

For Public Release

v. 2019 06 18 TOP SECRET Canadian Eyes Only (with attachments)

Critical Election Incident Public Protocol Panel - Meeting Two

80 Wellington, Ottawa, Ontario
June 20, 2019
8:30 am to 11:30 am

ATTENDEES:

PANEL

Ian Shugart PCO
~~Greta Bossenmaier PCO~~
Natalie Drouin JUSTICE
Marta Morgan GAC
Gina Wilson PS

Invitees

Ian McCowanPCO
Catherine BlewettPCO
Al SutherlandPCO
~~Caroline XavierPCO~~
Alia Tayyeb (Secretary)PCO
Shelly Bruce CSE
David VigneaultCSIS
Brenda LuckiRCMP
Tara DenhamGAC

GOALS:

- Introduction and Updates
- Table Top Exercises and Threshold Discussion
- Threat Briefing

AGENDA:

8:30 am Introduction and Update (PCO)

- Introduction - Clerk
- Debrief of Recent Activities
 - Protocol, Political Parties (Ian McCowan)
 - National Security Briefings (Alia Tayyeb)

9:00 am Table Top Exercise

10:00 am Discussion and Reflection on Exercise:

- Identify Threshold Questions
- Identify Gaps

10:30 am Threat Briefing (CSE, CSIS, GAC)

- Baseline Overview and Trend Briefing

Meeting Adjournment (Clerk)
Recap of any items to bring forward for next meeting

Documents:

TAB A Record of Discussion May 31, 2019
TAB B CSE Cyber Security Guide for Campaign Teams

Exercise - Provided at meeting
TAB C Incident Response Architecture
TAB D Global Case Studies

TAB E Primer: Anticipating Foreign Threats to Canada's 2019 Election
TAB F Examples of Recent CSIS Reporting
TAB G GAC RRM Reporting

This is overview of previous TTXs.

extra copy?
TS// [] CEO

Overview of Panel of 5 TTX

- The P5 TTX will be one already exercised at the DG/ADM Electoral Security tables
- The TTX will focus either on a cyber scenario or a foreign interference scenario. Regardless of the scenario, "the Panel will be provided with the actions taken by their organizations and will only be required to weigh in with respect to the role of the Panel" and whether the incident meets the threshold for them to deliberate, whether or not they advise the PM/political parties, and whether a public statement should be made. Ultimately the scenario will be geared towards the exercise of the Critical Election Incident Public Protocol
- Below, you will find information on all SITE TF, SONOROUS and community TTXs to date.

SITE TF TTX's to Date

March 26th, 2019:

- Participants included SITE TF representatives from CSIS and CSE
- The TTX focused on three scenarios: Criminal, Hostile State Actor – [] and Hostile State Actor – China
- **Criminal scenario:** based on CSE reporting into a Ukraine-based individual observed establishing fraudulent news sites appearing to originate within Quebec, and sharing their content across social media
 - o CSE: []
 - o CSIS: discussed the utilization of the [] to develop further intelligence, and possible collaboration with CSE's []
 - o Issues: []
- **Hostile State Actor []** based on a situation in which [] using bots/trolls to promote one Canadian political party over another on social media
 - o CSE: []
 - o CSIS: discussed [] ability to evaluate the activity as well as potential engagement with social media platforms when there is suspicion of inauthentic accounts
 - o Issues: []
- **Hostile State Actor – China:** based on a situation in which China uses closed social media groups (WeChat) in Canada to influence the Canadian electorate

For Public Release

TS// //CEO

- o CSE:
 - o
-

June 26th, 2019:

- Participants will include all SITE TF members
- TTX to focus on 7 different scenarios, specifically:
 1. The National Register of Electors server was hacked and voter information was stolen by possible foreign organized crime entity sold on various e-Crime sites. State-sponsored cyber actors are likely to use the information for attack campaigns
 2. APT29 leaking disclosures of sensitive Canadian information of a Canadian electoral candidate via a successful phishing campaign
 3. state actor using bots/trolls to promote one Canadian political party over another on social media
 4. Ukraine-based actor seeding particular new stories on fraudulent news platform appearing to originate from Canada
 5. China uses closed social media networks (WeChat) in Canada to influence Canadian electorate
 6. A Russian in Canada using Twitter to create noise and confusion on a controversial Canadian political issue key to the Canadian federal election in an attempt to sway voter's opinions
 7. Elections Canada electronic information or information infrastructure is threatened by a foreign cyber operation for which existing defenses on the victim system prove inadequate to mitigate

SONOROUS TTX's to Date**April 25th, 2019:**

- **Malware scenario:** The scenario involved Host Based Sensor (HBS) tradecraft alerting Cyber Centre analysts to an unknown and unsigned piece of software moving laterally through the Elections Canada network.
 - o Key findings include:
 - Participants came away with a better understanding of roles and responsibilities, communications channels and information sharing – but there is still more work to do in this space based on the wide spectrum of stakeholders involved

For Public Release

TS// //CEO

- External communications need to be engaged early and often for visibility into potentially high-profile issues
- Communications and information flow can continue to be improved – these processes are being formalized via joint Concept of Operations with Elections Canada, an internal Cyber Centre Elections Playbook, etc.
- Consolidating the flow of information through SONOROUS for any updates is critical; this message was reinforced through the exercise and with the After Action Report

May 30th, 2019:

- **Person in the Middle scenario:** The scenario involved a Person in the Middle attack in which an Elections Canada website redirects visitors to a malicious foreign domain where personal identifying information is collected.
 - Key findings included:
 - There were conflicting outreach strategies for engagement with political parties from various CSE and GC groups – this process has been addressed following break-out discussions after the exercise.
 - Processes and procedures for the Contact Centre Hotline are being finalized and were thus unable to be fully tested in time for this exercise – Event SONOROUS is planning to continue testing these processes during the final exercise.
 - Information sharing and classification needs to be done at the lowest possible level to ensure stakeholders at the various sites, including off-site Cyber Centre personnel, are receiving critical information and not operating independently. This will be mitigated via classified and unclassified chatrooms that will be operating during the surge, and the expected availability of a


July 11th, 2019:

- **DDoS Scenario:** The exercise will involve a Distributed Denial of Service (DDoS) attack against a likely Elections Canada website. The exercise design team is planning to also test the Contact Centre (Hotline) and a Democratic Institution scenario for C-59 authorities.

DMNS TTX**September 2018:**

- DMs participated in a TTX that took into consideration the various threats from Hostile State Activity. The exercise was intended to clarify roles and responsibilities and ensure sound incident response. The TTX included scenarios cascaded from the pre-election period, to the pre-writ period, and then late into the writ period. The exercise involved multiple “targets” and Canadian sovereignty and security more generally.

For Public Release

TS///CEO**Electoral Security Steering Committee (ESSC) TTXs****April 11, 2019:**

- Included DG ESSC, and an ADM debrief
- Focused on cyber security with spear phishing exploiting an EC network

May 7th, 2019:

- Included DM ESSC, P5
- Focused on cyber security with spear phishing exploiting EC network

June 2019:

- Included ADM ESSC, and an DM ESSC debrief
- Focused on terrorist attacks against voting stations

June 2019:

- Includes ADM ESSC, DM ESSC, and P5
- Focusing on sensitive foreign interference

July 2019:

- Includes ADM ESSC, DM ESSC and P5
- Focus on D&PC

July 2019:

- Includes political parties
- Focus on cyber security

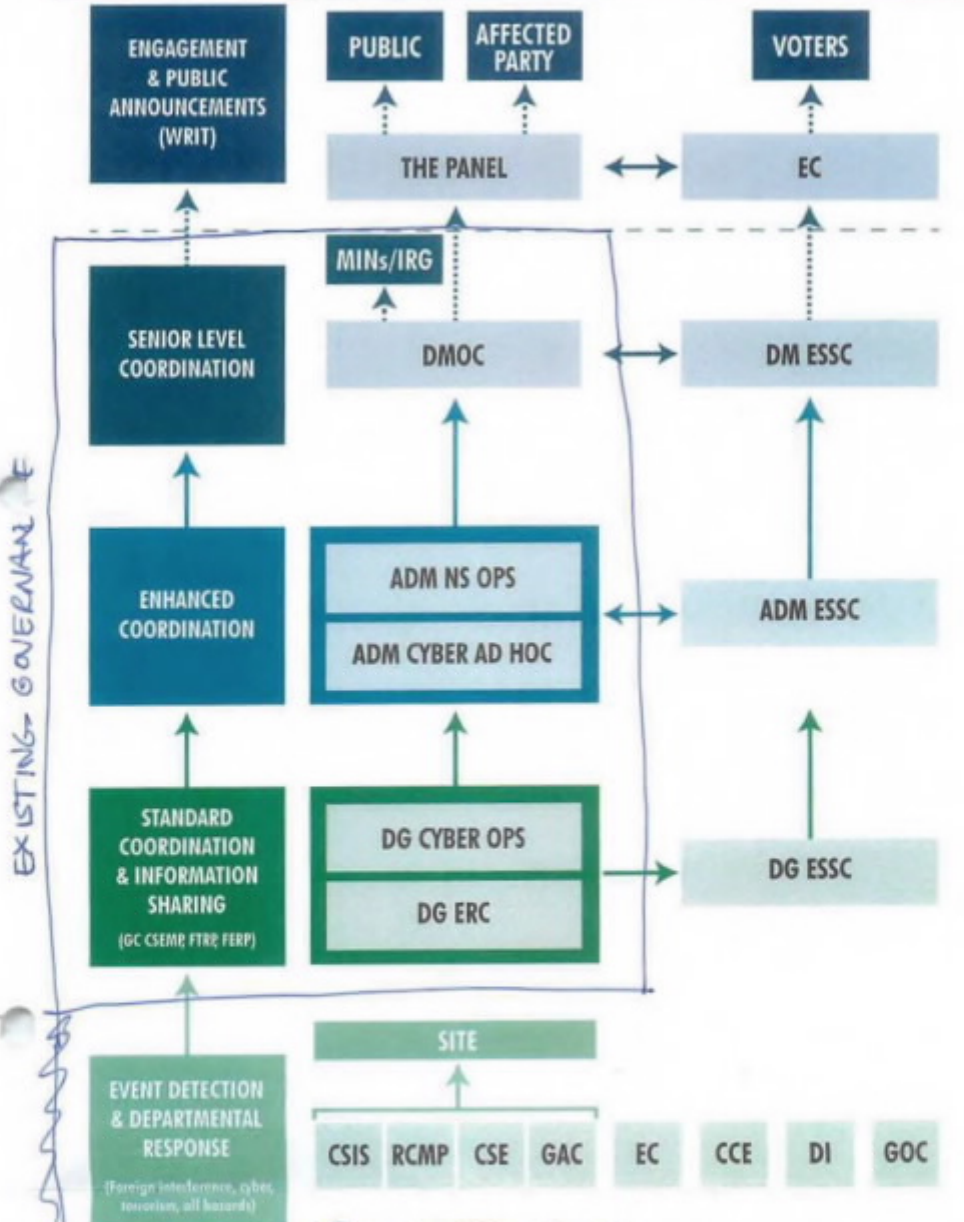
August 2019:

- Includes ADM ESSC, DM ESSC and P5

For Public Release

DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT DRAFT Election Incident Response Playbook

Unclassified
17 June 2019



- ADM Cyber Ad Hoc: Assistant Deputy Ministers ad hoc meeting on cyber
- ADM ESSC: Assistant Deputy Ministers Elections Security Steering Committee
- ADM NS OPS: Assistant Deputy Ministers National Security Operations Committee
- CCE: Commissioner of Canada Elections
- CSE: Communications Security Establishment
- CSIS: Canadian Security and Intelligence Service
- DG Cyber Ops: Directors General Cyber Ops Committee
- DG ERC: Directors General Emergency Response Committee
- DG ESSC: Directors General Elections Security Steering Committee
- DI: Democratic Institutions
- DM ESSC: Deputy Ministers Elections Security Steering Committee
- DMOC: Deputy Ministers Operational Committee
- EC: Elections Canada
- FERP: Federal Emergency Response Plan
- FTRP: Federal Terrorism Response Plan
- GAC: Global Affairs Canada
- GC CSEMP: Government of Canada Cyber Security Event Management Plan
- GOC: Government Operations Centre
- IRG: Incident Response Group
- MINs: Ministers
- RCMP: Royal Canadian Mounted Police
- SITE: Security and Intelligence Threats to Elections Task Force

Privy Council Office
Bureau du Conseil privé

For Public Release

v. 2019 06 05 SECRET

Critical Election Incident Public Protocol Panel - Meeting One
Record of Discussion

[Redacted], 80 Wellington, Ottawa, Ontario
 May 31, 2019
 3:00 pm to 4:30 pm

Attendees:Panel Members

Ian Shugart, Clerk of the Privy Council
 Greta Bossenmaier, National Security and Intelligence Advisor to the Prime Minister (NSIA)
 Nathalie Drouin, Deputy Minister of Justice and Deputy Attorney General
 Marta Morgan, Deputy Minister of Global Affairs
 Gina Wilson, Deputy Minister of Public Safety

Additional Invitees

Catherine Blewett, Deputy Clerk of the Privy Council
 Ian McCowan, Deputy Minister of Democratic Institutions (DM DI)
 Shelly Bruce, Chief of the Communications Security Establishment
 David Vigneault, Director of the Canadian Security Intelligence Service
 Gilles Michaud, Deputy Commissioner of the Royal Canadian Mounted Police (Federal Policing)
 Caroline Xavier, Assistant Secretary to the Cabinet, Security and Intelligence (PCO)
 Al Sutherland, Assistant Secretary to the Cabinet, Machinery of Government (PCO)
 Alia Tayyeb, Director of Operations, Security and Intelligence (PCO) - Secretary

Goals:

- Deliver a briefing on the Protocol and expectations
- Provide an overview of community governance and parallel streams of activity
- Approve the proposed workplan, including format and timing of future meetings

Agenda:**1) Briefing on the Critical Incident Election Public Protocol (CIEPP) (DM DI):**

During this portion of the discussion, the Panel:

- Agreed to the current version of the Protocol;

1/3

For Public Release

v. 2019 06 05 SECRET



- Noted that political parties would be provided with a final copy of the Protocol in advance of its public release, for their awareness.

On the CIEPP Threshold, the Panel:

- Agreed to conduct exercises to work through scenarios on how to apply the threshold for informing the public;
- Noted the need to clearly explain the threshold to the public, to instil a high degree of confidence in the process;
- Discussed that the Protocol describes the threshold as requiring the consideration of both the *material impact* of the incident on the ability to hold a free and fair election, and the *perception* that an incident may undermine the credibility of the election;
- Noted that if a public announcement is deemed necessary, the Panel would make the decision and the Clerk, on behalf of the Panel, would ask the relevant agency head(s) to issue a statement to notify Canadians; however, the Panel would actively support the agency head(s);
- Discussed the potential requirement to publicly address incidents that do not meet the threshold;
- Noted that while the focus of the Protocol is on foreign interference, the Protocol notes that a disruptive event or interference may also emanate domestically or have been conducted in collaboration with domestic actors; ultimately, the impact of the incident is the determining factor in determining if the threshold has been met; and,
- Noted that a decision is still to be taken on which entity will be asked to conduct the independent report on the implementation of the Protocol, as called for in the document.


On substitutes and delegates for Panel members, the Panel:

- Agreed that there would be no formal substitutes permitted for members that may be unavailable on a scheduled meeting date; however, that member could arrange for another member or a representative from his/her department to articulate the relevant interests and considerations on his/her behalf; and,
- Agreed that a Panel member can only be formally substituted if that Panel member becomes incapacitated.

2/3

For Public Release

v. 2019 06 05 SECRET

**2) Overall governance (NSIA)**


During this portion of the discussion, the NSIA presented the Elections Activities Map and explained the concurrent intergovernmental activities underway with respect to elections security.

3) Discussion and finalization of proposed workplan (All)

During this portion of the discussion, the Panel:

- Endorsed the proposed workplan;
- Noted the importance of exercising the Panel and agreed to hold a table top exercise (TTX) using a complex scenario;
- Agreed to meet with Elections Canada at an upcoming meeting, potentially in July;
- Considered the communications approach and agreed to discuss a communications strategy at an upcoming meeting of the Panel, with the ADM for PCO Communications to be invited.

Action Items:

- 
- Schedule ½-day retreat in June, which would include threat briefings and a TTX;
 - Arrange for individual sessions to brief Panel members on activities to date and community architecture (e.g. governance, incident management procedures), as requested;
 - Invite Elections Canada to a future meeting; and,
 - Schedule a discussion on Strategic Communications at an upcoming Panel meeting, possibly at the June retreat if the agenda permits.


