	4
2.1	(U) MISSION AND MANDATE	4
2.2	(U) WHAT DID SITE TF DO?	4
2.2.1	(U) Operational Activities before Writ and Electoral Periods	4
2.2.2	(U) Operational Activities: Writ and Electoral Periods	6
2.2.3	(U) Briefings, Communications and Engagements	7
2.2.4	(U) Engagement with International Partners	8
3.0	(U) FOREIGN INTERFERENCE THREATS RECAP	9
3.1	(U) INITIAL THREAT COVERAGE REVIEW	9
3.2	(U) SUMMARY OF THREAT ISSUES OBSERVED	10
3.2.1	(U) Category 1: Cybersecurity Threats against Electoral Infrastructure	10
3.2.2	(U) Category 2: Cybersecurity Threats against Political Parties and Government Officials	10
3.2.3	(U) Category 3: Foreign Interference - Political	10
3.2.4	(U) Category 4: Foreign Interference - Public	11
3.2.5	(U) Category 5: Overt Influence	12
3.3	(U) OVERALL THREAT ASSESSMENT	12
4.0	(U) SITE TF LESSONS LEARNED	13
4.1	(U) THREAT ANALYSIS	13
4.1.1	(U) Detection of Interference Threats	13
4.1.2	(U) Assessment of Interference Threats	14
4.2	(U) SITE TF RESPONSE POSTURE	15
4.2.1	(U) Responding to Threats	15
4.3	(U) ENGAGEMENT AND COMMUNICATIONS	15
4.3.1	(U) Internal SITE TF Engagement	15
4.3.2	(U) Engagement with Other Government Departments	16
4.3.3	(U) Engagement with Political Parties	16
4.3.4	(U) Engagement with Social Media	17
4.3.5	(U) Engagement with Traditional Media	17
4.3.6	(U) Engagement with Non-Government Experts	17
4.3.7	(U) Engagement with International Partners	17
4.4	(U) A FINAL TAKE-AWAY	18
4.5	(U) Future of SITE	18
5.0	(U) ANNEX	19
5.1	(U) GLOSSARY	19
5.2	(U) SITE TF TERMS OF REFERENCE	20
5.3	(U) DETAILED THREAT ASSESSMENT	ERROR! BOOKMARK NOT DEFINED.1

SITE TF AAR

Highest Classification:
TOP SECRET//[REDACTED]/CEO**1.0 (U) EXECUTIVE SUMMARY**

(U) In August 2018, the Government of Canada (GoC) created the Security and Intelligence Threats to Elections Task Force (SITE TF or "the Task Force") – an operationally-focused body – to address threats of foreign interference in the 2019 Canadian federal election. SITE TF's mandate necessitated a range of activities by the Communications Security Establishment (CSE), the Canadian Security Intelligence Service (CSIS), the Royal Canadian Mounted Police (RCMP), and Global Affairs Canada (GAC), in what was a first time for an interdepartmental effort, around the collection and use of intelligence related to foreign interference. This after action report (AAR) details SITE TF's activities, foreign interference threats observed, operational successes and challenges, and the way forward for the Task Force.

(U) FOREIGN INTERFERENCE THREATS

(S//[REDACTED]) Shortly after its inauguration, SITE TF established a baseline assessment of key foreign state actors and foreign interference threats to the 2019 Canadian federal election ("the election") to help prioritize collection and assessment efforts. Over the course of its operations from September 2018 to October 2019, SITE TF saw no evidence to indicate that foreign state actors were specifically targeting Elections Canada (EC) or Canadian electoral systems and networks. The Task Force also saw no evidence of a broad-based foreign state-directed interference campaign in the digital information ecosystem, but notes that there were blind spots in SITE TF's ability to determine state attribution and distinguish between foreign and domestic disinformation campaigns. However, SITE TF did observe foreign interference activities targeting certain ridings and candidates in relation to the election, directed largely from China, and to a lesser extent from India and Pakistan, [REDACTED] SITE TF assessed that none of these foreign interference activities were part of a broad-based electoral interference campaign and did not have an impact on the overall outcome of the election. In addition, none of the activities met the threshold to pursue criminal investigations.

(U) SITE TF SUCCESSES

(U) SITE TF fulfilled all four parts of its mandate:

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.

(U) The well-defined mandate and relatively narrow focus on the election allowed for a concentration of effort and efficient use of resources. Additionally, the multi-disciplinary approach allowed for the leveraging of SITE TF agencies' different mandates, methodologies, and information, while the small group allowed for focused and topical discussion.

(U) Other successful aspects of operations included:

- The **development of a threat categorization system**, which served internally as a common base of understanding but also as a key communication tool for partners and stakeholders as to the nature of the foreign interference activity Canada was facing.
- The **development of a Response Options Matrix** for scenario-based decision making on key foreign interference threats.

SITE TF AAR

Highest Classification:
TOP SECRET//CEO

The **establishment of a joint analytic effort** (i.e. the Technical Table or "the Tech Table") focused on intelligence collection assessment, and open-source analytics related to foreign interference activities online.

- An **open and collaborative approach** to sharing and discussion among SITE TF members.
- A novel engagement with **SECRET-cleared representatives of political parties**, service as both an education platform and assisting in instilling confidence that confronting foreign interference was a priority.

(U) SITE TF CHALLENGES

(S//CEO) SITE TF experienced a number of challenges, primarily around technical operations, engagements, and the assessments of threats:

- Re-orienting collection assets and training analysts to better understand and identify foreign interference activities takes time, highlighting the need to **prioritize and resource foreign interference efforts** over the long-term, and not exclusively around election periods.
- **Frequent ad-hoc inquiries** – often related to media headlines, and sometimes outside the scope of SITE TF's work – distracted the Task Force at times from focusing efforts on adversaries of concern.
- While openness and collaboration were positive attributes of SITE TF, instances of classified information leaked to the media was concerning. This accentuated the need to **reinforce the sensitive nature of information** during extended briefings and distribution of material.
- **Social media companies were reluctant to provide data**, in absence of a formal legal process, leaving SITE TF with the same information available to the public.
- The **determination of "foreignness"** of suspicious actors and the distinction between foreign versus domestic interference were difficult. This will become more challenging as sophisticated foreign actors emulate or amplify domestic actors.
- Joint assessment was challenging with **differences in methodologies** among SITE TF members, highlighting the need for common attribution criteria, analytical standards, and language to avoid delays and withstand rigorous review outside SITE TF.
- It is difficult, if not impossible, to assess the impact of foreign interference activities in the digital information ecosystem on an election, given the **opacity and complexity of voter behaviour**.

SITE TF AAR

Highest Classification:
TOP SECRET, [redacted]//CEO

2. (U) ABOUT SITE TF

2.1 (U) Mission and Mandate

(U) In August 2018, the Government of Canada (GoC) created the Security and Intelligence Threats to Elections Task Force (SITE TF or "the Task Force") to identify and advise the government on covert, clandestine, or criminal activities interfering with or influencing electoral processes in Canada. SITE TF was specifically tasked to:

1. Provide government partners engaged in elections-related work with a clear point of engagement within the 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; and
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.

(U) The membership of the SITE TF included CSE, CSIS, RCMP, and GAC. To ensure the Task Force fulfilled its mandate, two principal bodies were established: an assistant deputy ministers (ADMs) forum, which set SITE TF's priorities; and an operational-level forum, which oversaw its day-to-day operations. The ADM forum included the Task Force's chairperson, CSE Deputy Chief of Signal Intelligence (SIGINT), CSIS Deputy Director of Operations, RCMP Executive Director General of the Federal Policing National Security and Protective Policing, GAC ADM of International Security, and Privy Council Office (PCO) Assistant Secretary to Cabinet, Security and Intelligence. The operational level similarly comprised the Task Force's chairperson from CSE, and representatives from CSIS, RCMP, and GAC. The SITE TF Terms of Reference (TOR) can be found in Annex 5.2.

2.2 (U) What did SITE TF do?

2.2.1 (U) Operational Activities before Writ and Electoral Periods

(U) The majority of SITE TF's operational work occurred prior to the issuance of the writ. The Task Force met weekly to share relevant intelligence, provide general updates, and discuss ongoing operational matters.

(S// [redacted]) Establishment of the Tech Table

(S// [redacted]) In November 2018, the SITE TF directed their respective analytic units to coordinate efforts to combat foreign interference operations online. Known as the "Technical Table" (or the "Tech Table"), analytic units from CSE, GAC, and CSIS held discussions and tabletop exercises (TTXs) to better understand each other's mandates, authorities, and capabilities. The results informed the development of SITE TF information sharing processes and internal coordination. The mandate of the Tech Table is as follows:

- Review and focus intelligence collection assessment, and open-source analytics related to foreign interference activities online threatening democratic institutions and electoral processes in a coordinated manner.
- Improve communication and share information between GoC partners pursuant to existing authorities, including reporting to the SITE TF.

SITE TF AAR

Highest Classification:
TOP SECRET//[REDACTED]/CEO

(S/[REDACTED]) The Tech Table met on a regular basis, and members attended the SITE TF meetings to provide updates on their efforts. An AAR specifically focused on the Tech Table was also completed along with this SITE TF report.

(U) Analytic Products

(U) SITE TF developed several analytic products, which helped in defining and addressing threats to the election and clarifying engagement processes both internal and external to SITE TF: the *Combined Threat Coverage Review*, the *SITE TF Playbook and Response Options Matrix*, and a series of *SITE Bulletins*.

• (U) *Combined Threat Coverage Review*

(S/[REDACTED]) SITE TF's *Combined Threat Coverage Review* was created for the Task Force to establish a baseline assessment of foreign state actors who had the capability and intent to interfere in the Canadian election. [REDACTED] the *Review* outlined the key foreign state actors of potential threat, identified the targets' capabilities and intent, prioritized their threat level to Canada, and compared existing intelligence coverage of those targets. This *Review* provided guidance for SITE TF to align collection and analytical efforts, identify and address intelligence gaps, as well as inform future TTXs and SITE TF response mechanisms as outlined in the *SITE TF Playbook and Response Options Matrix* below.

• (U) *SITE TF Playbook and Response Options Matrix*

(S/[REDACTED]) SITE TF members held a series of TTXs in order to reinforce awareness and compliance of the Task Force members' respective mandate and authorities, and to test responses to the various threats scenarios. The results of these TTXs were used as a basis for building the *SITE TF Playbook* – a detailed document that outlines different foreign interference scenarios along with a range of potential responses based on each agency's respective mandates and authorities. An abbreviated version of the *Playbook* – *The Response Options Matrix* – was created as a quick reference guide for SITE TF and senior decision makers, which was circulated among SITE TF ADMs, Deputy Ministers (DMs), and the Critical Election Incident Public Protocol Panel ("Panel of Five").

• (U) *Bulletin on Monitoring and Responding to the 2019 Threat Landscape*

(S/[REDACTED]) SITE TF created this bulletin to provide situational awareness of the threat to a broader audience at a lower classification level (SECRET). This bulletin included the key takeaways from the *Combined Threat Coverage Review*, as well as additional assessments of the foreign interference threat actors and their tradecraft. This bulletin principally focused on China and Russia as the most significant threat actors.

• (U) *Bulletin on Understanding Foreign Interference*

(U) To better contextualize the threat environment for stakeholders, the Task Force published an unclassified bulletin defining four categories of foreign interference activities and distinguishing that from foreign influence activities. In this document, SITE TF defined foreign interference as an "activity conducted or supported by a foreign state/actor that is detrimental to Canadian national interests and is clandestine, deceptive or involves a threat to a person. The objective is to affect electoral outcomes and/or undermine public confidence in Canadian democratic institutions." With the broad range of foreign interference activities, the *Bulletin* focused on foreign state-directed activities intended to impact electoral outcomes and/or undermine public confidence in Canadian democratic systems or processes. This categorization allowed SITE TF to understand and triage incoming threats, coordinate responses, and identify the agency best positioned to address the threat. The categories were:

1. Cyber security threats against election infrastructure (CSE and CSIS lead)
2. Cyber security threats against government officials, political parties, or electoral candidates (CSE and CSIS lead)
3. Foreign Interference – Political (all SITE TF)

SITE TF AAR

Highest Classification:
TOP SECRET//[]/CEO

4. Foreign Interference – Public (all SITE TF)
5. Overt foreign influence (GAC lead, identified to distinguish diplomatic practice from interference)

- *(U) Bulletin on Social Media and Foreign Interference*

(U) The use and abuse of social media for foreign interference purposes was and remains a complex issue for SITE TF, and an area of concern for stakeholders. This bulletin was drafted to better define SITE TF's role and to clearly articulate which agencies would engage with partners in the social media space and how. For example, CSE would collaborate with social media companies to pursue cyber threats against Canadian democratic institutions through threat intelligence sharing and incident management coordination. Whereas, CSIS would engage government, external partners and social media companies on specific instances of social media activity possibly linked to foreign interference in the election. GAC's Rapid Response Mechanism (RRM) Canada would examine trends and tactics across the digital information landscape to identify coercive, corrupt, covert or malicious activities undertaken by foreign actors. Finally, the RCMP would be responsible for investigating criminal activities associated with foreign interference in the election over social media.

- *(U) Bulletin on Communications Protocols*

(U) Recognizing the need for clear communications guidelines, SITE TF developed a communications protocol in preparation for the election. The protocol had three main goals:

1. Provide clarity on how GoC departments and agencies should engage with the Task Force;
2. Explain what the other government departments (OGDs) could expect from SITE TF following a request; and
3. Enable notification of SITE TF members in emergencies.

(U) To ensure timely dissemination of information, tracking protocols were established and included the integration of each Task Force member's operation centre. Operating 24/7, these operation centres were responsible for disseminating incoming alerts to SITE TF members based on operational directives.

- *(TS//CEO)* [redacted]

(TS//CEO) [redacted]

Summary of potential inauthentic foreign state-sponsored activity on various social media platforms.

2.2.2 (U) Operational Activities: Writ and Electoral Periods

(U) During the writ and electoral periods, SITE TF developed a proactive response posture to reflect the anticipated pace of a possible foreign interference event.

(U) First, an off-hours communications and response protocol was established during the writ period to ensure that all Task Force members were alerted to any foreign interference threats related to the Canadian election in timely manner.

(U) These calls also acted as a clearinghouse, allowing SITE TF agencies to focus on medium- and long-term issues during the regular meetings.

(U) Finally, daily situational reports (SITREPs) were issued to SITE TF ADMs and the Panel of Five providing timely information on relevant foreign interference threats, SITE TF's corresponding activities and an overall threat level on the day.