3/3

For Public Release

UNCLASSIFIED
TLP: GREEN



Communications
Security Establishment

Centre de la sécurité
des télécommunications

CANADIAN CENTRE FOR CYBER SECURITY

CYBER SECURITY GUIDE FOR CAMPAIGN TEAMS

CAMPAIGN TEAMS

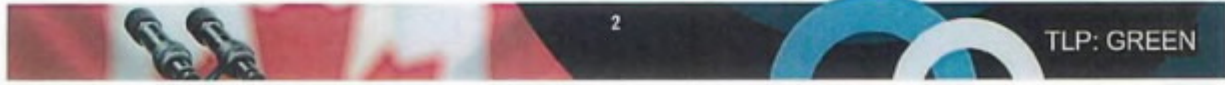
© Government of Canada
This document is the property of the Government of Canada. It shall not be altered, distributed
beyond its intended audience, produced, reproduced or published, in whole or in any substantial part
thereof, without the express permission of CSE.



UNCLASSIFIED
TLP: GREEN

TABLE OF CONTENTS

INTRODUCTION: WHY THIS GUIDE IS IMPORTANT TO YOUR CAMPAIGN PLANNING	3
BEFORE WE START... SOMETHING FOR EVERYONE	4
STEP 1: ASSESS WHAT CYBER SECURITY MEANS FOR YOUR CAMPAIGN.....	5
EXAMPLE OF A PLANNING CHART	6
STEP 2: UNDERSTAND WHERE YOUR DATA LIVES.....	7
STEP 3: SECURE YOUR DATA AND TECHNOLOGY	8
Devices.....	8
Passwords and passphrases.....	9
Two-factor authentication (2FA).....	10
Encryption	10
Camera lens covers	10
Securing devices in a bring your own device (BYOD) scenario.....	11
Phone specific threats	11
Social Media and Messaging	12
Instant messaging and texting apps	12
Social engineering	13
Malicious messages including emails.....	13
Data and Networks	14
Cloud services	14
Wi-Fi in the campaign office	15
Wi-Fi outside the campaign office.....	15
Backups and recovery of data.....	16
Portable data storage devices	16
Physical Spaces	16
STEP 4: PROVIDE CYBER SECURITY TRAINING	17
STEP 5: KNOW WHAT TO DISPOSE OF OR ARCHIVE.....	17
WHAT TO DO WHEN THINGS GO WRONG	18
Loss of control of social media channels	18
Identify and handle malicious messages	19
ADDITIONAL RESOURCES	20



For Public Release

UNCLASSIFIED

TLP: GREEN

INTRODUCTION: WHY THIS GUIDE IS IMPORTANT TO YOUR CAMPAIGN PLANNING

Welcome to the Cyber Security Guide for Campaign Teams.

The Canadian Centre for Cyber Security prepared this guide to assist campaign teams across Canada in the lead up to elections at the federal, provincial, territorial, and municipal levels.

In 2017, and again in 2019, the Canadian Centre for Cyber Security advised Canadians that foreign actors are likely to try to interfere in Canadian election processes using cyber systems to target political candidates and campaigns.

So if you're involved in politics – as a volunteer, paid staffer or candidate – you are more likely to be a target, particularly in the lead-up to an election.

Consider the information it takes to run a campaign. You start with a campaign strategy and a plan. Your team will also have lists of donors, supporters, and registered voters, as well as research you may have commissioned.

The bottom line is that, as a member of a campaign team, **you hold valuable, strategic data that others want to access and that you need to protect.** The information systems and devices you use and run as part of your political campaign are an important part of the election process. For that reason, **you have to prioritize cyber security before, during, and after your campaign.**

The decision of where and how to invest in cyber security is based on your campaign's requirements. However, if you focus on these decisions before the heat of a campaign, you won't have to worry about it midway through when time is scarce and the pressure is on.

With this Cyber Security Guide for Campaign Teams, we've outlined practical advice and guidance about cyber security that is applicable to all campaigns. It will help your campaign team's thinking about cyber security related to your candidate, your strategies, your data, and your technology. By following this guide, you will help protect your campaign from cyber security compromises and the accompanying consequences.

The Cyber Centre is pleased to work with you, through this Campaign Guide, to help you have a cyber safe campaign.



UNCLASSIFIED

TLP: GREEN

BEFORE WE START... SOMETHING FOR EVERYONE

As a kickstart to your cyber security planning, here are important, practical measures you and every member of your campaign team can take right now on any device to make your campaign more secure. Read more about these measures later in this guide or visit www.cyber.gc.ca for more on any of these steps.

Practice good password etiquette (page 9)

- Use unique passphrases or complex passwords.
- Don't share passwords. Don't use the same password for multiple accounts, websites, or devices.
- Use two-factor authentication (2FA) when available. (page 10)

Apply updates to your mobile devices, computers, and applications.

- Those updates are crucial to your security: they contain what we call security "patches". Don't ignore them.
- Be sure to apply updates to your mobile applications in addition to your device operating systems and get them to automatically update.
- Schedule a mandatory training session in which all campaign members update their devices and applications.

Secure your social media accounts (page 12)

- Use as many security options (settings) as you can for each social media platform.
- Know your options for delegating authority (what to do when you need multiple users to access one account).

Be on guard for phishing and spear-phishing messages (page 14)

- Know how to spot phishing and spear-phishing messages.
- Be wary of suspicious links – don't click on them.
- Use anti-virus or anti-malware software on computers.

Store your data securely and know your back-up procedures (page 16)

- Use only new USB memory sticks purchased by the campaign team. Use them for campaign-related work only. Do not use them on untrusted computers. (page 16)
- Secure data stored in the cloud or online by turning on the available security features. Consider storage solutions with restricted access. (page 14)
- Backup your vital campaign information and know where you have it backed up.
- Practice recovering your data at least once. This way you'll know what to do if you become a ransomware victim.

UNCLASSIFIED

TLP: GREEN

STEP 1: ASSESS WHAT CYBER SECURITY MEANS FOR YOUR CAMPAIGN

The data your campaign team holds and the technology you use during the campaign are unique to your campaign, so you need to have a strong understanding of what you're protecting. The planning chart on page 6 shows you how to take the next steps. But we'll start with the creation of three important lists.

DATA: First, create a list of the data your team will be relying on during the campaign. Email? Strategies? Plans? Lists? Photos? Videos? Research? It's important to itemize each data set or document, because you need to know what to do with it and how to protect it.

TECHNOLOGY: Next, consider what technology and devices your team will use during the campaign. Will the candidate have his or her own device? Who on the campaign gets a smart phone? Are volunteers using their own devices? Do you have to consider laptops, desktops or tablets?

PLATFORMS: Now, think about the communication platforms your team will use. It's likely your team will establish email addresses for the campaign. You will also likely use social media during the campaign, so make sure you itemize which social media platforms you've chosen. Identify the applications (apps) you expect to use, such as chat apps or messaging apps. Consider file sharing networks and video or photo databases. Make sure you list them all.

With these three lists, you're ready to move on.

Next, think about how your team will share—or won't share—your campaign data. For instance, you will not share your campaign budget with every volunteer, but communications volunteers might require access to your social media plan.

- Decide on and communicate about whom on your campaign team needs access to what information. In order to make your campaign secure, be clear on the access privileges that an individual will have.
- Determine what happens when you add to or change those lists during the campaign. What new information or technology do you expect to obtain, create or receive during the campaign? A new stump speech? New video clips? New polling data? A brand new laptop or mini-recorder? Adding items during a campaign will be easier if you've thought about them at the start. It will also be clear to the campaign team who should have access to new information or technology if you've established that up front.
- Establish and communicate policies and standards. For example, your volunteers will be eager to help, but if you don't make it clear to them that they aren't permitted to copy voter lists to their devices, your campaign risks a security breach.
- Consider how your campaign team will receive training on cyber security. You may have specific messages for team members to use as they knock on doors, but do they know what to do if they want to use a thumb drive on a laptop in the campaign office? Is it clear to them what to do if they receive links in emails?

As you establish your campaign team, you should also establish a culture of cyber security. Set clear expectations at the start, and you reduce the risks of cyber breaches throughout the campaign.

If you'd like to read more about the cyber threats within Canada and have a broader contextual knowledge of the cyber threats you could face, take a look at the Communications Security Establishment's *Cyber Threats to Canada's Democratic Processes* report from 2017 and the [update from 2019](#), as well as the Canadian Centre for Cyber Security's *National Cyber Threat Assessment* released in late 2018.

For Public Release

UNCLASSIFIED

TLP: GREEN

EXAMPLE OF A PLANNING CHART

DATA OR TECH	PERMITTED ACCESS	STORAGE	SECURITY	DISPOSE/ARCHIVE
Campaign Strategy	<ul style="list-style-type: none"> • Candidate • Campaign Manager • Finance Officer 	<ul style="list-style-type: none"> • Cloud provider 	<ul style="list-style-type: none"> • Create access control lists for individuals in permitted access column 	<ul style="list-style-type: none"> • Send to riding association office • Delete from all other storage
Social Media Plan	<ul style="list-style-type: none"> • Candidate • Campaign Manager • Communications Manager • Social Media Lead • Social Media Volunteers 	<ul style="list-style-type: none"> • Network folder • Dedicated Communications device 	<ul style="list-style-type: none"> • Create access control lists for individuals in permitted access column 	<ul style="list-style-type: none"> • Send to riding association office • Delete from all other devices
Donor List	<ul style="list-style-type: none"> • Candidate • Campaign Manager • Donor Coordinator • Finance Officer 	<ul style="list-style-type: none"> • Campaign leadership devices 	<ul style="list-style-type: none"> • Create access control lists for individuals in permitted access column 	<ul style="list-style-type: none"> • Send to riding association office • Delete from all other devices
Voter List	<ul style="list-style-type: none"> • Campaign Manager • Voter Coordinator 	<ul style="list-style-type: none"> • Network folder 	<ul style="list-style-type: none"> • Create access control lists for individuals in permitted access column 	<ul style="list-style-type: none"> • Return to Party Headquarters • Destroy local copies
Campaign devices	<ul style="list-style-type: none"> • As designated by the campaign leadership 	<ul style="list-style-type: none"> • With designated volunteers • In campaign office 	<ul style="list-style-type: none"> • Control access to devices, configure security settings, and apply all required updates 	<ul style="list-style-type: none"> • Remove all content • Wipe Devices
Volunteers devices (BYOD situation)	<ul style="list-style-type: none"> • Volunteer, allowed by campaign leadership 	<ul style="list-style-type: none"> • Kept with volunteers • Not stored in campaign office 	<ul style="list-style-type: none"> • Configure security settings on device and update during training sessions. 	<ul style="list-style-type: none"> • Encourage the removal of all campaign documents. • Change access permissions for volunteers (change passwords, remove access to networks etc.)

For Public Release

UNCLASSIFIED

TLP: GREEN

STEP 2: UNDERSTAND WHERE YOUR DATA LIVES

In order to protect your data and documents, you need to know where you're storing them. You'll want to keep a few things in mind as you consider this.

We recommend applying security based on your risk tolerance and budget. You may choose to hire an IT service professional or company to manage the set-up of your IT networks. For some campaigns, this could mean contracting with a managed service provider to **store your data in a cloud solution.** Cloud storage solutions specifically designed for election campaign use are available in Canada. **We recommend this option.** They move some of the data-protection risk from your campaign team to professional services. But not all cloud services are equal. Take a look at page 14 for advice on how to evaluate and choose cloud services.

For campaigns that do not choose to use a cloud solution, other IT set-ups are available. You might elect to establish a server or network file-sharing option. Or have all files saved on a limited number of devices. You may choose a

combination of both cloud and local file sharing. No matter what storage solution you chose, you will use the same cyber security principles for determining access to, and protection of, your campaign information.

The decision about how you access your information when you need it will likely play into how you conduct your campaign. Consider how access to the documents you've identified as critical for the campaign will meet the objectives of the campaign. How will you conduct your day-to-day business? Do you need to share the latest party messages on a daily basis? With whom? Should they be stored on a shared drive or on one specific communications device? Will you share updated strategies often and should you store them in the cloud?

To complete this assessment of where to store your data, you need to have a clear understanding of who has responsibility for what function on your team. Does this affect where your data is stored?

RISK TOLERANCE

As we mentioned earlier in this document, each campaign's needs are unique, as is your risk tolerance. Understanding your risk tolerance can help you make decisions about how you will secure your data and technology.

Risk tolerance is about making reasonable judgements about what could happen and what the result might be. What are you willing to lose, and what cannot be lost, at any cost? Determining risk tolerance should begin with a risk management meeting with your campaign team to review potential risk scenarios for your IT security and other elements of your campaign.

Take a look at lessons learned from previous campaigns and consider how issues have changed since that time. Consider the evolution in technology and the communications practices that exist today.

UNCLASSIFIED

TLP: GREEN

STEP 3: SECURE YOUR DATA AND TECHNOLOGY

The best approach to cyber security is to think about layers. Each cyber security action you take adds a layer of protection to your campaign.

The next pages walk you through specific cyber security tools and actions you should be using now, both in a campaign office and out on the campaign trail, because any piece of technology can be an attractive target during a campaign. The advice is grouped in four sections: **Devices, Social Media and Messaging, Data and Networks, and Physical Spaces.**

DEVICES

Your campaign team and candidate will certainly use mobile devices extensively, and these are attractive targets to threat actors. Lost, stolen, or compromised devices give threat actors unauthorized access to your network, and put work-related and personal information at risk. Secure the devices you use with the following measures:

- Lock all mobile devices with a strong password, PIN, or biometric (see password section, page 9).
- Apply operating system and application updates as they become available. This includes third-party apps as they may provide a conduit into social media accounts such as Twitter and Facebook. Always accept the updates when prompted because they often provide important security patches.
- Use an anti-virus application on your desktops, laptops and mobile devices.
- Do not use "Remember Me" features which store your ID and password on websites and mobile applications.
- Back-up your mobile device regularly.
- Turn off or disable features such as location services, Bluetooth, or Wi-Fi when you're not using them.
- Be wary of connecting your devices to unsecured or free Wi-Fi networks. Use a data plan with a reputable carrier instead of using free Wi-Fi. (see the Wi-Fi Security section, page 15).
- Use a power receptacle, like a portable battery pack, to charge your device instead of a USB port on a computer or in a free charging station. Using unknown USB power charging stations is not recommended because, not only can they charge your device, information can be transmitted to and from the device.
- Do not connect devices that you suspect are compromised to your PC or any other networked computer, especially if you only need to charge the device. Connecting compromised devices can infect the entire network. If you suspect your device is compromised, give it to your campaign team or IT professional for review.
- Do not leave your devices unattended in public places.
- Restrict others—even family members—from using your mobile devices.
- Avoid jailbreaking (modifying the phone to install unauthorized software) or trying to remove the security measures imposed by the device manufacturer.
- Do not install applications on your work devices without understanding the relevant campaign policies.
- Review the privacy policies and the access requirements (e.g. access to camera, microphone, calendar, location services) of approved applications before installing them on your mobile devices.
- Be aware of your surroundings when using devices, especially when entering passwords or sharing sensitive information.
- Take note of any odd device behaviour (e.g. rapid battery drainage or strange texts/emails) as it may indicate a compromise.

For Public Release

UNCLASSIFIED

TLP: GREEN

PASSWORDS AND PASSPHRASES

Passwords control access to your mobile devices, social media accounts, and email accounts. A weak or compromised password could lead to stolen campaign data. We recommend that you use **passphrases** that are longer and easier to remember than passwords. However, websites, applications, and services are all set up differently. You may have to follow the password creation rules of the website, application, or service that you're using. If you're able to use a passphrase, do so—otherwise be sure to use a strong password.

PASSPHRASES	PASSWORDS	PASSCODE
A memorized phrase consisting of a sequence of mixed words or other text. Use passphrases whenever you are able. (e.g. "closet lamp bathroom painting")	A string of characters used to gain access to sensitive data or devices. (e.g. Mj#wlpcsw27!)	Short codes made up of numbers. (e.g.385462).

For either passwords or passphrases, consider the following:

- Do not include common expressions, song titles or lyrics, movie titles, quotes etc. Keep the words random.
- Consider including words from different languages.
- Change only when there is a good reason to do so (e.g. a suspected or a known compromise).
- Do not use the same password on multiple accounts or devices.
- Do not change a password or passphrase by simply changing the number at the end of it (e.g. falsehousebookspeed1 to falsehousebookspeed2).