SITE TF AAR

Highest Classification:
TOP SECRET///CEO

2.2.3 (U) Briefings, Communications and Engagements

(U) Since the launch of the Task Force in August 2018, engagement and communications have been a primary line of effort for SITE TF. Engagement and communications span a range of activities from the production of weekly records of discussion (RoDs), to meetings with social media companies. The group also engaged with numerous domestic and foreign partners to build relationships, exchange operational best practices, and share insights on foreign interference threats observed.

(U) SITE TF Internal Communications

(U) SITE TF met weekly and the ADM fora met monthly. RoDs were maintained for all of these meetings to provide transparency to the groups' discussions and decisions, and to keep track of action items and threat issues.

(U) Briefings to Government Officials

(U) SITE TF regularly briefed senior government members on the Task Force's ongoing work and key foreign interference threats observed. These briefings proved essential to the success of SITE TF by keeping relevant government officials apprised of key events and developments, as well as instilling confidence that SITE TF was prepared to address foreign interference threats as they arose. In addition, SITE TF also delivered regular classified threat briefings to SECRET-cleared representatives of Canadian political parties. These briefings provided opportunities for the Task Force to inform the political parties on key foreign interference threats, and to address their concerns on dealing with these threats.

(U) Communications with Traditional Media

(U) Responses to media inquiries were done via the external communications departments of each SITE TF agency. The respective communications departments then coordinated with PCO's communications department on delivering a succinct and consistent messaging on behalf of the SITE TF via PCO. In addition, SITE TF ADMs provided a technical briefing to members of the media ahead of the January 2019 public announcement on GoC efforts to safeguard the election from foreign interference.

(U) Engagement with Domestic Partners

(U) On the domestic front, SITE TF engaged with many GoC partners, including PCO Security and Intelligence Secretariat (PCO SI), PCO Intelligence Assessment Secretariat (PCO IAS), PCO Democratic Institutions (PCO DI), PCO Tiger Team, Director General of Electoral Security Coordination Committee, Department of Public Safety's Hostile Activities by State Actors (HASA) Team, EC, and the Commissioner of Canada Elections (CCE). Most often, these engagements were to inform partners of SITE TF's work, advise on the threat landscape, and build an operational rapport to facilitate information exchange.

(U) Engagement with Non-Government Experts

(U) SITE TF engaged with non-government experts leading to the writ, including the Atlantic Council's Digital Forensics Research Lab, Oxford Internet Institute, Institute for Strategic Dialogue, and McGill University. This engagement contributed to a better understanding of emerging threats in the digital information ecosystem and helped calibrate open source methodologies and approaches to identify foreign interference activities in the digital information ecosystem. However, given caretaker period-related constraints around communications, engagement was limited during the writ period.

(U) Engagement with Social Media Companies

(S//) Recognizing the importance of social media in combatting foreign interference and disinformation, the Task Force reached out to various social media companies to establish relationships.

SITE TF AAR

Highest Classification:
TOP SECRET//[REDACTED]/CEO

[REDACTED]

(U) Engagement with International Partners

- (U) Five-Eyes partners

(S//[REDACTED]) United States (US) – [REDACTED]
[REDACTED]

(S//[REDACTED]) Australia – [REDACTED]
[REDACTED]

(S//[REDACTED]) United Kingdom (UK) – [REDACTED]
[REDACTED]

- (U) European partners

(U) European Centre of Excellence for Countering Hybrid Threats – In early 2019, GAC engaged with the European Centre of Excellence for Countering Hybrid Threats, based in Helsinki, to better understand their analytic and training efforts. Two training sessions were hosted in Canada, whereby over 200 GoC personnel were trained on aspects of protecting democratic institutions and best practices for countering information influence activities.

(S//[REDACTED]) – From March to May 2019, RCMP [REDACTED] deployed personnel to [REDACTED] as part of an RCMP arrangement with the [REDACTED]. The analysts were embedded within [REDACTED] and observed [REDACTED] electoral security operations in the lead up to their presidential elections.

[REDACTED]

(S//[REDACTED]) SIGINT Seniors Europe (SSEUR) – [REDACTED]
[REDACTED]

SITE TF AAR



Highest Classification:
TOP SECRET///CEO

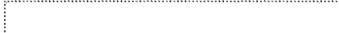

- (U) Other international partners









(U) Singapore - SITE TF had discussions with the Singaporean Ministry of Home Affairs, and a follow-up visit with their Ministry of Defence to discuss how the GoC was preparing to secure the elections, and more specifically how SITE TF was functioning.


3. (U) FOREIGN INTERFERENCE THREATS RECAP

3.1 (U) Initial Threat Coverage Review

(TS///CEO) The SITE TF's *Combined Threat Coverage Review* identified  key state actors posing potential foreign interference threats to the Canadian electoral process. The table below captures SITE TF's assessment of their capability and intent to interfere with the elections.

 Even though these  state actors were of higher priority, the Task Force maintained situational awareness on other threat actors who might arise over the course of its operations.

Country	Capability	Intent
 PRC		
 Russia		
 India		
 Pakistan		
 Iran		
		

(TS///CEO) SITE TF also forecasted the overall threat landscape ahead of the election period as follows:

1. The threat landscape in Canada would likely remain consistent with previous patterns and behaviours.
2. HUMINT threat activity would likely be the most pervasive form of foreign interference threat to the Canadian electoral processes.
3. The use of social media by hostile foreign states to conduct disinformation campaigns had increased globally, with some instances of this activity being directed against Western democracies. This trend was likely to extend to Canada as well.

SITE TF AAR

Highest Classification:
TOP SECRET/[redacted]/CEO

3.2 (U) Summary of Threat Issues Observed

(S/[redacted]) From September 2018 to October 2019, SITE TF regularly discussed and tracked foreign interference-related issues and incidents, including those directed at Canada and those not directed at Canada but warranting SITE TF's attention (e.g. adversary capability building and/or posturing for potential foreign interference campaigns).

[redacted] The section that follows is a summary of observed threats organized according to the foreign interference threat categories outlined in the *Bulletin on Understanding Foreign Interference*. Annex 6.3 provides further details on these threats.

3.2.1 (U) Category 1: Cybersecurity Threats against Electoral Infrastructure

(S//CEO) As the principal lead for cyber security threats to the election and electoral infrastructure, CSE's Canadian Centre for Cyber Security (CCCCS) did not observe any instances of cyber activity specifically targeting the Canadian electoral infrastructure. Cyber events that took place before and during the electoral period;

(U) Category 1 Definition: Malicious and deliberate attempt directed, subsidized or undertaken by (or on behalf of) a foreign state/actor to breach the information system of the election infrastructure. Election infrastructure includes, but not limited to: information technology systems that support the election processes; owners and operators of elections systems; individuals accountable for elections (e.g. election officials); and vendors of election system hardware and

3.2.2 (U) Category 2: Cybersecurity Threats against Political Parties and Government Officials

(U) Category 2 Definition: Malicious and deliberate attempt directed, subsidized or undertaken by (or on behalf of) a foreign state/actor to breach the information systems of Canadian political parties, government officials or electoral candidates.

(TS/[redacted]) [redacted]

3.2.3 (U) Category 3: Foreign Interference - Political

(S/[redacted]) Foreign interference targeting Canadian politicians and political parties was the second most common foreign interference activity observed by SITE TF. Within this category, the People's Republic of China (PRC) was the most active foreign state actor.

(TS/[redacted]/CEO) During the election period, [redacted]

(U) Category 3 Definition: Covert, deceptive or coercive activities directed, subsidized or undertaken by (or on behalf of) a foreign state/actor against Canadian government officials, political organizations or electoral candidates to affect electoral outcomes and/or undermine their policies, positions and opinions.

SITE TF AAR

Highest Classification:
TOP SECRET [redacted] CEO

[redacted]
[redacted]
(TS//CEO) [redacted] China was primarily interested in supporting political candidates whom they believed would reinforce China's overall strategic interests in Canada, regardless of party affiliation. [redacted] PRC officials likely manipulated one of the nomination contests in the Toronto riding of Don Valley North.

(TS//CEO) [redacted] These international students were reportedly bussed to the nomination vote [redacted]

PRC government supporters were possibly attempting to manipulate voting procedures to advantage their preferred candidate. While these [redacted] allegations remain unconfirmed, [redacted] advised relevant stakeholders in the GC of this report immediately in order to deter any possible activity from occurring.

(TS//CEO) To a lesser extent than China, [redacted] some indications of Indian interference operations in Canada. [redacted]

(TS//CEO) Pakistan [redacted] CSIS responded by initiating a Threat Reduction Measure (TRM) against Pakistan. [redacted]

[redacted] the TRM had a tangible effect [redacted]

3.2.4 (U) Category 4: Foreign Interference - Public

(U) Category 4 Definition: Covert, deceptive or coercive activities directed, subsidized or undertaken by (or on behalf of) a foreign state/actor aimed at the Canadian public and/or discrete populations (e.g. local diaspora) to affect electoral outcomes, sow societal discord, sway public sentiment within Canada to undermine public confidence in the electoral system and processes and/or support the national interests or agenda of the foreign state/actor.

(S// [redacted]) Foreign interference in the public domain was by far the most common foreign interference activity noted by SITE TF.

(TS//CEO) The PRC was assessed to be the most prominent actor in this space. China sought to realize its goals through engagement with regional Chinese diaspora community members. Acknowledging the pervasiveness of Chinese activity within Canada. [redacted]

(TS//CEO) [redacted]

SITE TF AAR

Highest Classification:
TOP SECRET [redacted] /CEO

(TS) [redacted] /CEO

(U) SITE TF did not observe broad-based foreign interference campaigns in the digital information ecosystem related to the election. SITE TF did note the publication of disinformation by foreign alternative information sources that in some instances were amplified by mainstream and social media. In one instance, the Buffalo Chronicle website published numerous salacious articles with a focus on Prime Minister Justin Trudeau. The Chronicle did not appear to publish this content to generate ad revenue and there were news reports that the Chronicle's US owner accepted payment in the past to publish negative articles about clients' political opponents. There was no indication of large-scale foreign, coordinated activity.

(U) SITE TF identified some coordinated and inauthentic activity on Twitter, involving accounts engaged in transnational discussions, which at times overlapped and included other transnational issues. Much of this showed limited significance in the larger election discourse and was likely not a part of a covert foreign interference campaign. Most high-profile stories spread due to public interest rather than foreign interference and any related inauthentic amplification. Domestic actors across the political spectrum were amplifying false narratives and spreading disinformation and misinformation, including domestically driven online discussions that likely involved inauthentic accounts and activity. Domestic actors fall outside of SITE TF's mandate, and therefore these instances were referred to GoC partners where appropriate.

3.2.5 (U) Category 5: Overt Influence

(U) Category 5 Definition: 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. The often overt and transparent nature of this activity will likely prompt alternative diplomacy response mechanisms.

(U) SITE TF did not focus on overt influence activities. The line between overt influence and covert influence is increasingly difficult to ascertain in the digital space, especially where state actors can use proxies and users can spread state propaganda wittingly or unwittingly. To help mitigate some of these activities, GAC had issued a diplomatic message requesting all foreign missions in Canada to refrain from such activities.

3.3 (U) Overall Threat Assessment

(S/[redacted]) SITE TF's initial assessment in the *Combined Threat Coverage Review* and forecast of the threat landscape remained valid before and during the electoral period. Over the course of its operations from September 2018 to October 2019, SITE TF saw no evidence to indicate that foreign state actors were specifically targeting Elections Canada (EC) or Canadian electoral systems and networks. The Task Force also saw no evidence of a broad-based foreign state-directed interference campaign in the digital information ecosystem, but notes that there were blind spots in SITE TF's ability to determine state attribution and distinguish between foreign and domestic disinformation campaigns. However, SITE TF did observe foreign interference activities targeting certain ridings and candidates in relation to the election, directed largely from China, and to a lesser extent from India and Pakistan, [redacted]. [redacted] SITE TF assessed that none of these foreign interference activities were part of a broad-based electoral interference campaign and did not have an impact on the overall outcome of the election. In addition, none of the activities met the threshold to pursue criminal investigations.

SITE TF AAR

Highest Classification:
TOP SECRET////CEO

4. (U) SITE TF LESSONS LEARNED

(U) In reflection of its mandate, SITE TF believed it had successfully fulfilled all parts of its mandate by: providing government partners a clear point of engagement; adjusting intelligence collection postures toward prioritized foreign interference threats; increasing government partners' situational awareness; and, promoting the use of intelligence with OGDs and/or taking action, when mandates permitted. This section captures critical elements that contributed to the success of SITE TF, as well as identifies challenges and areas for improvement. The information in this section is aimed at providing useful lessons learned for future SITE TF and other similar interdepartmental S&I efforts.

4.1 (U) Threat Analysis

4.1.1 (U) Detection of Interference Threats

(U) Scope and remit of activity

(U) The well-defined and narrow focus of SITE TF was a critical success factor. It provided the appropriate breadth and depth given Task Force's available resources. This focus also created a niche for SITE TF to operate in among broader government efforts related to foreign interference. Along with this focus was the clarity in SITE TF's mandate, which set out achievable objectives for the group.

(S//CEO) While SITE TF tried to be responsive and helpful to inquiries from government partners, the frequency of those inquiries and expectations of immediate responses were sometimes distracting for the Task Force. This could be particularly challenging when some inquiries were about ad-hoc one-time events and media headlines, which were not necessarily related to foreign interference threats to electoral processes. Some of these inquiries also had the potential to create the perception of partisanship when they were weighted towards issues affecting the government of the day. It was critical for SITE TF to maintain a level of independence that supports its non-partisan role and responsibilities in carrying out its activities.

(U) Refocusing collection assets and resources

(S//) SITE TF agencies were generally able to refocus collection assets and analytical resources to provide additional coverage on key targets of interest based on the assessment from the *Combined Threat Coverage Review*. This resulted in SITE TF's ability to generate relevant intelligence on potential foreign interference activities engaged by those key adversaries of concern.

Re-orienting collection assets and analytical resources to better understand and identify foreign interference activities can take a significant amount of time, This highlights the need for ongoing prioritization, as well as timely planning and coordination among the Task Force agencies.

(U) Limitations on access to data

(S//)

(S//) Detection of the "foreignness" in foreign interference is becoming increasingly difficult

SITE TF AAR

Highest Classification:
TOP SECRET//CEO

(S/ [redacted])
 [redacted] To overcome this challenge, GAC began a collaboration with [redacted]
 [redacted] A technical limitation for SITE TF was the limited capacity of existing commercial and non-commercial social media analytical tools. [redacted]

4.1.2 (U) Assessment of Interference Threats

(U) Multidisciplinary teaming

(U) SITE TF functioned well as a joint practitioner group, leveraging each agency's mandates and engaging in a collective decision-making process to detect and assess threats. The Tech Table was a successful joint analytical unit, where analysts with different skillsets and experiences worked together to evaluate complex and technical data that provided analytical conclusions for overall SITE TF response.