For passphrases:

- Choose four random words to create a passphrase that is at least 15 lowercase letters long.
- Use association techniques like scanning a room in your home, such as your bedroom and select "closet lamp bathroom painting".
- Do not use the names of your kids or members of your favourite sports teams. These could be easily guessed by a threat actor watching your social media.

For passwords:

- Use a minimum of 12 characters for complex passwords (if the creation rules allow for that length).
- Use a memorable phrase to help you remember a complex password (e.g. the phrase: "My jersey number when I played competitive soccer was 27!" could help you remember the password: "Mj#wlpcsw27!").
- Do not use something simple, like Password01, as a password. Do not simply substitute letters for numbers or symbols like Pa\$\$w0rd01.

For passcodes:

- Use passcodes only when you are specifically required to do so; otherwise use passphrases or passwords.
- Use randomly generated PINs where available.
- Avoid easily guessed combinations when choosing your PIN. (e.g. 1111, your birthday, your phone number).

For Public Release

UNCLASSIFIED

TLP: GREEN

TWO-FACTOR AUTHENTICATION (2FA)

Two-factor authentication (2FA) involves adding an additional factor beyond a username and password when you access an account to make it more secure. 2FA uses a combination of two different factors including something you know (e.g. a password), something you have (e.g. a token or a phone), or something you are (e.g. a biometric, like a fingerprint).

Because of the widespread nature of phishing attacks and password theft, many services, including most social media platforms, have added 2FA options. **We strongly recommend the use of 2FA** for these platforms, especially for important public-facing campaign accounts. Check with the service provider on how you can turn 2FA on.

For campaign office infrastructure that may allow remote access Virtual Private Networks (VPNs) and email services that give access to or contain sensitive campaign materials, campaigns should consider investing in 2FA infrastructure to provide the appropriate authentication to secure them. For systems containing sensitive campaign information, we recommend any 2FA solution over a password alone. Not all 2FA solutions are equal – but all 2FA solutions will improve your campaign's overall cyber security posture.

ENCRYPTION

Encryption converts readable information into unreadable cipher text to hide its content and prevent unauthorized access. Encryption can take place when your data is in transit (such as HTTPS web traffic) or at rest (such as the encrypted contents of a phone, laptop or computer hard drive). Encryption is the key mechanism to protect the security and privacy of campaign information in transit over the internet. It is also one of the primary ways to protect the contents of devices that may be lost or stolen during the campaign.

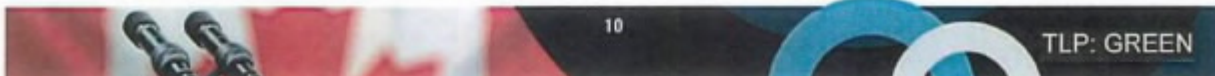
Most modern devices have options to encrypt your data. **We recommend turning encryption on where you can.** For example, on most mobile devices, setting a passcode to lock the device also encrypts the data it contains. Consult an IT professional to determine when you should encrypt memory cards, USB sticks, web sites, or any other means you use to store or transmit your campaign information.



CAMERA LENS COVERS

If you allow an app access to your camera and microphone, and threat actors access the app, they can access both the front and the back cameras, record you at any time an authorized app is in use, take pictures and videos without permission and upload them online instantly, and even livestream the camera to the internet.

- Consider using a camera lens cover on your phone and denying apps access to your phone camera. A camera lens cover is a thin mechanical privacy cover that you put over your device's camera. These covers can be purchased at electronic shops and allow easier access than covering with tape or other material.



For Public Release

UNCLASSIFIED

TLP: GREEN

SECURING DEVICES IN A BRING YOUR OWN DEVICE (BYOD) SCENARIO

If your campaign allows personal devices for official business use, remember that campaign staff and volunteers who leave the campaign may have sensitive information stored on their devices. Their personal devices may not have up-to-date software and security updates installed, which would leave sensitive information vulnerable. The sensitive information may not be encrypted on personal devices. Anyone using a personal device should:

- Follow BYOD policies to address expected behaviours and manage associated risks.
- Participate in cyber security training offered by the campaign. Campaigns should use training sessions to have all members update their cyber security measures.
- Request the installation of anti-virus software on their device, if they have not already been using it.

PHONE SPECIFIC THREATS

Most mobile and landline phone calls are not secure. Phones are susceptible to intrusion, and threat actors are able to monitor them with communication interception devices that mimic cell towers. **Consider having sensitive conversations in a private space away from electronic devices.** If this is not possible, be mindful of your phone's potential lack of security the next time you place a call.

If your campaign team holds or participates in regular teleconferences, consider changing the conference identification number on a scheduled basis. Consider who needs to have the call-in numbers and how those numbers are shared.

Bluetooth vulnerabilities

Threat actors can use Bluetooth vulnerabilities to steal your information. Hackers can exploit Bluetooth to gain complete control of your devices.

KNOWN BLUETOOTH ATTACKS

- **Bluejacking**—A threat actor sends unsolicited messages to your Bluetooth-enabled mobile devices. If you respond to the message or add the contact to your address book, you give the threat actor the opportunity to connect to your devices because you are establishing them as a known contact. Threat actors can then control your device remotely.
- **Bluebugging**—A threat actor poses as a device you're looking to connect to (e.g. headphones). You may not even realize that you are connecting to a spoofed device. Once connected, your device and your data are accessible as long as the spoofed device is in your list of paired devices.
- **Car Whisperer**—Car Whisperer software allows a threat actor to send or receive audio from the car kit installed in your vehicle. If exploited, threat actors could eavesdrop on your conversations by receiving audio from the car microphone.
- **Crackle**—A threat actor exploits flaws in the pairing process that allows key recovery so that your devices can be accessed.
- **GATtack**—An attacker creates a man-in-the-middle attack (i.e. secretly relays and can alter communications between sender and recipient) to intercept, clone, block, or change messages.

For Public Release

UNCLASSIFIED

TLP: GREEN

Bluetooth technology is continuing to evolve. New versions of Bluetooth have increased ranges and speeds, making data transfers easier and more convenient. The technology is changing, but you can protect your data and devices with a few simple actions:

- Turn off Bluetooth when you're not using it. On many devices you can find the option to turn off Bluetooth by swiping down on your home screen.
- Turn off discovery mode when you're not connecting devices.
- Avoid pairing devices in public spaces.
- Pair only with devices that you know and trust.
- Never transfer sensitive information over Bluetooth.
- Avoid using Bluetooth-enabled keyboards to enter sensitive information or passwords.
- Remove lost or stolen devices from your list of paired devices.
- Delete all stored data and devices from Bluetooth-enabled cars.

Voicemail

Threat actors can gain access to your voicemail and compromise your campaign. Since many voicemail PINs are only four digits long, intruders can easily guess or crack them. Use a voicemail PIN that is different from the factory setting default, and change it regularly. If possible, use a PIN longer than four digits for added security.

SOCIAL MEDIA AND MESSAGING

Activity on your campaign team's social media accounts impacts the public's perception of your campaign. If threat actors access your accounts, they can post sensitive or false information that discredits or embarrasses your candidate and puts your campaign at risk.

- Use strong and unique passwords (see password section on page 9) for each of your social media accounts to prevent all your accounts from being compromised in a single hack.
- Use two-factor authentication (2FA) when possible. (see 2FA section on page 10)
- Restrict access to social media platforms. Allow a limited number of campaign staff access to post or edit on social media channels.
- Know your options for delegating authority and approving content (what to do when you need multiple users accessing one account).

INSTANT MESSAGING AND TEXTING APPS

Instant messaging and chat apps are great for communicating quickly. Many use end-to-end encryption to secure conversations and offer features, like disappearing messages and identity confirmation, to maintain confidentiality. Be aware that conversations you assume are private can still be exposed. Exposure doesn't always come from a compromise of your application or the systems running the app. Despite a device's security settings or app encryption, an untrustworthy recipient can still take a screenshot of a conversation and post online. Take a moment to consider the sensitivities of your messages before you send them, regardless of your device's security.

UNCLASSIFIED

TLP: GREEN

SOCIAL ENGINEERING

Keep in mind that there's a human element to cyber security that could put you and your campaign at risk, even if you've taken all the technical steps to secure your networks and devices.

Social engineering relies on a threat actor's ability to exploit using technology. Rather than hacking into a system or account through technical means, a threat actor will try to manipulate the prospective victim. For example, a threat actor may claim to have a legitimate connection to you by pretending to be a constituent in your riding, a potential donor to your campaign, or a journalist. Threat actors may ask you to provide information (e.g. phone numbers or account information), open emails with attachments or visit specific websites – all for malicious purposes.

Social engineering tactics have a high success rate.

- Be suspicious of phone calls, visits, or emails from individuals asking about you, whom you know, and what you know.
- Verify who people are before giving them any information online. For example, if someone claims to be from a community organization or a media outlet, ask them to provide you with official identification.
- Never click on links. Instead, manually search for the web page in your browser.

MALWARE

Malicious software is designed to infiltrate or damage a computer system, without the owner's consent. Malware can come from software, email attachments, website downloads, links in texts, or infected media shared between users.

MALICIOUS MESSAGES INCLUDING EMAILS

Email may be your most common form of communication, and is therefore a highly attractive cyber target. Be aware that malicious emails, such as spam, phishing, and spear-phishing emails, could put you, your devices, and your information at risk. Malicious messages can also come through texts or apps.

Your campaign will likely receive messages, many by email, from organizations and members of the public that you may not know or have never worked with. Your campaign team needs to know how to sift out legitimate messages from malicious ones. At first glance, malicious messages may appear to be legitimate.

We recommend that you set up, with your email service provider, a DMARC (Domain-based Message Authentication, Reporting & Conformance) service. For example, DMARC services let you know if the emails you receive from Canada Revenue Agency (CRA) are actually sent from a CRA email account. This type of service effectively verifies that the domain, in this case CRA, is real.



Spam messages

Spam messages are any unsolicited electronic messages. Spam messages are often a source of scams or offensive content, and may contain malicious links that redirect you to an unsafe or fake website that contains malware or asks you to enter sensitive information (e.g. passwords). Spam may also contain malicious attachments that could infect your devices with malware.

For Public Release

UNCLASSIFIED

TLP: GREEN

Phishing and Spear Phishing

Phishing messages target a group of people by simulating a legitimate message from a trusted sender, such as an email or SMS (text message) from your political party or a community group in your riding. Phishing messages can include good news (e.g. someone is donating to your campaign) or include a threat (e.g. someone has information about you that they will release to the media). Either way, the aim of these messages is to get you to give up personal information or click on malicious links and attachments.

Spear-phishing messages are like phishing messages, but they are tailored to you based on your line of work, your interests, or personal characteristics. As someone openly

working on a campaign, threat actors can easily gather information about you so that they can create a personalized spear-phishing message.

Phishing and spear-phishing messages target people like you. These messages appear to be legitimate; they may use real logos or familiar colours, layouts, and fonts, which make it difficult for you to see the threat. **Email phishing is the most common method that attackers use to spread ransomware and malware.**

See page 19 for advice on how to identify and handle malicious messages.

RANSOMWARE

Ransomware is a type of malware that threat actors use to deny a user's access to a system or data until a sum of money is paid. Even if the victim pays the ransom, the threat actors may continue to demand more money. If you are a victim, we recommend that you don't pay but your decision should be based on the assessment of your risk tolerance.

DATA AND NETWORKS

CLOUD SERVICES

Cloud services offer software, file storage, email services, remote access to documents and other services which may make your campaign team more productive. **We recommend that your campaign team work with a cloud service provider to set up the IT networks that suit your specific needs.**

Choose a reputable cloud service provider. Read reviews and get recommendations on reputable cloud service providers.

- Ask your cloud service provider where your data and backups physically reside. Cloud service providers frequently use facilities outside of Canada. These facilities are subject to the laws of their host country and may be subject to additional scrutiny by that country's security services.
- Confirm that the service provider uses anti-malware protection, software patching, encryption, and redundant (backup) power.
- Encrypt sensitive files in the cloud. Many cloud service providers offer file encryption by default.



For Public Release

UNCLASSIFIED

TLP: GREEN

WI-FI IN THE CAMPAIGN OFFICE

If your campaign chooses to establish a Wi-Fi network, use these technical measures to strengthen your Wi-Fi network.

- Change the default Wi-Fi network name and the router access password on your network router. The network name is the Service Set Identifier or SSID. You can usually make changes online by following the router manufacturer's instructions.
- Install software or hardware firewalls on your network and its devices (e.g. software firewall on laptops).
- Use Wi-Fi Protected Access 2 (WPA2-Enterprise) on your wireless router.
- Create a guest Wi-Fi access point to ensure your sensitive information cannot be accessed. To create the Wi-Fi access point there are two options:
 - Subscribe to a separate data line with your provider. This preferred option keeps your guest network and campaign network completely separate.
 - Use a router that has a separate guest network. This alternate option requires regular maintenance, and does not totally remove the threat of a compromise from the guest account.
- Ensure that router firmware is up-to-date.
- Use hardware that is currently supported by a vendor and make sure to apply all security updates.
- Set up a VPN to allow staff to access campaign networks and systems remotely.

WI-FI OUTSIDE THE CAMPAIGN OFFICE

Instruct all staff and volunteers to **avoid using unsecured or free Wi-Fi**.

Unsecured or free Wi-Fi may be convenient, but it is relatively easy for anyone else on the network to eavesdrop (i.e. intercept communications or data). For instance, you may receive a common password at a local coffee shop, but that does not make the Wi-Fi network secure. It is very hard to protect phones or devices when they are connecting to an unsecured or free Wi-Fi hotspot. Threat actors can create "Sign-in for free Wi-Fi" fake web pages on the local network and add malware to that page. The malware will then spread easily and threat actors can gain complete control over your device, even with a password provided by a coffee shop.

- Ensure that all staff and volunteers use a data plan with a reputable carrier, especially when doing sensitive work. They should not connect to unsecured or free Wi-Fi networks.
- Make sure the Wi-Fi settings on your device do not automatically connect you to a network. Turn the "automatic connection" function off.
- Do not allow staff and volunteers to connect devices that connect to unsecured or free Wi-Fi to the sensitive IT resources used by your campaign. They should use a different device that has not connected to unsecured or free Wi-Fi.

If your staff or volunteers need to use unsecured or free Wi-Fi on their personal or campaign devices, they should not type any sensitive information while connected to that network. This includes passwords to social media accounts or login information for special sites.

You can use your own campaign-specific Virtual Private Networks (VPN) and anti-malware services to lessen the risk associated with using unsecured or free Wi-Fi. A VPN is a private communications network created over an often less-secure shared or public network. Organizations use VPNs as closed, restricted networks, allowing only authorized users access. VPN communications are typically encrypted or encoded to keep non-authorized users from accessing all data flowing over the public network. However, you should assume the devices and any data communicated over VPNs may be compromised.

- When looking to create or use a VPN, choose a commercial VPN appliance or cloud product that is purposely installed on your network. Be aware some commercial "VPN services" simply mask identities to increase privacy but do not enhance the security of your data.

UNCLASSIFIED

TLP: GREEN

BACKUPS AND RECOVERY OF DATA

You should have a plan for recovering from successful cyber attacks (e.g. ransomware, denial of service, defacing websites). Maintain backups of your information so you can recover from an attack or a lost or stolen device.

Steps 1 and 2 of this guide should have helped you identify the information and data that is critical to your campaign. An IT service provider or cloud service provider can help you ensure that the right information is backed up frequently and that you can quickly recover the backed up information in a timely manner.

PORTABLE DATA STORAGE DEVICES

You might store copies of your files on portable data storage devices, such as USB memory sticks (thumb drives), so that you can work from anywhere. If you don't protect portable storage devices and information properly, a threat actor can access and copy that information.

- Use only new USB memory sticks purchased by the campaign team.
- Use USB memory sticks for campaign-related work only. Do not use a campaign USB on a personal device, as malware may jump from one device to another.
- Do not connect untrusted USB memory sticks to your devices, as they may have preinstalled malware on them.
- Report a lost or stolen portable data storage device to your campaign team.
- Consider encrypting your portable data storage devices.

An untrusted USB memory stick may be one you receive at a conference or from someone else. Remember, if your campaign did not purchase it new, you should either throw it out or have it scanned for viruses and malware.

PHYSICAL SPACES

Not all volunteers or campaign staff need the same access to your office or devices. Set restrictions on who has physical access to equipment and facilities. Physical theft and equipment tampering should be a real concern as it relates to cyber security. You should consider the following security protocols for your physical spaces:

- Determine who has access to servers, laptops, or teleconference equipment.
- Limit knowledge of any physical combination locks your campaign uses.
- Keep a list of who needs and who possesses a key to the office, and determine who locks up at the end of the day.
- Decide how you lock or secure essential equipment so it doesn't go missing.

Establish device-free physical spaces to hold private discussions and forbid the use of devices in those spaces. If a device has been compromised, the microphone or camera may be turned on remotely and without your knowledge. **Keeping devices out of certain discussions is the only way to ensure those discussions stay private.**

UNCLASSIFIED

TLP: GREEN

STEP 4: PROVIDE CYBER SECURITY TRAINING

Most of the people on your campaign team will be familiar with technology, but they will likely not all have the same appreciation for cyber security and how their actions on their devices could affect the campaign.

Despite the best cyber security tools and measures, breaches still happen, and people are often the weak link. It is human nature to be curious about a document or link, but clicking on the link or opening the document could mean you get compromised.

Once you have a strong understanding of what data and technology you are working with, **you need to train everyone on proper cyber security awareness. Do not underestimate the value of good training.**

First, understand what volunteers need to know. You should have a clear idea of what role each person or group is taking on. This will determine what devices you permit individuals to use. Campaign members should know what you require of them.

Next, using this guide, establish procedures and policies for handling campaign data and technology. If you expect team

leads to be the only ones to access files, you should make this clear. If only certain people can save or edit documents, that should also be clear.

A culture of cyber security can help keep your campaign secure. Campaign team members should reinforce the established procedures and policies established by living them. Shortcuts may seem easier, but they leave your campaign vulnerable. **Establish a practice that allows all campaign team members to admit when they have made a security error.** You want them to identify potential cyber security problems as soon as they occur so you can work to fix them before your campaign is compromised. If campaign members see something suspicious, they should report it.

Finally, run cyber security training sessions for all campaign team members. They should understand the impact of reusing passwords, clicking on unknown links, or using free Wi-Fi. Plan to present specific scenarios during the training and discuss the mitigating steps volunteers need to take if something goes wrong or they make a mistake.

STEP 5: KNOW WHAT TO DISPOSE OF OR ARCHIVE

The process of understanding what data and technology you will work with during a campaign (steps 1-3) leads you to this final step: What do you do after the campaign with the documents you've created and the devices you've used? Step 5 in this process shouldn't be too tough if you know what you're working with, hence the reasons steps 1-3 are important.

In terms of cyber security, **cleaning up after a campaign is as important as the start of a campaign.** Your campaign and candidate risk their reputations if you merely abandon documents in a cloud service or on a network server. Likewise, leaving files on a laptop makes you vulnerable to unauthorized access, depending on where the laptop goes after the campaign. Disposing of or archiving your data ensures you know who has control of it and eliminates the risk to your face.

As you determine what you need to keep or dispose, you'll need to consider a few things. Your party or riding office may have directives about where campaign information goes, and the elections authority, such as Elections Canada, has requirements for the types of information that you must submit. You may also have legal requirements to keep or dispose of certain information. The requirements will be different for each level of election (municipal, provincial, territorial, federal).

Finally, keep in mind what data you or your party are going to need for the next election. At the end of a campaign it may not seem like a problem, but with a few planning steps, your secure data and information will be ready for you when you decide to jump back into the democratic process.

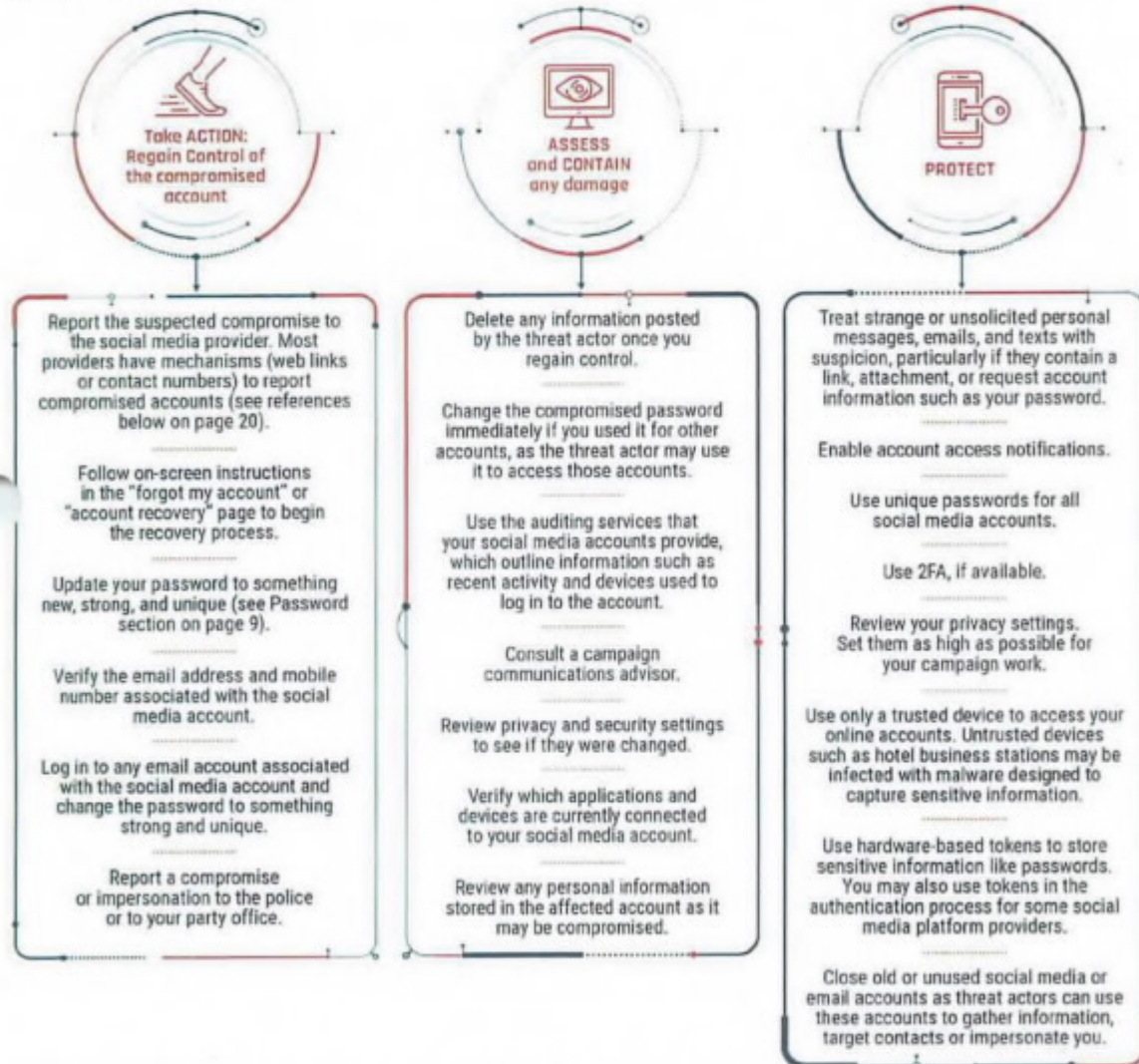
UNCLASSIFIED

TLP: GREEN

WHAT TO DO WHEN THINGS GO WRONG

LOSS OF CONTROL OF SOCIAL MEDIA CHANNELS

The results of an account compromise can be devastating. If one of your social media accounts are compromised: **take action, assess and contain, and protect.**



If you need to recover access to your social media, be aware that threat actors often use the recovery method to hijack account access. Any secondary account used for recovery, such as email, should be secured by a password that is not shared, and should be protected by 2FA. If the account recovery method uses personal questions, do not have answers that your social media pages easily provide.

For Public Release

UNCLASSIFIED

TLP: GREEN

IDENTIFY AND HANDLE MALICIOUS MESSAGES

All members of a campaign team should know how to identify malicious messages and how to handle them.



Verify that you really know the sender and, if possible, that the tone of the message is consistent with the sender.

Verify that the sender's address is valid. Sometimes threat actors will use addresses that look legitimate, but are altered in very slight ways.

Look for misspelled words in the body of the message. This is a trick used to bypass spam filters.

Look for unusual phrasing in the message, which may suggest that the author isn't legitimate.

Look for an offer that is too good to be true.

Pay attention to a request, which may include a threat, for sensitive information (e.g. personal or financial information).

Ensure the content of the message is relevant to your campaign work if the message is sent to your campaign email address.

Check that included links or attachments are relevant to the content of the message



Never click on links included in malicious or suspicious messages, even if they offer to remove you from a distribution list. If someone sends you a link (e.g. a news release) browse to the page or search for it online instead.

Never open attachments included in malicious messages. Malware often hides in attachments.

If you must open an attachment, open it on a computer that is not connected to the campaign IT infrastructure.

Do not reply to suspicious messages or spam messages. Doing so will only confirm that your address is valid, resulting in more spam.

Do not provide any confidential information (e.g. user name or password), even if the emails appear legitimate. If the email appears real, contact the sender another way (e.g. call them) to verify the request before providing information.

Do not forward suspicious messages to other people. If you need to show it to someone, ask the person to view it on your screen or print it out.

Delete spam messages or move them to a junk folder. If you're unsure whether it's spam or you don't know what to do with the message, talk to your campaign team lead.

HOW TO HANDLE POTENTIALLY CRIMINAL MESSAGES OR CYBERCRIME

The Royal Canadian Mounted Police (RCMP) generally interprets cybercrime to be any crime where the internet and information technologies (such as computers, tablets, personal digital assistants, or mobile devices), have a substantial role in the commission of a criminal offence. It includes technically-advanced crimes that exploit vulnerabilities found in digital technologies. It also includes more traditional crimes that take on new shapes in cyberspace. If you receive an offensive, abusive, or potentially criminal message, whether it seems to be spam, phishing or something else, or if you think criminals are asking you for confidential information, inform your local police and the RCMP. Save the message, as authorities may ask you to provide a copy to help with any subsequent investigations. Do not send the message to others.

For Public Release

UNCLASSIFIED

TLP: GREEN

ADDITIONAL RESOURCES

Recovering Access to Social Media Accounts:

The following table provides some quick reference links to help you should your social media account be compromised.

Platform vendor	Compromised account resources	Impersonation account resources
Facebook	https://www.facebook.com/hacked	https://www.facebook.com/help/174210519303259/
Twitter	https://help.twitter.com/en/safety-and-security/twitter-account-hacked https://help.twitter.com/en/safety-and-security/twitter-account-compromised	https://help.twitter.com/forms/impersonation
Instagram	https://help.instagram.com/368191326593075	https://help.instagram.com/446663175382270
Youtube	https://support.google.com/youtube/answer/76187?hl=en	https://support.google.com/youtube/answer/2801947?hl=en
LinkedIn	https://www.linkedin.com/help/linkedin/answer/56363/reporting-a-hacked-account?lang=en	https://safety.linkedin.com/identifying-abuse#profiles
Snapchat	https://support.snapchat.com/en-US/a/hacked-howto https://support.snapchat.com/en-US/article/locked	https://support.snapchat.com/en-US/i-need-help

We all play a role in protecting Canada's cyber landscape. The following reports provide additional information on some of the cyber threats facing Canada today.

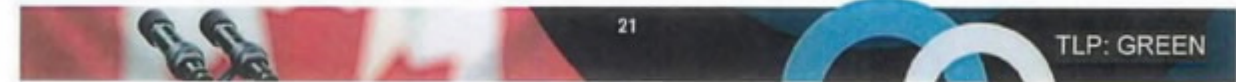
- [Cyber Threats to Canada's Democratic Process report 2017](#)
- [Update of the Cyber Threats to Canada's Democratic Process report 2019](#)
- [National Cyber Threat Assessment 2018](#)
- [An Introduction to the Cyber Threat Environment 2018](#)

For Public Release

UNCLASSIFIED

TLP: GREEN

NOTES



For Public Release

EXERCISE MATERIAL // FOR TRAINING PURPOSES ONLY

CASE STUDIES

Australia – Political party network hack

In February 2019, the Australian Cyber Security Centre, an intergovernmental agency that offers cybersecurity services and advice to the Australian government, announced that it had detected malicious activity that targeted the Parliament House IT networks earlier that month.

non-govt. HW

The head of the Australian Cyber Security Centre noted that the computer networks of the Liberal Party, the National Party and the Labor Party had been accessed. However, the agency did not publicize the type of material that was accessed, nor the technique used by the attackers to access the networks.

The Australian Prime Minister addressed Parliament on the issue on February 18. He assured his colleagues and citizens that there was no evidence of electoral interference and that measures would be put into place to ensure the security and integrity of the general election, which was held on May 18, 2019.

To help prepare for the coming general election, the Prime Minister instructed the Australian Cyber Security Centre to be ready to support any political party or electoral management body in Australia with technical expertise.

More Information:

<https://www.cyber.gov.au/news/parliament-house-network-compromise>

<https://www.abc.net.au/news/2019-02-18/prime-minister-scott-morrison-cyber-attack-hackers/10821170>

- gather info.
- alert panel
- alert victims.
- draft comms.
- manage ops
- update comms

parallel

- tests = stopped acty?
- damage assess?
- attribution?
- public?

prep! - work to pol parties hygiene

EXERCISE MATERIAL // FOR TRAINING PURPOSES ONLY

France – Political party leak

On Friday, May 5, 2017, two days before the second and final round of voting for the French presidential election, over 20,000 emails from the Emmanuel Macron presidential campaign were leaked on the Internet.

The Macron Leaks contained nine gigabytes of communication material that was stolen from the Macron campaign. The perpetrators released the material on the Internet immediately before the 48-hour media blackout that is stipulated by French electoral law. Traditional media organizations in France abided this blackout and did not report on the Macron Leaks, which severely limited their circulation.

The leaks were the culmination of a long-running campaign designed to discredit Macron. In the months leading up to the presidential election, state-sponsored Russian media began to circulate rumours about Macron's political donators, and his own personal finances. This is in addition to repeated attempts to infiltrate the Macron campaign by use of email spoofing and spear-phishing.

The French media abided by the blackout period. The Macron campaign was able to quickly respond to the attacks on social media. The attackers also attempted to use American and English-speaking networks to spread the leaks, which were largely ignored by the French-speaking public.

More Information:

https://www.diplomatie.gouv.fr/IMG/pdf/information_manipulation_rvb_cle838736.pdf

public —
— inform public

Considerations
- stop it?
- damage?
- attribution?
- media coop?

prep - media
dispos

EXERCISE MATERIAL // FOR TRAINING PURPOSES ONLY

Germany – personal information leak

Throughout December 2018 and January 2019, the personal information of an estimated 1,000 individuals was published on the Internet (specifically Twitter). This included information from German Members of Parliament, European MPs, and MPs from German state parliaments. The leaks included personal contacts and some correspondence.

The German Interior Minister told the press that the hacker collected information through the misuse of log-in information and security vulnerabilities for cloud services, email accounts and/or social media networks.

The German Federal Criminal Police Office apprehended a suspect on January 8, 2019. The suspect was a young man who claimed to have acted alone, with no foreign state assistance or sponsorship.

In the aftermath of the leak, it was determined that very little sensitive information was leaked to the public.

More Information:

<https://www.bbc.com/news/world-europe-46757009>

Germany – disinformation campaign

In January 2016, Russian and German television companies began airing reports about a German-Russian girl named Lisa, who claimed to have been kidnapped and gang-raped by a group of Muslim refugees in Berlin. These reports were widely debunked, but dominated the news cycle for weeks in Russia and Germany.

Despite the story being proven false, Russian diplomats accused German authorities of perpetuating a cover-up, while German officials asserted that their Russian counterparts were partaking in spreading propaganda.

Members of the Russian diaspora across Germany organized dozens of protests and demonstrations related to the Lisa case.

More information:

<https://www.nato.int/docu/review/2016/also-in-2016/lisa-case-germany-target-russian-disinformation/EN/index.htm>

public domain

police

- fast response
- common
- involves private] parallel

prop - cyber hygiene!

For Public Release

EXERCISE MATERIAL // FOR TRAINING PURPOSES ONLY

Ireland

An investigation into Facebook pages associated with the Thirty-sixth Amendment of the Constitution of Ireland, or the referendum of May 2018 on abortion, found that while a majority of Yes pages (pro-choice) were managed from Ireland, the majority of No pages (anti-abortion) were managed by a combination of Irish, British, and US users.

This raised some concern about the potential for foreign actors to attempt to interfere the domestic politics of Ireland. Both Facebook and Google banned foreign-purchased ads discussing the Irish referendum during the campaign. Google banned all advertising two weeks before the vote to further ensure that their advertising was not maliciously used.