(S/ [redacted]) At the same time, differences in methodologies, and nuances of different data sources made joint assessments of intelligence challenging. Each SITE TF agency has its own distinct analytical approaches, assessment terminologies and attribution thresholds. These differences generated delays in creating joint assessment products [redacted] Greater efforts should be made to understand the distinct analytical cultures of each SITE TF agency and to develop common analytical standards, assessment language and attribution thresholds for future joint assessment products.

(U) Defining and Understanding the Threat Landscape

(U) The use of a categorization system, as prescribed in the *Bulletin on Understanding Malign Foreign Influence*, was an effective tool to understand and triage the broad range of foreign interference activities. These categories helped SITE TF members understand the scope of activities observed and identify the appropriate lead agency to follow up on issues. The *Bulletin* was also useful in communicating threat activities to government partners. SITE TF should continue to use the threat categorization system and further refine those categories to reflect the evolving nature of foreign interference threats.

(S/ [redacted]) Initial SITE TF efforts concentrated on understanding the existing threat landscape, and ultimately, SITE TF was focused on the right key threats (i.e. PRC and Russia). However, the *Threat Coverage Review* could have been completed sooner; an earlier review would have assisted in steering collection efforts on other gaps [redacted] and in building a better understanding of the issue of foreign interference for analysts not normally familiar with the issue.

(S/ [redacted]) In addition to the *Combined Threat Coverage Review*, a more comprehensive review of areas vulnerable to foreign interference would be beneficial. [redacted]

(U) Limitations

(U) It is difficult, if not impossible, to assess the impact of most foreign interference activities on elections given the opacity and complexity of voter behaviour. This is especially the case in the digital information ecosystem.

SITE TF AAR

Highest Classification:
TOP SECRET//[redacted]/CEO

(U) It is also important to keep in mind that assessment and attribution take time. Further, intelligence indicating a foreign interference campaign has occurred may only surface many months after the end of the election.

(S) [redacted]

4.2 (U) SITE TF Response Posture

4.2.1 (U) Responding to Threats

(U) Process and Planning

(S) [redacted] The *SITE TF Playbook and Response Options Matrix* were useful references in outlining the range of possible responses by different agencies under the various categories of threat activities. The *Matrix*, in particular, was helpful in communicating SITE TF's response capabilities and mandates to other government partners. The *Matrix* should be maintained with adjustments made accordingly to the evolving threat landscape and participating agencies' mandates and capabilities.

(U) TTXs exercised by SITE TF helped clarify SITE TF members' respective mandates and authorities, as well as identified potential roadblocks and chokepoints that would hamper the Task Force's ability to respond to various foreign threat scenarios in a timely manner.

(U) Establishing thresholds for off-hours action, and engagement with 24/7 watch offices on standard operating procedures, on-call lists, and surge postures were crucial in ensuring that SITE TF members were alerted to critical foreign interference incidents related to the election at all times.

(S//CEO) SITE TF leveraged the established processes and standard operating procedures of Task Force members as much as possible without reinventing new protocols that would complicate and delay threat response times. An example was the OneVision operational deconfliction protocol already in use by RCMP and CSIS.

(S//CEO) With proactive planning and preparation, CSIS was able to activate [redacted] TRMs in effect [redacted] and Pakistan to prevent foreign interference activities against Canada's federal election. [redacted]

(U) Limitations

(S//CEO) CSE's processes for sanitization and action-on of SIGINT information were not always conducted in a timely manner, therefore delaying the ability for SITE TF to share and act upon useful SIGINT information with other partners in a more timely fashion. These processes need to be revamped to minimize the response and approval times.

(S//CEO) Although the CSE Act and Ministerial Authorizations for active and defensive cyber operations did not come into effect until late summer 2019, CSE had spent many months in advance consulting with stakeholders, drafting operational plans and procedures, conducting internal TTXs on foreign interference scenarios to optimize CSE's operational readiness. Planning and capability building in this domain can take time and needed to be carried out well in advance of an election.

4.3 (U) Engagement and Communications

4.3.1 (U) Internal SITE TF Engagement

SITE TF AAR

Highest Classification:
TOP SECRET//CEO

(U) SITE TF's weekly internal meetings were of appropriate frequency, which allowed the group to identify, discuss and respond to issues on a timely and coordinated manner. Through these regular meetings, SITE TF members established rapport, built confidence, created a collaborative environment where information was shared openly and differences in opinions were challenged in respectful and constructive ways.

(S//CEO) CSIS regular dissemination processes for what were, in most instances their CSIS Intelligence Reports (CIRs), inadvertently resulted in only SITE TF principal members and their DMs receiving the reporting. This limited the discussion that could take place at the SITE TF table and, in some cases, within partner agencies. When the challenge was identified to CSIS representatives, responses were taken to alleviate dissemination issues. Going forward, CSIS dissemination procedures will be reviewed in this area so that SITE TF agencies are fully informed.

(S//) Managing communications on both secure and unclassified platforms was challenging from both technical and physical perspectives. Some SITE TF agencies were reliant on the Canadian Top Secret Network (CTSN) for daily operational work and communications. This presented some inconveniences for agencies who did not have readily available access to the system. Attempts were made to use CSE-hosted secure information sharing platform, but not all SITE TF agencies had access to the platform.

Furthermore, CSE encountered numerous technical difficulties with setting up and maintaining distribution lists, particularly on the unclassified system. On a positive note, CTSN phones were installed efficiently at SITE TF agencies that needed them in time for the daily operational calls during writ period.

4.3.2 (U) Engagement with Other Government Departments

(U) Clear and frequent communications with senior government officials (i.e. ADMs, DMs, Panel of Five) during the writ period was crucial in providing reassurance and a common and timely understanding of the threat picture.

(S//CEO) CSE's 'hotline' provided a single entry point for Cabinet Ministers and political parties to confidently communicate with the S&I community, and allowed SITE TF agencies to coordinate and triage incoming information more efficiently.

(S//CEO) Engagement with entities beyond SITE TF and traditional S&I partners was highly valuable, but also presented certain risks. There were several instances of classified information appearing in media reporting, leading to concerns amongst SITE TF over whether the security of the information was well understood and respected by entities who had been briefed on SITE TF activities.

(S//CEO) The frequency of briefing to OGDs was sometimes challenging for SITE TF members who were carrying the duties and responsibilities of both their regular day jobs as well as SITE TF.

(S//CEO) Engagement with stakeholders at EC and the CCE was particularly useful. While engagement with PCO SI was strong, SITE TF could have done better to establish closer ties with other elements of PCO (e.g. DI, Tiger Team, IAS).

4.3.3 (U) Engagement with Political Parties

(S//REL TO FVEY) Engagement with SECRET-cleared representatives of political parties bolstered the relationship with S&I agencies and instilled confidence that SITE TF agencies were prepared to work collaboratively to safeguard the electoral process. Many party representatives were appreciative of this engagement, which had allowed them to stay better informed of potential threats and to understand the range of government support available to help address those threats. SITE TF noted that ongoing engagement with political parties and other government partners,

SITE TF AAR

Highest Classification:
TOP SECRET [redacted] /CEO

outside of election periods, could be beneficial in strengthening the government's collective ability to recognize, mitigate and defend against potential foreign interference threats.

4.3.4 (U) Engagement with Social Media

(S/[redacted]) SITE TF's engagement with social media companies [redacted] was helpful [redacted] and facilitating dialogue with the S&I community. However, more time and effort would be required to build trust and further these relationships. [redacted]

[redacted] There is a need to build stronger and longer-term relationships, not limited to just electoral periods, with social media companies to foster trust and support future cooperation.

(S/[redacted]) Social media companies, such as Twitter and Facebook, were reluctant to share additional data [redacted] in absence of a formal legal process (i.e. warrants). [redacted]

[redacted] SITE TF recognized the need for an appropriate and efficient legal process to obtain relevant data from social media companies.

(S//CEO) Documentation and sharing of information received during meetings with social media needs to improve due to the precision and accuracy required for using it in assessments and reporting.

4.3.5 (U) Engagement with Traditional Media

(S//CEO) PCO took the lead on coordinating the communication of messages to the media throughout the 2019 election period. This created a clear and efficient delineation of responsibility, and enabled SITE TF and the GoC to speak with one voice. However, there was an over reliance on a single set of talking points, agreed to before the election period, which resulted in a lack of nuanced messaging that actually addressed the media's questions or allowed SITE TF to tell its story. A more nuanced approach to public messaging, and a greater willingness to share more information will help the public better understand both the relevant threats and the government's response to those threats. An informed public is the best line of defence against foreign interference.

(S//CEO) Opinion differs among SITE TF over the future of communications. The majority are happy to continue with the PCO protocol, but there is a recommendation for SITE TF to begin engaging the public and media directly with the goal of educating them on foreign interference threats and how the GoC counters them.

(S/[redacted]) SITE TF needs to engage communications elements in a coordinated fashion much earlier (i.e. to establish a strategic communications plan early, delineate how to engage the public and media, and prepare lines for media for consistency across SITE TF agencies and to avoid rushed responses upon tight deadlines, etc.).

4.3.6 (U) Engagement with Non-Government Experts

(S/[redacted]) There is a need to establish clear protocols for better leveraging the expertise and insights of non-government experts engaged in identifying foreign interference and debunking disinformation. This could involve contracts or information sharing agreements, whereby SITE TF partners share data, including publicly available account information as appropriate, with non-government partners for the purpose of identifying possible foreign interference and communicating findings with the public.

4.3.7 (U) Engagement with International Partners

SITE TF AAR

Highest Classification:
TOP SECRET//[REDACTED]/CEO

(U) Engagement with international partners provided useful lessons on the processes, successes and challenges from their electoral security frameworks, as well as information related to foreign threat actors and capabilities.

(U) Engagements with partners on matters of foreign interference need to be persistent – including outside of election cycles – as the toolkits and capabilities of both adversaries and allies continue to evolve. Collaboration and partnerships are a key strength and imperative to countering foreign interference.

4.4 (U) A Final Take-Away

(S//[REDACTED]) Overall, a key concern was the observation by SITE TF of long-term and often non-distinct activities (such as ongoing diaspora community influence activities and challenges to *Canadian Charter*-based rights) that did not constitute electoral interference but were highly concerning. Such activities impacted a wide area of Canadian democratic freedoms and processes, and therefore constitute threats to Canadian democratic institutions. [REDACTED]

[REDACTED] Identifying and finding the appropriate mechanisms to mitigate against such activities may require further analysis by SITE TF. This will include how intelligence can be shared with the right agencies, what proposals for action should be considered, and how to address policy gaps exploited through foreign interference activities.

4.5 (U) Future of SITE

Foreign Interference in Canada is a persistent threat that exists beyond election cycles. Members agree that SITE TF's work on combatting foreign interference needs to continue, taking advantage of the momentum gathered to build and improve upon the processes and relationships established. It is important to guard to highlight the principles that made SITE TF successful, including:

- clear mission and focus
- clear work plan and objectives
- core group of practitioners and regular engagement
- open and forward-leaning approach to sharing by contributing members secretarial/administrative support.

SITE TF AAR

Highest Classification:
TOP SECRET//[REDACTED]/CEO**5. (U) ANNEX**

5.1 (U) Glossary

A	AAR	after action report
	ADM	assistant deputy minister
C	CCCS	Canadian Centre for Cyber Security
	CCE	Commissioner of Canada Elections
	CSE	Communications Security Establishment
	CIR	Canadian Security Intelligence Service Intelligence Report
	CSIS	Canadian Security Intelligence Service
	CTSN	Canadian Top Secret Network
D	DM	deputy minister
E	EC	Elections Canada
	EU	European Union
F	FSB	Russian Federal Security Bureau
G	GAC	Global Affairs Canada
	GCHQ	Government Communications Headquarters
	GoC	Government of Canada
	GRU	Russian General Staff Main Intelligence Directorate
H	HASA	Hostile Activities of State Actors
	HUMINT	human intelligence
M	MP	Member of Parliament
O	OGD	other government department
P	Panel of Five	Critical Election Incident Public Protocol Panel
	PCO	Privy Council Office
	PCO DI	Privy Council Office's Democratic Institutions
	PCO IAS	Privy Council Office's Intelligence Assessment Secretariat
	PCO SI	Privy Council Office's Security and Intelligence Secretariat
	PRC	People's Republic of China
R	RCMP	Royal Canadian Mounted Police
	RoD	record of discussion
	RRM	Rapid Response Mechanism
S	S&I	security and intelligence
	SIGINT	signals intelligence
	SITE TF	Security and Intelligence Threats to Elections Task Force
	SITREP	situation report
	SSEUR	SIGINT Seniors Europe
T	TRM	threat reduction measure
	TTX	tabletop exercise
U	UFWD	United Front Work Department
	UK	United Kingdom
	US	United States

SITE TF AAR

Highest Classification:
TOP SECRET//CEO

5.2 (U) SITE TF Terms of Reference

(U) Leading up to Canada's 2019 Federal Election, a security and intelligence community task force has been created to improve situational awareness of the threat landscape related to foreign interference in Canada's electoral process, and to coordinate across Government to facilitate coverage and engagement of those threats.

(U) Mandate

- To provide a clear point of engagement with the security and intelligence community for Government partners engaged in related work.
- To review and focus intelligence collection, assessment, and open-source analytics related to foreign interference of Canada's democratic process in a coordinated manner.
- To provide situational awareness for Government partners, senior public servants, and Cabinet.
- To 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.

(U) Membership

(U) Operational-Level Forum

- Communications Security Establishment
- Canadian Security Intelligence Service
- Global Affairs Canada
- Royal Canadian Mounted Police

(U) Senior Level Forum

(U) Chair:

- Deputy Chief SIGINT of the Communications Security Establishment

(U) Members:

- Deputy Director of Operations of the Canadian Security Intelligence Service
- Assistant Deputy Minister International Security of Global Affairs Canada
- Assistant Commissioner Federal Policing Operations of the Royal Canadian Mounted Police

(U) Members may appoint delegates and additional executive participants within their agency/department as appropriate. Where appropriate, additional Government partners will be invited to participate.

SITE TF AAR

Highest Classification:
TOP SECRET [redacted] CEO

5.3 (U) Detailed Threat Assessment

(U) Category 1: Cybersecurity Threats against Electoral Infrastructure

(U) The *CCCS 2019 Update: Cyber Threats to Canada's Democratic Processes*, noted four key trends from recent global cyber threat activity against democratic processes:

- Cyber threat activity against democratic processes is increasing worldwide.
- Cyber threat activity against democratic processes increasingly targets voters.
- Cyber threat activity persists against political parties, candidates and their staff.
- Elections continue to be targeted by cyber threat activity, though less frequently than voters, political parties, candidates and their staff.