More Information:

<https://www.cnn.com/2018/05/18/tech/ireland-abortion-referendum-facebook-google-intl/index.html>

fragment ad space

For Public Release

EXERCISE MATERIAL // FOR TRAINING PURPOSES ONLY

United Kingdom – Brexit referendum interference

Investigative reports began to raise concerns about the possibility of Russian interference in the June 2016 United Kingdom European Union membership referendum. Journalists raised questions about the sources of certain influxes of money, which was donated to support the Brexit "Leave" campaign, and the actions of figures from the United Kingdom Independence Party which supported leaving the EU.

While the official position of the Russian government was neutral regarding Brexit, Russian sponsored television such as RT and Sputnik covered the referendum campaign extensively, and showed significant bias to the leave campaigners.

Months after the vote, additional investigators showed that 150,000 Twitter accounts which had communicated about Brexit had ties to the Russian government. Similar concerns about foreign interference were raised about other social media companies.

Independent academics and reporters continued to publish news and studies on major cyberattacks against the UK government, and media and telecommunications and energy sectors perpetuated by Russia.

In July 2018, the Electoral Commission announced it was issuing a fine against the official Vote Leave for breaking legal spending limits and illegally coordinating with another campaign, BeLeave.

The full extent of the interference attempts in the British referendum are not yet known. There are investigations underway by numerous British authorities, including the Electoral Commission

More Information:

<https://www.theguardian.com/world/2018/jan/10/russian-influence-brexit-vote-detailed-us-senate-report>

For Public Release

EXERCISE MATERIAL // FOR TRAINING PURPOSES ONLY

United States – Political party leak

In the months leading up to the 2016 presidential election, thousands of internal emails from the Hillary Clinton presidential campaign team, the Democratic National Committee and the Democratic Congressional Campaign Committee were leaked to the public. The United States intelligence community has concluded that the malicious actors behind the leaks were sponsored by the Russian Government, with the explicit goal of influencing the election.

The email hacks were carried out through relatively simple email phishing. High-level members of Hillary Clinton's campaign team were targeted with phishing emails which successfully enabled the hackers to use email passwords to access campaign staff emails.

The hackers also used malware, injected on the Democratic Congressional Campaign Committee's network, to access email passwords, research, staff communication, and personal banking information. Through this, the hackers also gained access to the Democratic National Committee's network.

These organizations learned they were hacked in May 2016 and hired a private security network to remove the malware, but the company was still removing malware on the networks up to October 2016.

Once hackers had possession of material, they used a variety of outlets to spread the leaked communications. This included fake websites and social media accounts, and giving material to third parties (in this case, WikiLeaks) to further spread the leaks. The hackers also contacted reporters and media figures with information of the hacks and members of the Trump campaign.

More Information:

<https://www.foreign.senate.gov/imo/media/doc/FinalRR.pdf>

https://www.washingtonpost.com/news/politics/wp/2018/07/13/timeline-how-russian-agents-allegedly-hacked-the-dnc-and-clintons-campaign/?utm_term=.723b3bd389eb

For Public Release

Secret
Canadian Eyes Only / Réservé aux Canadiens

ANTICIPATING FOREIGN THREATS TO CANADA'S 2019 ELECTION

~ A BACKGROUNDER ~

CONTEXT

Cyber threat activity against the democratic process has been increasing around the world, and Canada is not immune. A small number of nation-states have undertaken the majority of the electoral interference against democratic processes worldwide. The internet, evolving technologies, and social media are introducing new issues, such as fake news and misinformation. Traditional espionage and foreign influence continue, fully incorporating these tools.

As such, countries are subjected to a variety of efforts by foreign states that are intended to manipulate, disrupt or discredit the integrity of democracy. These activities are conducted by a range of actors, including foreign governments, state proxies, non-state actors, co-optees, and private individuals. With just over a year to go before Canada's next federal election, it is worthwhile to consider the types of foreign threats we could expect before, during, and immediately after the election. The present focus is on state-sponsored activities that are covert, deceptive or threatening, rather than activities that fall within the boundaries of overt advocacy or diplomacy. Any activity by or at the behest of a foreign state and others that is intended to influence the outcome of an election in Canada can undermine our democratic process.

Broadly speaking, the foreign threats to Election 2019 can be assessed in four categories, based on their intended effects:

- Changing the prospects for political actors;
- Manipulating public discourse;
- Damaging the integrity of the electoral process; and,
- Influencing the behaviour of elected officials.

CHANGING THE PROSPECTS FOR POLITICAL ACTORS

- Attacking the reputation of individuals or parties: Russia made a deliberate effort to damage the electoral prospects for Secretary of State Clinton in 2016, through an unprecedented in scope "hack-and-leak" operation. This has undeniably affected the credibility of the electoral process in the minds of many Americans. A hacker group connected to Russian military intelligence leaked over 21,000 emails two days before the 2017 French presidential election, in a failed attempt to damage the campaign of Emmanuel Macron. Russia has employed similar techniques against Canadians in non-political contexts, notably against individuals associated with the World Anti-Doping Agency. In 2019, Canadian political parties, candidates, and their IT infrastructure are potential targets.
- Advancing a favoured individual or group: Foreign state-directed support for preferred candidates or political parties, in concert with resources, information or cyber tools, could alter the balance in a competitive race. Some foreign actors have: stated their intention to provide financial assistance to candidates planning to run for public office; offered to reimburse individuals for their donations to political parties or candidates; and, conducted cyber-based operations and information operations to discredit or promote candidates or political parties.

For Public Release

Secret
Canadian Eyes Only / Réservé aux Canadiens

lists, polling place enhancement features) are protected and resilient, but not invulnerable. We do not have any current intelligence pointing to a credible attempt to sabotage Canada's electoral machinery, but we should not entirely rule out the possibility of an attempt.

- Suppressing turnout: In addition to information operations aimed at spreading political misinformation or propaganda, more aggressive approaches are available, such as using social media or "robocalls" to promote false information about polling stations or registration, or to spread fear of election-related violence. It is conceivable that a motivated and capable state actor could attack related infrastructure (e.g., electrical grid, transportation infrastructure) and systems in order to disrupt voting in one or more locations, but this would be a high risk undertaking with a low chance of meaningful success. We have no intelligence that these systems would be under heightened threat during the election period.

INFLUENCING THE BEHAVIOUR OF ELECTED OFFICIALS

- Leveraging prior support for an individual or group: Applying pressure on elected officials to do (or not do) specific things after Election 2019, activating influence that has been slowly developed over months or years of cultivation.
- Active operations to build new inappropriate relationships: Identifying and targeting vulnerable elected officials after the vote, to prepare the way for future direct influence.

WHAT WILL HAPPEN, AND WHEN?

Some activities may be time-bound, depending on specific deadlines or events (candidate selection, platform release, election date, Cabinet and committee formation). Hostile actors tend to calibrate their activities to times or locations that promise the greatest impact. They are also learning and adjusting based on recent successes and failures (e.g., Macron leak may have been too close to election date).

Some of the actions taken against Election 2019 may be driven by events, with foreign actors taking into account opportunities which present themselves unexpectedly, such as a domestic or foreign event or a trending news story. Not all actions may be specifically directed by foreign governments; some may reflect innovation or entrepreneurship on the part of proxies, co-optees, and perhaps individuals. In addition to foreign states and non-state actors, we need to also consider that other threat actors, such as hacktivists and cyber criminals.

From experience we know that timely attribution of such interference efforts can be difficult. Measuring the impact of interference will be harder still. As outlined in the attached sampling of recent electoral interference activities, adversaries seek specific vulnerabilities in democratic systems, so no two attacks may look alike.

In addition, the technologies used are constantly evolving and becoming less expensive and easier to acquire. This enables state and non-state actors. Advanced instruments such as artificial intelligence-based systems and "deepfake" technologies are meanwhile advancing in real time, offering new opportunities for deception and disruption.

While we cannot predict the exact nature and scale of attacks on Election 2019, we know Canada is not immune, and can expect little or no warning.

For Public Release

Secret
Canadian Eyes Only / Réservé aux Canadiens

index

RECENT INTERFERENCE ACTIVITIES (Examples)

TARGETS	INTERFERENCE ACTIVITIES
 New Zealand (NZ) 2000-present	Chinese agents, including diplomats, work closely with local community groups in NZ, such as the Peaceful Reunification of China Association of New Zealand, to support and facilitate bloc-voting and fund-raising for ethnic Chinese political candidates in NZ who support the People's Republic of China agenda.
 Italy 2018	Russia promoted a fake sex crime to stir fear of migrants and Muslims, and amplified a false claim that former Prime Minister Matteo Renzi was associated with a top Mafia boss. Russia also worked to establish friendly relations with the far-right, Euroskeptic, anti-immigration party <i>Lega</i> .
 France 2017	Russia gave €9 million euros in financial support to far-right Front National (FN), and mounted a propaganda and "hack-and-leak" campaign against President Macron. Botnets were used to amplify extreme opinions prior to the election, and some bots—also active during the 2016 United States election—promoted false, defamatory information about Macron.
 Spain 2017	Bots were used to expand the reach of hyper-partisan information prior to the Catalan independence referendum. Confident attribution of a particular threat actor has been difficult in this case, though some Kremlin-backed media outlets and social media profiles were responsible for spreading some of the false news and hyper-partisan information.
 Australia 2012-2017	Two billionaires linked to the Communist Party of China donated millions to Australian parties, and a senator was effectively bribed into publicly calling for Australia to respect China's claims in the South China Sea.
 Netherlands 2015-2017	Kremlin-backed media agency, RT, spread false news, including fake polling results to suggest the majority of Dutch citizens wanted to leave the European Union.
 Mexico 2016	Russia's RT broadcasted Spanish language programming favouring President Andres Manuel Lopez Obrador. Prior to the election, Russian IP addresses were among the most frequent visitors to the country's new online voting infrastructure.
 Ghana 2016	Unknown adversaries gained access to the Central Election Commission as votes were being counted, and fake results were tweeted. The outcome of the election was not altered, but the incident sowed confusion, and demonstrated attribution to a specific threat actor is difficult.
 UK 2016	Bots were strategically placed to amplify hyper-partisan information prior to the Brexit referendum. Bots accounted for at least 5% of Twitter profiles that tweeted "Vote Leave" or "Vote Remain" messages and hashtags before the referendum, and only 1% were identified as Russian. UK Parliament is currently investigating foreign interference in the referendum.
 USA 2016	The Kremlin-backed Internet Research Agency managed botnets to promote fake news and organize rallies in several states on socially divisive issues. Both major political parties were subjected to cyber espionage attempts by Russia, including, a hack-and-leak operation against presidential candidate Hillary Clinton. The voter registers of Arizona and Illinois were forced to be shut down after several attempted cyber intrusions, and Pennsylvania's voting systems were rendered unusable by ransomware.
 Germany 2015-2017	Russian hackers targeted top politicians and the Bundestag with two cyber attacks and marketed a false news story about a sex crime ("Our Lisa") to smear the German government and sow racial discontent. Russia nurtures links with far-right (<i>Alternative für Deutschland</i>) and far-left parties (<i>Die Linke</i>).

For Public Release

UNCLASSIFIED
RRM Canada

2019 UKRAINIAN ELECTIONS FINAL REPORT

Purpose

[1] This open source report is the final report in a series prepared by Rapid Response Mechanism (RRM) Canada on Foreign Interference (FI) during the 2019 Ukrainian presidential elections. The aim of the series was to enhance the global understanding of contemporary threats to democratic systems of governance while informing Canadian efforts aimed at safeguarding Canada's elections from FI. This report is a summary of key findings from the series of reports that was produced with the objective of identifying key lessons learned from the Ukrainian presidential elections. The reports were based on secondary sources, including insight from the RRM network and the community of experts, as well as primary research conducted by RRM Canada leveraging its open data monitoring and analytical capacity.

Overall Assessment

[2] Based on evidence summarized below and previous RRM reports, the Ukrainian presidential election was likely the target of a Russian FI campaign aimed at undermining local and international confidence in the Ukrainian democracy. Initial assessments by multiple observation teams conclude that this FI campaign did not achieve its aim.¹ Key findings include:

- Russian speakers were a priority audience for accounts employing automation.
- With the exception of the days following major incidents such as the July 2014 downing of Malaysian Air flight MH-17, covert social media influence campaigns appear most active during election periods in Ukraine as well as the days immediately following.
- Along with the use of bot and troll accounts, other tactics included the use of networks of disinformation websites and social media pages, and purported leaks.
- "Meta-trolling" or content designed to be detected and called out as Russian propaganda in order to discredit the information it contains may be a newly emerging tactic which RRM Canada will continue to monitor.

General Observations – Secondary and Primary Sources**Tactics/Strategies**

[3] Reporting from the United States Global Engagement Center (GEC) as well as the Alliance of Democracies (AoD) Transatlantic Commission on Election Integrity notes a high degree of automation observed in social media posts about Ukraine's elections. RRM Canada observed similar automated accounts or bots. In addition to the use of bots, RRM Canada observed that many accounts used a random string of alphanumeric characters as a username. These accounts were mostly created after January 2019 and were posting in the Russian language about the Ukrainian elections. The usernames and young age of these accounts indicates that a computer program was likely used to quickly generate new accounts for use in bot networks. Additionally, RRM Canada notes that the highest degree in automation was observed within communities discussing the Ukrainian elections in the Russian language indicating that Russian speakers were likely a priority target audience.

[4] Historical Twitter based analysis has shown that accounts associated with the Kremlin have been most active following the May 2014 elections. However, tweet volume was much smaller in comparison to the July 2014 downing of Malaysian flight MH-17.² While RRM Canada does not have a database of accounts associated with the Kremlin, within our collection of accounts discussing the 2019 elections,

¹ Previous reporting

² <https://voxukraine.org/longreads/twitter-database/index-en.html>

For Public Release

UNCLASSIFIED
RRM Canada

our team observed a large spike in account creation dates from 2014. Further analysis of account creation dates reveals another spike in January 2019. This spike was most pronounced among accounts posting in the Russian language. This indicates that although far below the level of resources dedicated to deflecting blame away from Russia for the downing of MH-17, covert social media influence campaigns are probably most active during election periods in Ukraine. Our data also indicates a spike in posting activity in the days immediately following the elections however, examination of the posts did not reveal any specific narrative being amplified.

[5] Two tactics which have to date been less frequently reported, were observed much more prominently during the Ukraine elections. These tactics were the purchase or renting of social media accounts and the use of "meta-trolling."

[6] New York Times and the Ukrainian Security Service (SBU) report that Russian intelligence agents had been offering to purchase or rent established social media accounts from Ukrainian citizens for the purposes of spreading divisive content or furthering other Kremlin narratives. Owners of these social media accounts reported that they were unaware they were dealing with Russian intelligence personnel or what purpose their accounts would ultimately serve once sold or rented. The number of accounts purchased by Russian agents remains unknown at this time and description of this tactic stems from a video-taped confession released by the SBU.³ Given the financial and human resources required to find and purchase established social media accounts from citizens willing to sell them, it is unlikely this tactic was widespread during this election and unknown if it will be employed in other FI campaigns.

[7] Finally, Government of Canada (GoC) partners deployed to Ukraine to assist with cyber security during the elections period reported a new meta-trolling technique. In this technique, certain content was designed to be detected as Russian propaganda and publicly called out as such in an effort to discredit the information it contained. While we cannot attribute the employment of this tactic to Russia, it falls within the well-known concept of "reflexive control." This concept, whereby specifically prepared information is conveyed in order to incline an opponent to voluntarily take a certain course of action, has a long history within Soviet and Russian military doctrine.⁴ RRM Canada has no further information or current examples of this technique and we cannot attribute it to any particular actor at this time.

[8] RRM Canada cannot tie the employment of automated accounts or the spread of divisive content to Russia. However, Facebook did shut down thousands of accounts posting about Ukraine which they attributed to Kremlin-linked Internet Research Agency (IRA) and Sputnik News.⁵ Based primarily on this evidence, RRM Canada assesses that the Russian state was likely conducting a disinformation campaign targeting the Ukrainian elections.

Narratives

[9] In addition to observations of automation, reports from the UK Foreign & Commonwealth Office's (FCO) Counter Disinformation Cell note divisive narratives being spread by these automated accounts. AoD notes that much of this content ostensibly⁶ emanated from Russia and, at least for a period in late

³ Previous reporting

⁴ <http://georgetownsecuritystudiesreview.org/2017/02/01/disinformation-and-reflexive-control-the-new-cold-war/>

⁵ Previous reporting

⁶ Alliance for Securing Democracies methodology relies on user selection of location within preference settings.