(S//CEO) Ahead of the elections, SITE TF assessed that the threat landscape in Canada would remain consistent with previous patterns and behaviours (including those above).

(S//CEO) As the principal lead for cyber security threats to the election and electoral infrastructure, CCCS did not observe any instances of cyber activity specifically targeting the Canadian electoral infrastructure. However, a wide range of cyber events took place before and during the elections; this was inline with expected activity. Overall, from 30 September 2018 through to the end of the election, CCCS [redacted] systems blocked 2,424 requests for compromised websites, stopped over 7,000,000 port scans and software vulnerability probes, while analysts triaged over 37,800 network security alerts. While they are too many to list in this report, a sampling of these events is offered below:

(PROTECTED B) [redacted] an EC website outage was reported to CCCS. Upon further investigation, it was discovered that an element of new infrastructure was configured in a way that interfered with Dynamic Defence, causing intermittent web site outages. A solution was put in place and validated by CCCS.

(PROTECTED B) [redacted]

(TS [redacted] /CEO) [redacted] EC contacted CCCS' cyber incident response team regarding [redacted]

(TS [redacted] /CEO) [redacted] CCCS identified activity that was associated with PRC cyber activity targeting [redacted] GoC departments. The observed activity [redacted] and there was no clear nexus to democratic interference.

(PROTECTED B) [redacted] the EC security team requested CCCS [redacted] CCCS analysis determined the IPs were associated with ADware.

SITE TF AAR

Highest Classification:
TOP SECRET [redacted] /CEO

(PROTECTED B) [redacted] EC experienced a passive sensor outage. Technical staff made unforeseen cabling changes to a core switch during a routine router upgrade. CCCS engaged and provided full support until the issue was resolved.

(PROTECTED B) [redacted] EC received multiple repurposed email messages containing a malicious attachment. Suspected emails were successfully quarantined and no compromise was detected. CCCS worked with EC to implement protective measures.

(PROTECTED B) [redacted] EC reported increased traffic to an EC website designed for internal use only. No malicious activity or compromise was observed. The webpage inadvertently exposed an internal hostname and IP for an unspecified amount of time.

(U) Category 2: Cybersecurity Threats against Political Parties and Government Officials

(S//REL TO FVEY) State actors such as China and Russia use cyber capabilities as a means of advancing their strategic objectives. These operations are persistent, typically geared towards intelligence collection (rather than disruption) and focus on traditional targets, such as government ministries, high-tech industry and other entities of strategic importance. In short, they are active all the time across a range of interests. While key adversaries such as China and Russia remained active throughout the period of September 2018 to October 2019, SITE TF observed a limited amount of activity directed at political parties and government officials.

(TS) [redacted] PRC cyber activity targeting senior government officials

(TS//SI//REL TO FVEY) [redacted] provided lead information to CSE on PRC [redacted] linked cyber actors. [redacted] CSE detected further instances of this activity, and issued additional reporting [redacted]

(TS [redacted] /CEO) CCCS [redacted] through established channels to provide advice and guidance on the issue to the Parliamentary Protective Services and House of Commons staff. CCCS also provided advice and guidance related to this activity to the department security officers across government, and developed and delivered an information package including email security practises and specific indicators to watch out for related to this campaign to DMs across the GoC.

(TS) [redacted] Follow-on CSE analysis and [redacted]

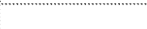

(S) [redacted] Russian cyber activity targeting Canadian interests







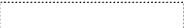
(TS [redacted] /CEO) [redacted] cyber actors from the Russian [redacted] containing contact information for a [redacted]


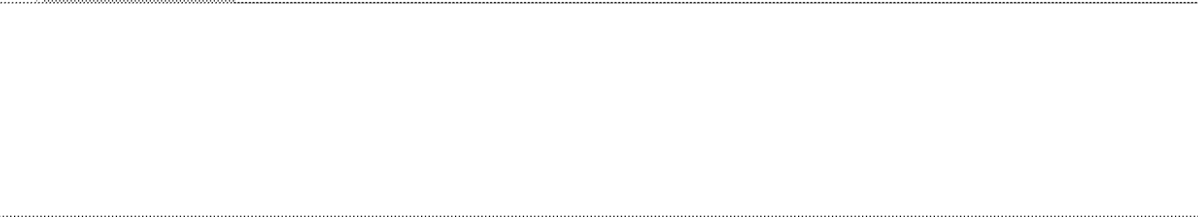
[redacted] At the time of reporting, CSE could not confirm the specific intent of this activity. It is not uncommon for [redacted] to target government entities as part of their standard intelligence-gathering operations.

SITE TF AAR

Highest Classification:
TOP SECRET////CEO

(S)  While Russian and Chinese cyber activity specifically targeting Canada was not frequent, general cyber activities targeting  remained active throughout the period. The following are some examples of Russian cyber activities not specifically targeting Canada that SITE TF monitored:

(TS/   cyber actors conducting extensive open source research on numerous  entities, such as the  Central Election Committee, the  and websites related to  statistics, data and electoral information. This formed part of a general increase in such activity observed by CSE from the beginning of 

(TS)  


(TS)  


(TS)  


(U) Category 3: Foreign Interference - Political

(S//CEO) China's Foreign Interference in the 2019 Federal Election:
The 2015 Canadian Federal Election Setting

(TS// CEO) 


SITE TF AAR

Highest Classification:
TOP SECRET////CEO

(TS//CEO)

[Redacted]

(S//CEO) PRC Approach to Foreign Interference in Canadian Politics 2019

(TS//CEO)

[Redacted]

(TS//CEO)

[Redacted] a mixed picture emerged of the PRC's preferred outcome in the 2019 election.

PRC officials to continue to utilize a 'hedging strategy' across Canadian political party lines. This involved a strategy of pragmatism and adaptation: picking potential political winners in Canadian politics, and seeing if they could be developed by PRC officials over time in PRC influenced social and business-based networks.

[Redacted]

The PRC's pragmatic approach to Canadian political parties remained anchored in ensuring the ability to improve PRC influence and representation in Canadian politics and economic affairs.

(TS//CEO)

[Redacted]

This approach was consistent with the PRC interfering with Canadian officials at all levels of the GC, whereby PRC officials attempt to place and groom preferred supporters at municipal levels of government

[Redacted]

(TS//CEO) In terms of the method of direction, PRC officials in the past have been adept at using WeChat to influence Chinese-Canadian citizens through closed communications platforms. However, this strategy was exposed following a media story on vote-buying during the B.C. municipal elections in October 2018 surrounding allegations of PRC official's interference activities.

[Redacted]

SITE TF AAR

Highest Classification:
TOP SECRET/[redacted]/CEO

[redacted]

(TS//CEO)

[redacted]

(TS//CEO)

[redacted]

(TS//CEO) CSIS Response to Potential PRC Interference Efforts

(TS//CEO)

[redacted]

(S//CEO) Key PRC Interference Activity

(TS//CEO) During the 2019 Federal election, [redacted] foreign interference activities were likely being directed by PRC officials at a prominent riding in the Toronto area, Don Valley North, [redacted]

[redacted]

SITE TF AAR

Highest Classification:
TOP SECRET/[redacted]/CEO

[redacted]

(TS//CEO)

[redacted]

(TS//CEO)

[redacted]

(TS//CEO)

[redacted]

(TS//CEO)

[redacted]

[redacted]; PRC foreign interference efforts and established tradecraft do appear consistent in key Canadian political areas in which PRC co-optees have leverage in community affairs. These foreign interference efforts are becoming increasingly embedded in community-based networks that link federal, provincial, and municipal politics in key Canadian cities [redacted]. Such socio-political networks are potential tools of leverage against Canadian political officials through the growing economic relationships and interdependence being built in Chinese-Canadian communities with PRC officials and their co-optees.

(TS//CEO) India's Foreign Interference in the 2019 Federal Election:

(TS//CEO)

[redacted]

SITE TF AAR

Highest Classification:
TOP SECRET///CEO

[Redacted]

(TS//CEO)

[Redacted]

(TS//CEO)

[Redacted]

(TS//CEO)

[Redacted]

(TS//CEO)

[Redacted]

(TS//CEO)

[Redacted]

(TS//CEO)

[Redacted]

SITE TF AAR

Highest Classification:
TOP SECRET [redacted] /CEO

[redacted]

(S//CEO) Pakistan's Foreign Interference in the 2019 Federal Election:

(TS//CEO)

[redacted]

(TS//CEO)

[redacted]

(TS//CEO)

[redacted]

(S//CEO) Russia's Foreign Interference in the 2019 Federal Election:

(TS//CEO) Given that Russia globally is a significant foreign interference threat actor with particular focus on attempting to undermine Western democratic institutions, it was assessed that Canada's electoral processes would be targeted in 2019 if Russia saw disruption and interference as strategically beneficial.

[redacted]

(TS//CEO) However, Russian activity against Canada's 2019 election and Canadian democratic institutions was minimal.

[redacted]

SITE TF AAR

Highest Classification:
TOP SECRET/[redacted]/CEO

[redacted]

(TS//CEO) [redacted] Canada's election was not a priority target for Russia, [redacted] No Russian cyber activity specifically targeting Canadian electoral infrastructure during the Federal election was observed.

[redacted]

(TS//CEO)

[redacted]

(S//CEO)

[redacted]

(TS//CEO)

[redacted]

(TS//CEO)

[redacted]

(TS//CEO)

[redacted]

[U] Category 4: Foreign Interference - Public

(U) RRM Canada began evaluating the Canadian digital information ecosystem a year prior to the 2019 Federal Election, based on research and lessons learned from recent elections in other democracies, in order to establish a baseline for the identification of anomalies indicative of foreign interference. Using this baseline, RRM Canada was able to triage anomalies as new subjects and trends emerged in the lead-up to the election. Signalling these anomalies at SITE TF functioned as an early warning mechanism. Regular baseline assessments also allowed RRM Canada analysts to better

SITE TF AAR

Highest Classification:
TOP SECRET//[REDACTED]/CEO

Understand the origins and nature of disinformation and evaluate alleged foreign interference reporting generated by the media and academia during the election.

(U) RRM Canada also tested and refined its methodological approaches by monitoring the Alberta and Manitoba provincial elections and by actively identifying issues and events potentially susceptible to foreign interference in consultation with other government departments and non-government experts. While RRM Canada anticipated foreign interference activity in the digital information ecosystem, the analysts were cognisant that the election took place in a highly charged geopolitical context that likely deflected potential foreign interest elsewhere, including protest movements in Hong Kong and Russia, tensions between Iran and Saudi Arabia, the conflict in Syria, and considerable focus on impeachment and Brexit debates in the US and UK respectively.

(U) RRM Canada did not observe any broad-based foreign interference campaigns in the digital information ecosystem related to the election.

(U) RRM Canada noted the publication of disinformation by foreign alternative information sources that in some instances were amplified by mainstream and social media. For example, numerous salacious publications were identified, in particular about Prime Minister Justin Trudeau, on the Buffalo Chronicle website. These publications might have been designed to influence public perceptions in the context of the election. The Buffalo Chronicle did not appear to publish content about Canada for the purpose of generating ad revenue (i.e. clicking on the content does not steer the reader to ads), and there were unconfirmed reports that the Chronicle's US owner accepted payment in the past to publish negative articles about clients' political opponents. The publications were shared online, garnering a minimum of 279,500 social media engagements. However, RRM Canada found no indication of large-scale foreign, coordinated activity in the dissemination of these stories. Alternative and mainstream information sources cited some of these stories, while other actors, including Canadaland, Agence-France Press, and Snopes, debunked them. As RRM Canada could not conclusively establish whether foreign state actors were involved in the publication and dissemination of the stories, investigations concluded after findings were shared with SITE TF.

(U) RRM Canada noted some coordinated and inauthentic activity on Twitter involving accounts engaged in transnational discussions. For example, inauthentic and coordinated activity with respect to #Trudeaucorruption involved accounts who also engaged in transnational discussions on various topics. However, the hashtag only trended for five days with limited reach. There was also coordinated but likely authentic activity with respect to #Trudeaumustgo. As noted by a Middle East-based, UK professor in the media, a number of the active users of the hashtag had the acronym "MAGA" in their profiles — for "Make America Great Again", the slogan of Donald Trump's 2016 presidential campaign — as well as other related hashtags and indicators. RRM Canada and its trusted partners assess this is likely a result of authentic cross-border discourse and not a coordinated and covert foreign interference campaign.

(U) Domestic actors across the political spectrum were amplifying false narratives and spreading disinformation and misinformation. RRM Canada identified domestically driven online discussions that likely involved inauthentic accounts and activity. Domestic actors fall outside RRM Canada's mandate, and therefore these instances were referred to GoC partners where appropriate.

(U) A number of actors engaged in fact-checking, independent analysis and reporting in order to combat disinformation. One consequence of this is that actors, at times, both knowingly and unknowingly, amplified false and misleading content through their efforts, giving more prominence to false narratives. Discussion, reporting and awareness of disinformation created a greater focus on the issue, and led to an increase in ongoing discussion about the potential cases of disinformation during the election, as compared to previous elections. These examples represent in part the complex and nuanced nature of the digital information space surrounding the Canadian election, and the potential vulnerabilities and incidents warranting closer examination for foreign interference.

SITE TF AAR

Highest Classification:
TOP SECRET, [REDACTED]//CEO

(U) Most high-profile stories largely spread due to public interest rather than foreign interference and related inauthentic amplification. For example, RRM Canada assesses that the black/brown face scandal was the lead story on multiple international news outlets as a result of organic activity versus artificial amplification.

(U) In some instance, organic discussions originating outside the Canadian public discourse in foreign contexts touched on Canadian political issues, e.g., the US Democratic Primary debate on immigration amplified a story from February 2018 about PM Trudeau's willingness to accept refugees and immigrants. This resulted in an organic spike in online discussion with respect to PM Trudeau, which was unrelated to the Canadian election context.

(U) Known foreign propaganda outlets (e.g., RT, Sputnik, sites associated with the FAN network) posted stories about the Canadian election but did not conduct sustained campaigns.

(U) Category 5: Overt Influence

(U) While SITE TF efforts did not focus on overt influence activities, during the course of our activities no specific instances of overt influence activities were observed. However, the line between overt influence and covert influence is increasingly difficult to ascertain in the digital space, especially where state actors can use proxies and users can spread state propaganda wittingly or unwittingly. To help mitigate some of these activities, GAC had issued a diplomatic message requesting all foreign missions in Canada to refrain from such activities.