For Public Release

UNCLASSIFIED
RRM Canada

March,⁷ dominated approximately 13% of the conversation on social media about the Ukrainian elections. Previous RRM Canada reports have noted that divisive content was primarily along the following themes:

- Ukraine was reverting to its Nazi past while chauvinism and xenophobia were current state policy;
- Ukraine was becoming increasingly corrupt and becoming a banana republic.
- Ukraine was not capable of hosting free and fair elections; and
- The illegitimacy of the Ukrainian Orthodox Church was put forward.

[10] While the break of the Ukrainian Orthodox Church from the Moscow patriarch is uniquely Ukrainian, claims of corruption, elections fraud, and otherwise divisive content are common tropes within FI campaigns.⁸ Along with the use of bot and troll accounts, other tactics included the use of networks of disinformation websites and social media pages, and purported leaks.⁹ The Atlantic Council's Digital Forensics Research Lab notes these tactics appear to be common across both foreign and domestic disinformation campaigns targeting elections.¹⁰

On Gender

[11] On the gender dimensions of FI within the Ukrainian elections, RRM Canada observed crudely Photo-shopped, degrading, highly sexualized imagery targeting the most prominent female candidate, Yulia Tymoshenko. RRM Canada cannot attribute any of these images to any specific actor. We note that this imagery dominated our collection of all images related to political candidates for a period in February indicating the possibility of some level of coordinated amplification; however, there are many plausible explanations related to this imagery.

On Diasporas

[12] Lastly, RRM Canada detected and analyzed two multilingual groups discussing the Ukrainian elections in the Ukrainian, Russian and English languages on Twitter. Within these groups, relatively few indications of automated content spreading or accounts assessed to be possible Kremlin trolls were observed. Based on the mix of languages, RRM Canada assesses these communities to likely be Ukrainian diaspora communities from English speaking countries. Based on the lack of automated content spreading within these communities, RRM Canada assesses they were likely not priority target audiences for disinformation campaigns.¹¹

Released: 4 June 2019

Disclaimer: Rapid Response Mechanism Canada team monitors and shares information consistent with Canada's privacy laws and the [Ministerial Direction for Avoiding Complicity in Mistreatment by Foreign Entities](#). The information sharing practices of Global Affairs Canada are subject to review by the Privacy Commissioner, the Information Commissioner of Canada, the Office of the Auditor General and the National Security and Intelligence Committee of Parliamentarians, among others. Nothing in the present document shall be construed as adding any obligation or normative commitment under international or national law for any G7 member.

⁷ Other reports from the Alliance of Democracies did not mention the amount of content possibly emanating from Russia.

⁸ As noted within research conducted by the Atlantic Council's Digital Forensics Research Lab.

⁹ Previous reporting

¹⁰ As presented by DFR Lab.

¹¹ Previous reporting

For Public Release

OPEN DATA ANALYSIS REPORT

UNCLASSIFIED
RRM CANADA

ALBERTA ELECTION ANALYSIS

PURPOSE

This report analyses open source data gathered in the lead-up to the provincial elections in Alberta held on April 16, 2019. Its purpose was to identify any emerging tactics in foreign interference and draw lessons learned for the Canadian general elections scheduled to take place in October 2019. Prepared in support of the [G7 Rapid Response Mechanism](#) (RRM), the report was penned by RRM Canada. The RRM is mandated to strengthen G7 coordination to identify and respond to diverse and evolving threats to G7 democracies, including through sharing information and analysis, and identifying opportunities for coordinated response.

KEY FINDINGS

Based on primary and secondary research, RRM Canada concludes that there were very likely **no significant foreign interference campaigns** targeting the Alberta election in the online space in April 2019. However, coordinated inauthentic activity was detected:

- RRM Canada identified accounts that demonstrated coordinated inauthentic behaviour. RRM Canada judges the activity is very unlikely to comprise one third of the online conversation as reported by [Press Progress on April 11, 2019](#).
- RRM Canada identified cases of social media accounts, which were likely inauthentic, coordinated behaviour¹ around online discussions about the Alberta election. However, the majority of these accounts were very likely not foreign.
- RRM Canada identified known national far-right and hate group actors who have previously disseminated material, using similar tactics as known malign foreign actors.
- RRM identified accounts tied to lobbying groups that were unaffiliated with a political party spreading disinformation online in the run-up to the Alberta election.
- The Alberta election provides an example of a situation where there may be evidence of coordinated inauthentic behaviour undertaken by Canadian actors, making the identification of foreign interference more difficult.

Alberta Election Findings

[1] RRM Canada reviewed social media data to search for obvious cases of coordinated, inauthentic behaviour with the objective of identifying any potential foreign activities. Based on available information, it is very unlikely there was any foreign interference. The two largest components of the graph are made up of supporters of the former Premier Notley and Premier Kenney, as expected in an election campaign [Annex A].

[2] RRM Canada assesses that none of the major communities taking part in online conversations related to the elections are driven by foreign interference. The presence of automated inauthentic activities does not appear central or crucial to the overall conversation or activity.

¹ Scale of Estimative Language: Almost No Chance – [0 – 10]; Very Unlikely/Very Improbable – [11 – 29]; Unlikely/Improbable – [30 – 39]; Roughly Even Chance – [40 – 59]; Likely/Probable – [60 – 69]; Very Likely/Very Probable – [70 – 89]; Almost Certainly – [90 – 100]

For Public Release

OPEN DATA ANALYSIS REPORT

UNCLASSIFIED
RRM CANADA

[3] RRM Canada's findings stand opposite to the [April 11, Press Progress report](#), which claimed that a third of accounts talking about the Alberta election were bots. RRM Canada's findings, using multiple tools and methods, judges that the online activity is very unlikely to comprise one third of bots. The article appears to rely only on the online tool mentionsmap as a metric for "bot activity", which is not a proper means of assessment for inauthentic account behaviour or bot activity. RRM Canada therefore does not support the findings articulated in the Press Progress Report.

[4] RRM Canada identified communities that **demonstrated a suspicious account creation pattern that is indicative of troll or bot activity**. Recent spikes in account creation suggest the presence of accounts developed for a specific purpose; however, **the community was determined to very likely be domestic**, as it was mainly comprised of supporters of the United Conservative Party (UCP). A second small community was identified as supporters of the People's Party of Canada, which had similar suspicious patterns of account creation. This pattern was not identified within communities of supporters of the Alberta Liberal Party or Alberta New Democratic Party. The overall number of accounts is a small percentage of a larger collection [Annex B]. This highlights a key point, namely that **domestic actors are also emulating the tactics used by foreign actors, within the context of provincial elections. This behaviour will make it increasingly difficult to distinguish national from foreign interference efforts in the upcoming Federal election.**

[5] The RRM identified a small group of anonymous accounts pushing a pro-separation movement in Alberta and the Prairies. Though Alberta has an official separatist party, <https://albertaindependence.ca/>, these accounts do not appear affiliated with this movement. Creating false separatist movements or amplifying domestic ones is a known tactic in foreign interference. Though unaffiliated, at this time, RRM Canada cannot tie this small group of accounts to any foreign entity.

[6] In its review of the data of this election, RRM Canada found no evidence supporting a broad, coordinated campaign to influence the Alberta election. **RRM Canada assesses that automated inauthentic behaviour and trolling activities are very likely domestic in nature;**

Released: May 1, 2019

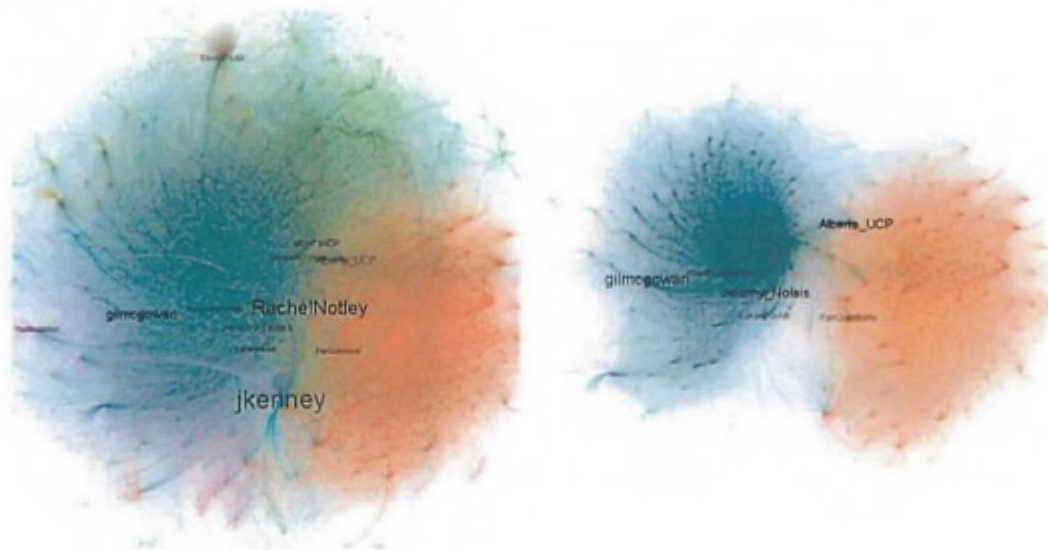
Disclaimer: G7 Rapid Response Mechanism Canada (RRM Canada) monitors and shares information consistent with Canada's privacy laws and the [Ministerial Direction for Avoiding Complicity in Mistreatment by Foreign Entities](#). The information sharing practices of Global Affairs Canada are subject to review by the Privacy Commissioner, the Information Commissioner of Canada, the Office of the Auditor General and the National Security and Intelligence Committee of Parliamentarians, among others. Nothing in the present document shall be construed as adding any obligation or normative commitment under international or national law for any G7 member.

OPEN DATA ANALYSIS REPORT

UNCLASSIFIED
RRM CANADA

Annex A

This Annex is a visual representation of RRM Canada's data collection illustrating a high level of normality in the online conversation related to the Alberta provincial election. The analysis of activity would have been noteworthy for RRM Canada if there were other communities that rivaled the main political communities in size, but were predominately unknown actors, or actors from another geographical location.

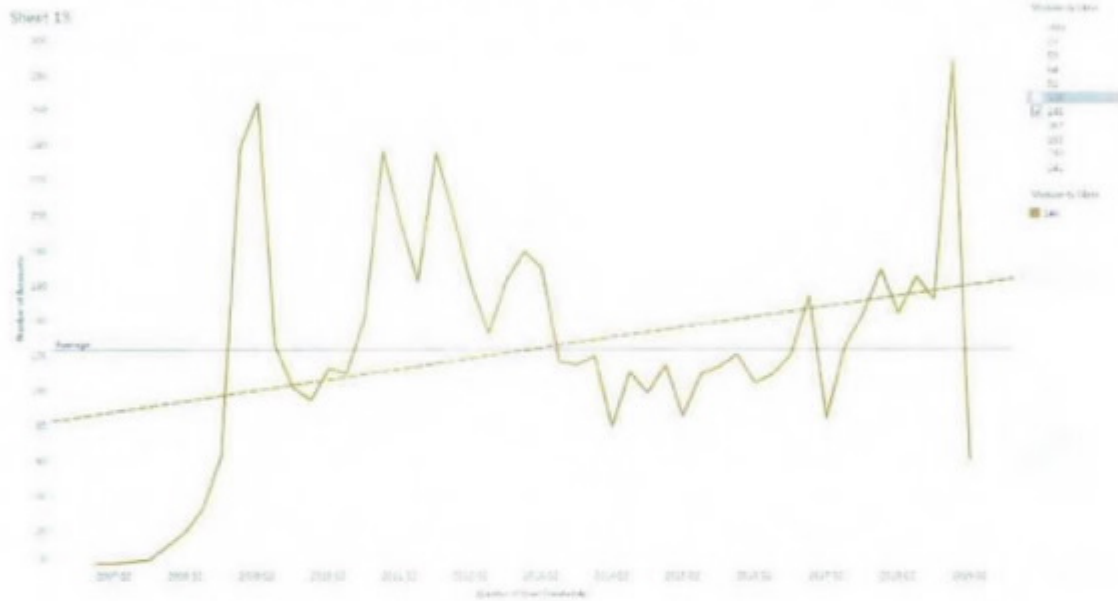


OPEN DATA ANALYSIS REPORT

UNCLASSIFIED
RRM CANADA

Annex B

A review of the account creation dates of accounts in the community of UCP supporters. The size of the final spike is an indicator of inauthentic activity. One indicator of bot activity is a large number of recently-created accounts. In this case, a large spike in accounts created in Q1 2019 is suggestive of inauthentic activity by either automated accounts or anonymous accounts. This combined with a qualitative evaluation of the accounts by RRM Canada, as well as their posting behaviours and the social network analysis; these are indications of likely inauthentic behaviour.



For Public Release



ETHICAL AND METHODOLOGICAL FRAMEWORK FOR OPEN SOURCE DATA MONITORING AND ANALYSIS

Rapid Response Mechanism Canada

Centre for International Digital Policy

Global Affairs Canada

June 2019

ETHICAL AND METHODOLOGICAL FRAMEWORK FOR OPEN SOURCE DATA MONITORING AND ANALYSIS¹

Contents

Purpose	2
Background and Mandate	2
Challenges and Obstacles	3
Thresholds and Protocols	3
Methodology and Tools	4
Human Rights Approach	5
Privacy	5
Freedom of Expression	5
Gender Equality	6
Principles and Ethical Considerations	6
Transparency and Accountability	6
Internal Oversight and Partnerships	6

¹ This document is meant to be iterative and sensitive to the evolving nature of digital technologies, foreign threats, policy orientation, and social and political issues. In developing this document several stakeholders have already been consulted, including multiple divisions at Global Affairs Canada, various other departments in the Government of Canada, the Oxford Internet Institute, and others.

For Public Release

Purpose

Contemporary international relations theory and practice must consider the rapidly evolving digital information ecosystem. This ecosystem, including social media platforms and their content ranking algorithms, is creating new opportunities for economic growth and connectivity, while also presenting a range of new challenges for foreign policy. The threat from malign foreign actors, who seek to leverage aspects of this ecosystem for nefarious activities that are detrimental to our democratic systems of governance, is among the most pressing issues requiring attention by democracies such as Canada. Governments are developing new capacities to better understand this threat, including by harnessing open source data monitoring and analytical tools and approaches.

The purpose of this framework is to outline ethical and methodological principles and guidelines for open source data monitoring and analysis undertaken by Rapid Response Mechanism Canada (RRM Canada). These open source data activities support the G7 Rapid Response Mechanism (RRM) – an initiative aimed at defending G7 democracies from foreign threats as well as Government of Canada efforts aimed at safeguarding its own democratic institutions and processes, including its general elections. The need for such a framework stems from the following three needs, among others:

- 1) Anchoring these relatively new activities in an existing policy, legal, and regulatory context.
- 2) Ensuring that the activities respect and reinforce human rights and freedoms.
- 3) Providing transparency and accountability to Canadians and the G7.

Background and Mandate

Supported by a team of policy and data analysts, RRM Canada is housed at Global Affairs Canada in the Centre for International Digital Policy. The RRM was announced at the G7 Charlevoix Summit in 2018 and re-affirmed at the G7 ministerial meeting in Dinard, France, in 2019. Led by Canada on an ongoing basis, its mandate is “to strengthen coordination to identify and respond to diverse and evolving threats” to G7 democracies.² More specifically, the foreign threats that G7 members committed to confront seek to undermine democratic institutions and processes through “coercive, corrupt, covert or malicious means.”³

While the threat landscape covered by the RRM is broad, disinformation in digital context figures prominently.⁴ In the lead up to the RRM’s announcement, Foreign and Security Ministers recognised the threat posed by “acts or measures by foreign actors with the malicious intent of undermining trust in the independent media, manipulating public discourse, and violating privacy,” by including these activities in the Toronto Commitment, among other key illustrative examples.

Additionally, RRM Canada supports the [Government of Canada efforts to safeguard the 2019 general elections](#). As part of the [Security and Intelligence Threats to Elections \(SITE\) Task Force](#), RRM Canada works with Canada’s Security and Intelligence organisations “to prevent covert, clandestine, or criminal activities from influencing or interfering with the electoral process in Canada.” The other members of

² Charlevoix Commitment

³ Toronto Commitment

⁴ Digital context in this note refers to the overarching network or framing environment generated by the digital information ecosystem.

For Public Release

the Task Force are: the Communications Security Establishment (CSE), Canadian Security Intelligence Services (CSIS), and the Royal Canadian Mounted Police (RCMP).

- The aim of RRM Canada's open source data activities is to support the RRM mandate to defend democracies, and help safeguard Canada's 2019 general elections, by better understanding foreign threats in the digital context, shining light on them, and recommending effective response options.

Challenges and Obstacles

Among the central challenges in addressing foreign interference in the digital ecosystems of G7 democracies is determining the foreign nature of the online activities being undertaken. This challenge reflects the limitations of employing open and publicly available information from social media platforms for analytical purposes. This is because foreign states and state proxies exploit the anonymity offered by digital platforms, "weaponise" elements of the digital information ecosystem, and continuously adapt to strategies aimed at stopping them. While anonymity can be integral to facilitating sensitive discussions online (where those discussions are discouraged or are otherwise dangerous to individuals engaging in them), it is also the same mechanism exploited by foreign actors to conduct coercive, corrupt, covert, or malicious activities.

Perhaps the most problematic aspect of distinguishing foreign interference from organic domestic debate is that foreign actors target domestic audiences with content that may resonate with the audiences' pre-existing opinions and worldviews. This targeting, often undertaken clandestinely, involves a foreign actor creating content that has been designed to sow discord or exploit existing societal differences in the domestic population. When this foreign content is received by domestic audiences, it then can be amplified further either wittingly or unwittingly. This sequence intertwines foreign and domestic narratives in ways that are difficult to untangle. Foreign actors may also coerce or induce Canadians to promote a given narrative, but these overtures are often hidden and difficult to substantiate.

The challenge of separating foreign interference from domestic engagement raises the potential of inadvertently affecting the enjoyment of human rights and freedoms of Canadians, in particular, freedom of expression and privacy rights. To avoid this situation, open source data activities conducted by RRM Canada are subject to clear thresholds and protocols for monitoring, analysis, and information sharing.

- RRM Canada thresholds and protocols ensure that its open source data monitoring and analytical activities fall under the RRM mandate, safeguard and reinforce human rights and freedoms of Canadians, comply with relevant legal and regulatory provisions, and meet high ethical standards.

Thresholds and Protocols

RRM Canada has developed thresholds for what are considered coercive, corrupt, covert or malicious activities as well as protocols for open source data monitoring and information sharing activities. To be the subject of RRM Canada monitoring activities, an account or network of coordinated accounts must display a number of characteristics outlined in the RRM Canada methodology. The methodology sets high thresholds established in cooperation with leading experts; computational social scientists; and

For Public Release

security, intelligence, and law enforcement organisations. Additional factors for open source data activities include concurrence with secondary sources and significant impact on public discourse.

These thresholds inform RRM Canada's monitoring activities, including its approach to analysing suspicious accounts and networks associated with foreign interference. These thresholds are not impacted by the accuracy or perceived acceptability of content that any given account or network disseminates. In the event that a foreign connection cannot be established within a reasonable period, monitoring activities cease, and no data is retained. However, in cases when suspicious activities may potentially meet criminal or national security thresholds, insight is shared with security, intelligence, and law enforcement organisations. When activities may potentially contravene the Canada Elections Act, the Commissioner of Canada Elections will be notified by RRM Canada. These organisations independently determine whether or not an investigation is required pursuant their respective mandates and legislative frameworks.

Furthermore, in January 2019 the Government of Canada announced a number of new measures to protect the 2019 general election, including the [Critical Elections Incident Public Protocol](#). This Protocol lays out a clear and impartial process by which Canadians may be notified of a threat to the integrity of the elections that occur within the writ period.

Methodology and Tools

RRM Canada examines trends, anomalies, and emerging narratives in online conversations across the digital information ecosystem pertaining to potentially divisive issues and public political actors that could be exploited by malign foreign actors. By observing baseline structures of what are considered normal conversations surrounding issues, as they evolve over time, it is possible to identify abnormalities that may indicate a concerted foreign information operation. RRM Canada examines multiple indicators of coordinated foreign interference campaigns, some of which are indicative of foreign coercive, corrupt, covert, or malicious behaviour.

Caution is exercised in divulging detailed indicators pertaining to threshold-setting in order to prevent malign foreign actors from developing counter strategies. Nevertheless, indicators for covert behaviour can include artificial or inauthentic amplification of narratives, for example. Narratives can be amplified by employing different tactics including bots, botnets, and trolls. RRM Canada uses indicators to identify bot and troll activity, as well as those to identify the foreign nature of suspicious activities. All determinations are made based on a confidence scale and identified using estimative language.

To monitor and analyse potential foreign interference, RRM Canada uses tools that are publicly available. The combination of these tools is not released in order to prevent malign foreign actors from developing strategies in response. To complement their use, RRM Canada also experiments with open source data modeling, natural language processing, social network analysis, machine learning and algorithms all of which process only openly available public data. Any automated outcomes these technologies render can be meaningfully explained.

- The methodologies and tools employed by RRM Canada are consistent with those adopted and employed by various actors in the private and public sectors as well as non-government organisations and advocacy groups. This is in line with a growing awareness of the digital information ecosystem as an important political, social, economic, and cultural space.

For Public Release

Human Rights Approach

Leading to the Charlevoix announcement of the RRM, all G7 Foreign and Security Ministers endorsed a strategic approach to responding to foreign threats that is consistent with universal human rights and fundamental freedoms. Canada is committed to respecting its international commitments and obligations including being a party to the [International Covenant on Civil and Political Rights](#). In Canada, the [Charter of Rights and Freedoms](#) protects a number of rights and freedoms, including those most evidently impacted by foreign interference in digital contexts, namely: privacy rights, freedom of expression, and the right to equality.

Privacy

The subject of RRM Canada open source data monitoring and analysis is limited to publicly available data. RRM Canada monitors, analyses, and shares information in a manner that is consistent with Canada's privacy laws, the [Access to Information Act](#), and the [Ministerial Direction for Avoiding Complicity in Mistreatment by Foreign Entities](#). The information sharing practices of Global Affairs Canada to which RRM Canada adheres are subject to review by multiple actors, including: the Privacy Commissioner, the Information Commissioner of Canada, the Office of the Auditor General and the National Security and Intelligence Committee of Parliamentarians. All RRM Canada analysts are required to complete the [Access to Information and Privacy Fundamentals](#) course, in order to strengthen the understanding of what is considered personal information and how best to protect it.

Moreover, RRM Canada takes care to limit unintended harms and therefore, is additionally guided by firm ethical and principled considerations to facilitate responsible practices for handling personal data, even if it is publicly available. The focus of RRM Canada's open source data monitoring and analysis is trends, tactics, and strategies undertaken by malign foreign actors. The questions RRM Canada seeks to answer include: How do foreign states and their proxies exploit online discussions? What tactics do they employ for coercive, corrupt, covert or malicious activities? How do they leverage tactics such as artificial or inauthentic amplification to manipulate online discussions and what type of coordination strategies do they employ? How do these tactics and strategies evolve over time?

Freedom of Expression

RRM Canada seeks to identify foreign activities with a coercive, corrupt, covert, or malicious dimension, which attempt to sway public opinion to undermine Canadian democracy. To mitigate risks related to the difficulty of separating foreign and domestic activities and unwittingly impinging upon the freedom of expression of Canadians, RRM Canada:

- Focuses on the structure and context of conversations, as opposed to the content, to understand what indicators may signal foreign interference.
- Relies on established open source data monitoring protocols that set out thresholds for foreign activity and guide information sharing with Canadian security, intelligence, and law enforcement organisations as well as the Commissioner of Canada Elections.
- Excludes personally identifiable information from public reports. In certain cases such as national security considerations shares such information with responsible security organizations.
- Does not undertake active measures or engage in any way with content creators or those sharing content.

For Public Release

Gender Equality

RRM Canada adopts a Gender-Based Analysis Plus (GBA+) approach as it undertakes open source data monitoring and analytical activities. Malign actors target, exploit, and sometimes co-opt women and marginalized groups and issues in their activities to undermine social cohesion. Understanding how these processes occur and how they differentially impact these groups is crucial to both countering foreign interference and protecting human rights.

The methodological approach is also informed by academics and civil society organisations who are experts on gender and intersectional identity issues. Several of these interlocutors are conducting research that directly supports the RRM Canada mandate. Finally, all RRM Canada analysts are required to take the [Gender-Based Analysis Plus \(GBA+\) online course](#) and integrate the approach systematically into their work.

Principles and Ethical Considerations

RRM Canada has incorporated principles and ethical considerations beyond the existing legal and policy considerations to enhance its approach to open source data monitoring and analysis that is effective in protecting Canadians, while limiting undue and unintended harms.

Transparency and Accountability

RRM Canada is committed to working in a manner that prioritizes transparency and openness. Our commitment is reflected in the following actions:

- Treatment of open and publicly available data *only*.
- Focus on tactics, strategies, and trends.
- Use of publically available tools, explainable algorithms and other technologies.
- Ethical and human rights respecting approach to monitoring and analysis.
- Established thresholds and information sharing protocols with Government of Canada organisations and G7 partners.
- Systematic engagement with a wide network of experts, academics, and civil society actors.

Internal Oversight and Partnerships

RRM Canada has developed an internal review mechanism to ensure analytical accuracy and robustness. Its multi-disciplinary team of social scientists, data experts and policy analysts allows for the agility and capacity to address evolving threats, while incorporating broader perspectives into its open source data activities. RRM Canada frequently engages in challenge functions or a peer-review process within the Government of Canada. This allows final conclusions to be determined through a rigorous process whereby results are challenged by fellow analysts and possibilities of cognitive and other bias are reduced. Collaboration beyond the Government of Canada is essential for developing innovative open source data monitoring and analytical capacity. RRM Canada relies on a growing community of experts which includes representatives from other governments, academia, civil society, and non-governmental organisations.



Intelligence Note
Note de renseignement

TOP SECRET//CEO

Dissemination: GAC; PCO; NSIA; PS

India

Synopsis:

The report relates to the efforts of an Indian official in Canada to engage in potential political interference, including possible actions against an MP for their perceived 'anti-India' positions.

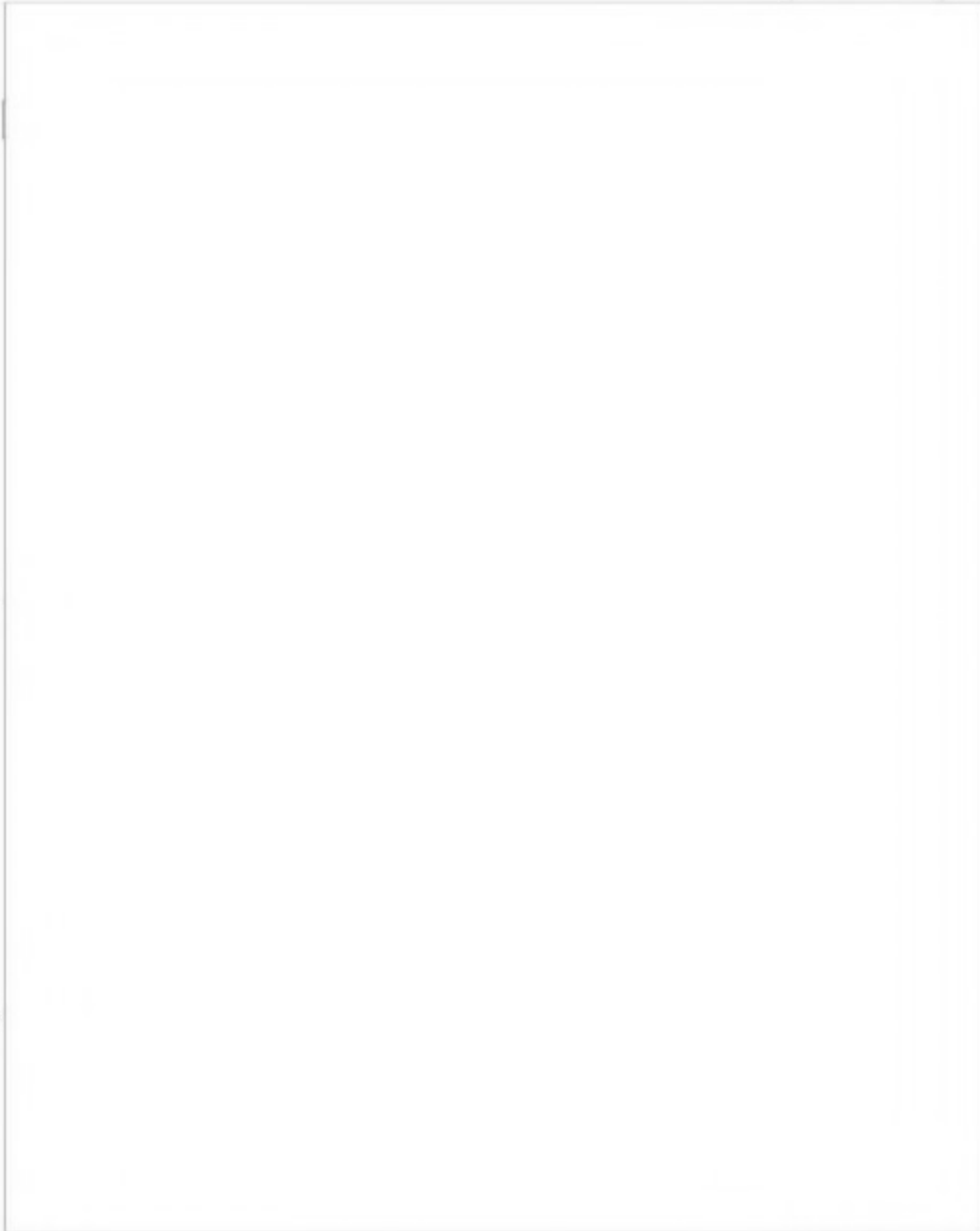
Source:

Information:

1.

For Public Release

TOP SECRET//CEO

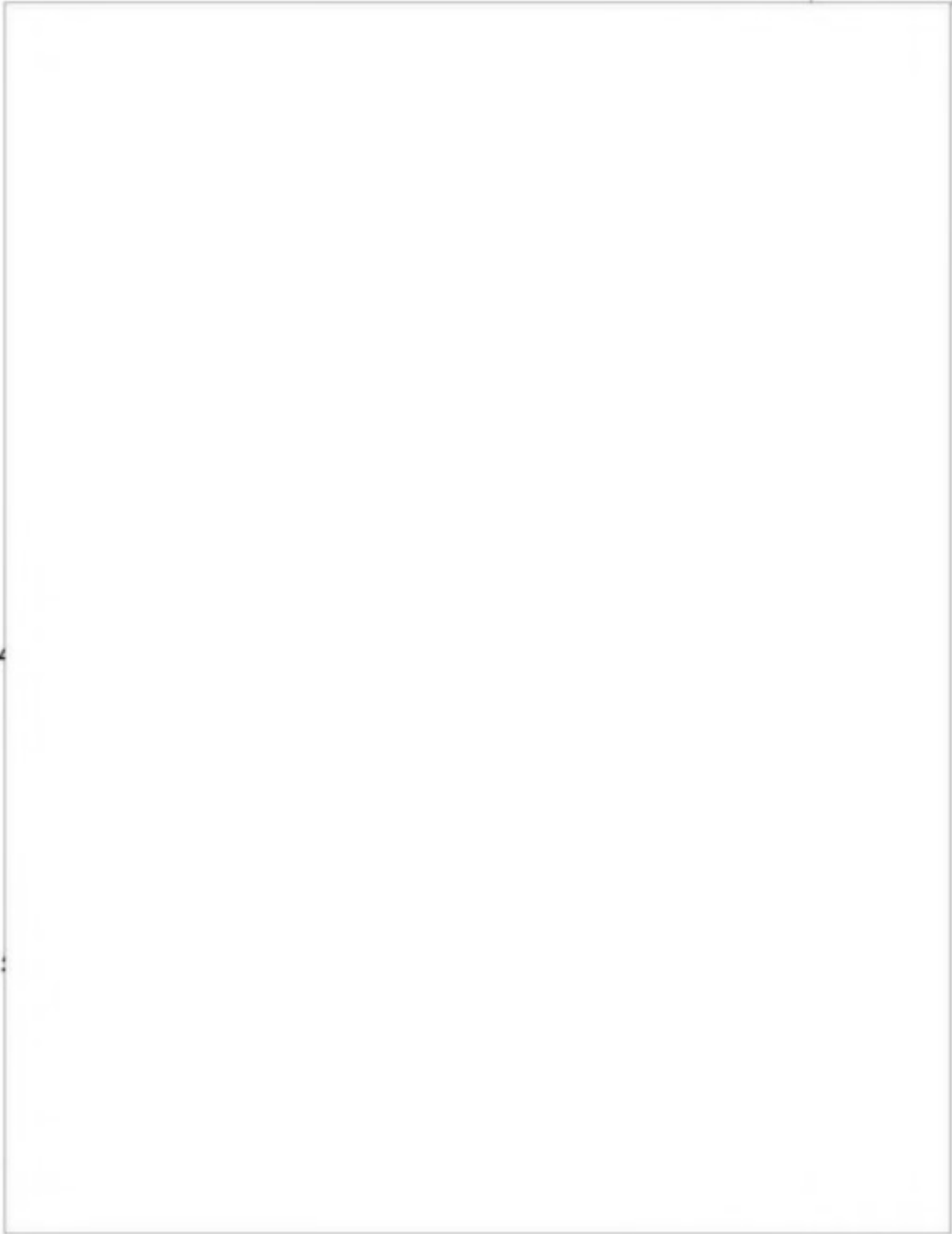


2.

3.

For Public Release

TOP SECRET//CEO



Page 3 of 7

For Public Release

TOP SECRET//CEO

6.

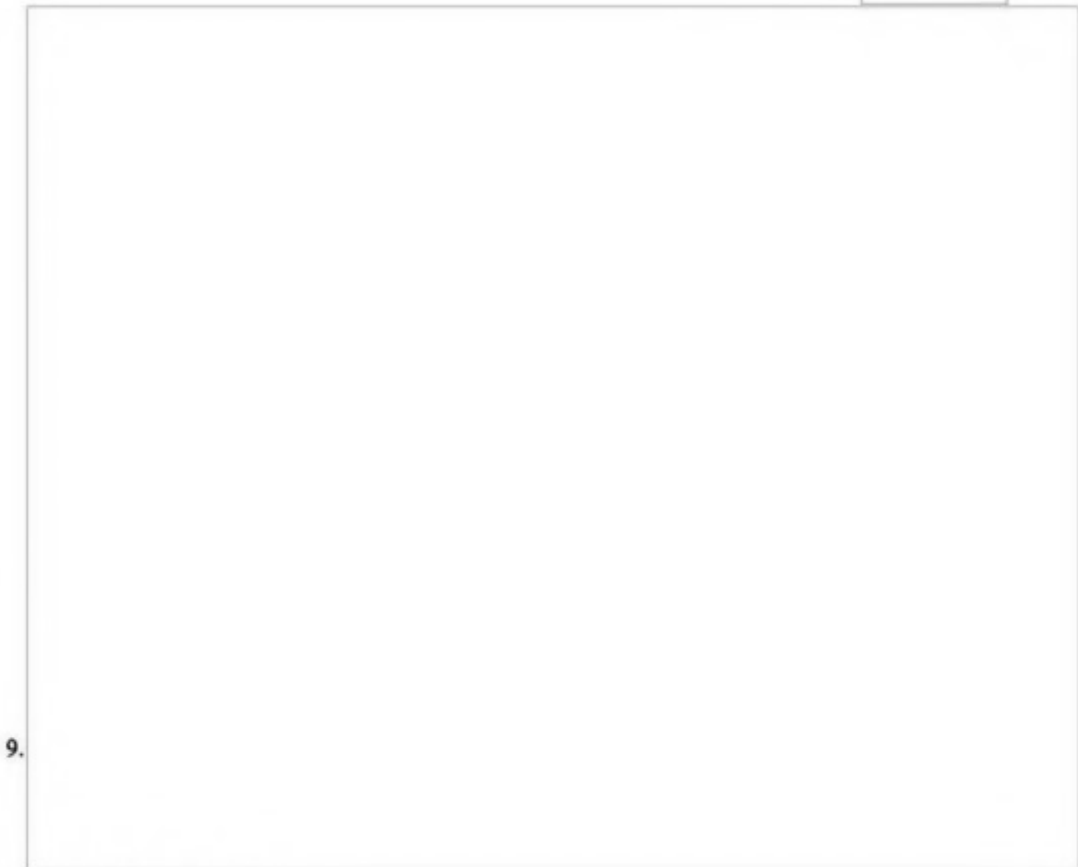
7.

8.

Page 4 of 7

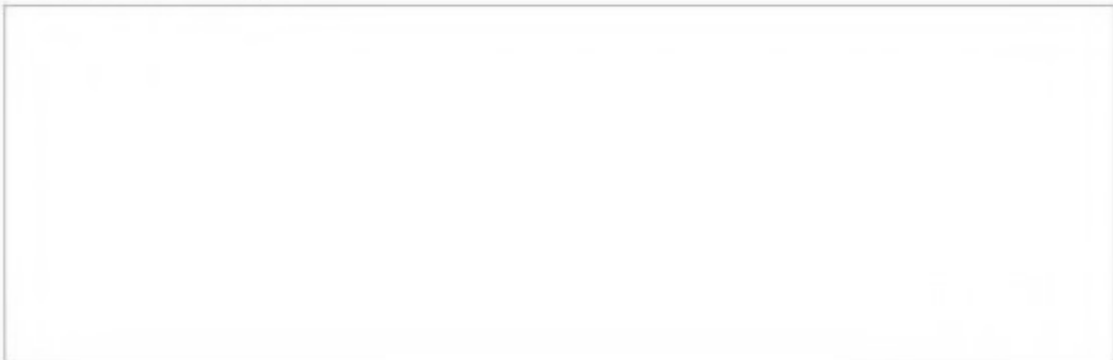
For Public Release

TOP SECRET//CEO



9.

CSIS Context / Analysis:



TOP SECRET//CEO

[Redacted]

[Redacted]

Your comments are essential to ensure the relevance of CSIS Intelligence Notes being provided to your department/agency.

[Redacted]

CAVEAT

This document constitutes a record which may be subject to exemption under the *Access to Information Act or the Privacy Act*. The information or intelligence must not be disclosed or used as evidence without prior consultation with the Canadian Security Intelligence Service.

This document is the property of the Canadian Security Intelligence Service (CSIS). It is loaned to your agency / department in confidence, for internal use only. It must not be reclassified or disseminated, in whole or in part, without the consent of the originator. If you are subject to freedom of information or other laws which do not allow you to protect this information from disclosure, notify CSIS immediately and return the document.

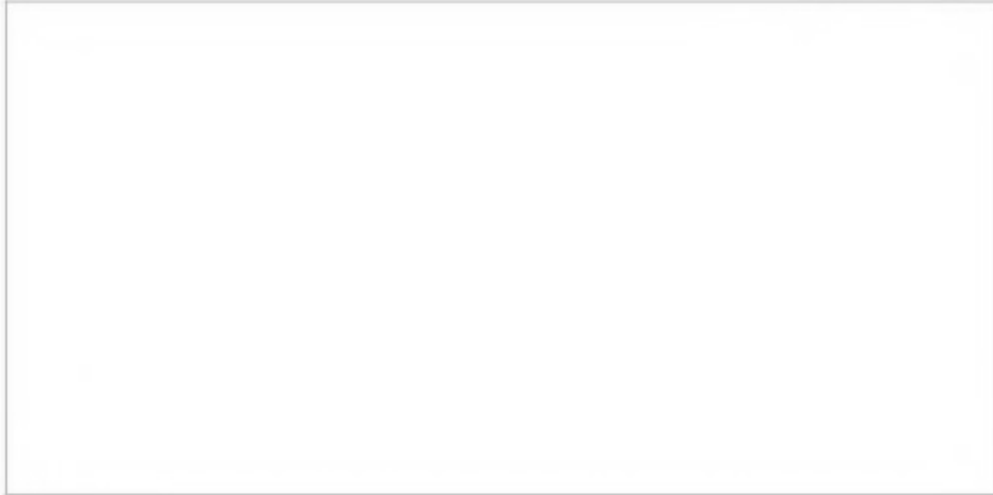
This document is the property of the Canadian Security Intelligence Service and may constitute "special operational information" as defined in the *Security of Information Act*. It is loaned to your agency / department in confidence. It must not be reclassified or disseminated, in whole or in part, without the consent of the originator.

Glossary of terms:

[Redacted]

For Public Release

TOP SECRET//CEO



Page 7 of 7



Intelligence Report
Bulletin de Renseignements

SECRET//CEO

Dissemination: GAC-DM; PCO-NSIA, Foreign and Defence Policy Advisor to the PM and Assistant Secretary to Cabinet S&I, Democratic Institutions-DM; CSE-Chief; PS-DM

China

Synopsis:

Source:

Information:

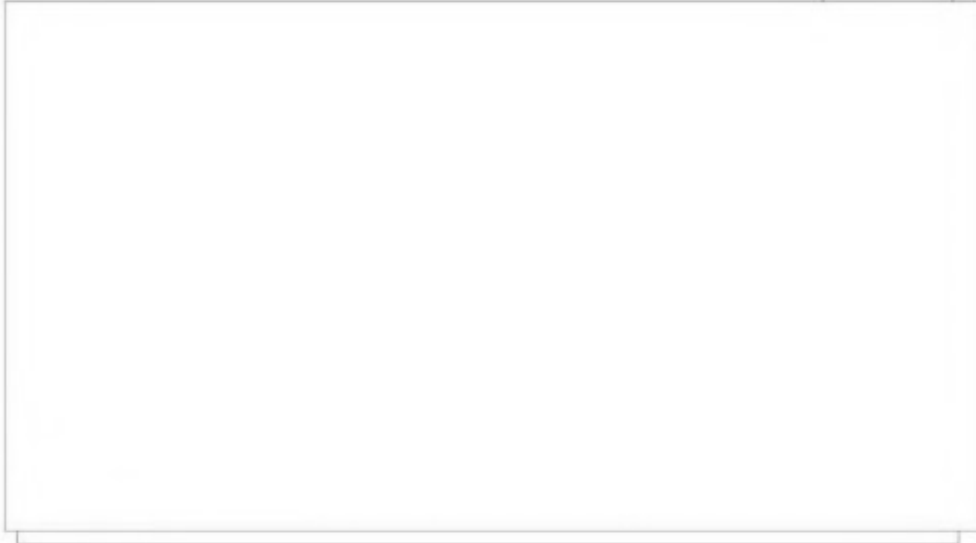
1.

2.

For Public Release

SECRET//CEO

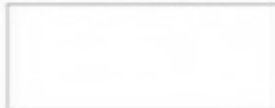
3.



CSIS comment:



Your comments are essential to ensure the relevance of CSIS Intelligence Reports being provided to your department/agency.



For Public Release

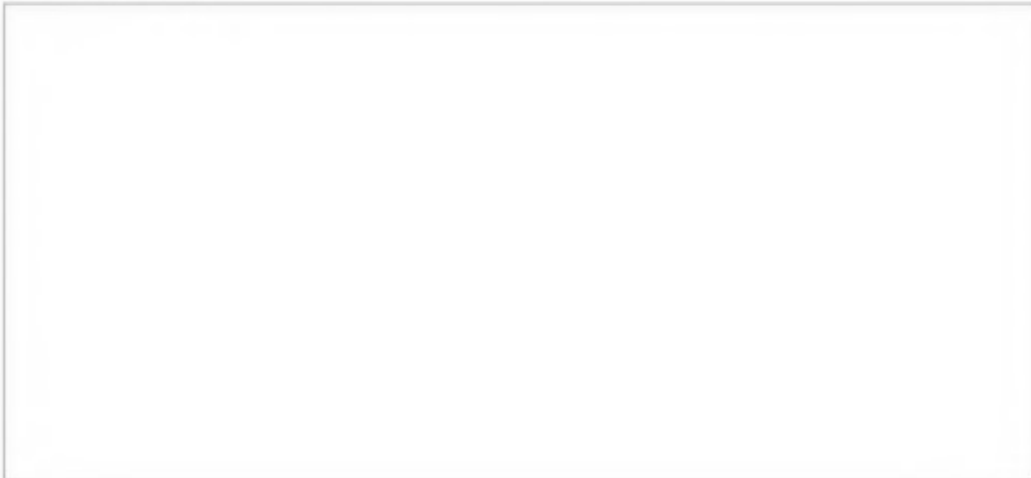
SECRET//CEO

CAVEAT

This document constitutes a record which may be subject to exemption under the Access to Information Act or the Privacy Act. The information or intelligence must not be disclosed or used as evidence without prior consultation with the Canadian Security Intelligence Service.

This document is the property of the Canadian Security Intelligence Service (CSIS). It is loaned to your agency / department in confidence, for internal use only. It must not be reclassified or disseminated, in whole or in part, without the consent of the originator. If you are subject to freedom of information or other laws which do not allow you to protect this information from disclosure, notify CSIS immediately and return the document.

This document is the property of the Canadian Security Intelligence Service and may constitute "special operational information" as defined in the Security of Information Act. It is loaned to your agency / department in confidence. It must not be reclassified or disseminated, in whole or in part, without the consent of the originator.

Glossary of terms:

Page 3 of 3



Intelligence Report Bulletin de Renseignements

SECRET//CEO

Dissemination: GAC-DM; PCO-; CSE-Chief; PS-DM

China

Synopsis:

Source:

Information:

1.

2.

For Public Release

SECRET//CEO

3.

CSIS comment:

Your comments are essential to ensure the relevance of CSIS Intelligence Reports being provided to your department/agency.

For Public Release

SECRET//CEO

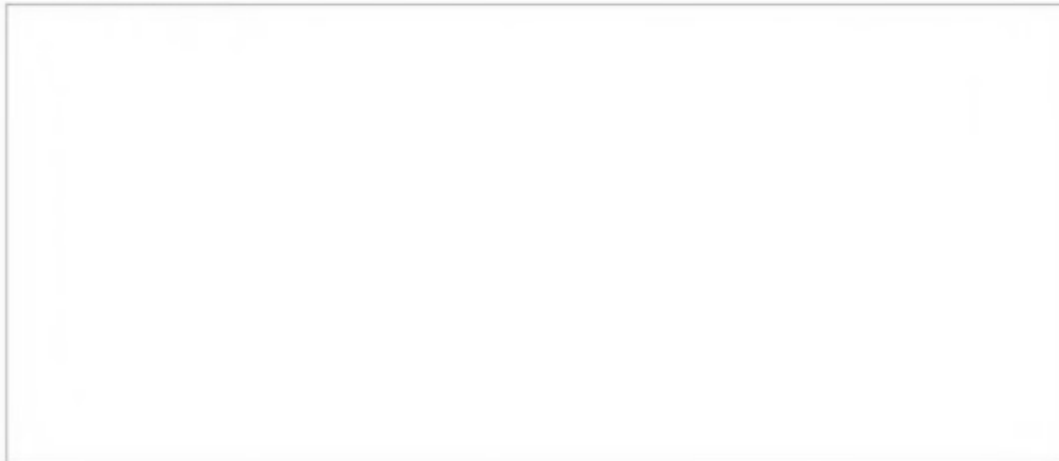
CAVEAT

This document constitutes a record which may be subject to exemption under the *Access to Information Act* or the *Privacy Act*. The information or intelligence must not be disclosed or used as evidence without prior consultation with the Canadian Security Intelligence Service.

This document is the property of the Canadian Security Intelligence Service (CSIS). It is loaned to your agency / department in confidence, for internal use only. It must not be reclassified or disseminated, in whole or in part, without the consent of the originator. If you are subject to freedom of information or other laws which do not allow you to protect this information from disclosure, notify CSIS immediately and return the document.

This document is the property of the Canadian Security Intelligence Service and may constitute "*special operational information*" as defined in the *Security of Information Act*. It is loaned to your agency / department in confidence. It must not be reclassified or disseminated, in whole or in part, without the consent of the originator.

Since disclosure of information contained in this document might be injurious to national security, the Canadian Security Intelligence Service (CSIS) objects to its disclosure before a court, person or any body with jurisdiction to compel its production or disclosure. The CSIS may take all steps pursuant to the *Canada Evidence Act* or any other legislation to protect this information or intelligence from production or disclosure."

Glossary of terms:

Page 3 of 3



Intelligence Report
Bulletin de Renseignements

SECRET//CEO

[Redacted box]

Dissemination: GAC-DM; PCO [Redacted box]; CSE-Chief; PS-DM

[Redacted box]

China

Synopsis:

[Redacted box]

Source:

Information:

1.

[Redacted box]

2.

For Public Release

SECRET//CEO

3.

CSIS comment:

Your comments are essential to ensure the relevance of CSIS Intelligence Reports being provided to your department/agency.

CAVEAT

This document constitutes a record which may be subject to exemption under the *Access to Information Act or the Privacy Act*. The information or intelligence must not be disclosed or used as evidence without prior consultation with the Canadian Security Intelligence Service.

This document is the property of the Canadian Security Intelligence Service (CSIS). It is loaned to your agency / department in confidence, for internal use only. It must not be reclassified or disseminated, in whole or in part, without the consent of the originator. If you are subject to freedom of information or other laws which do not allow you to protect this information from disclosure, notify CSIS immediately and return the document.

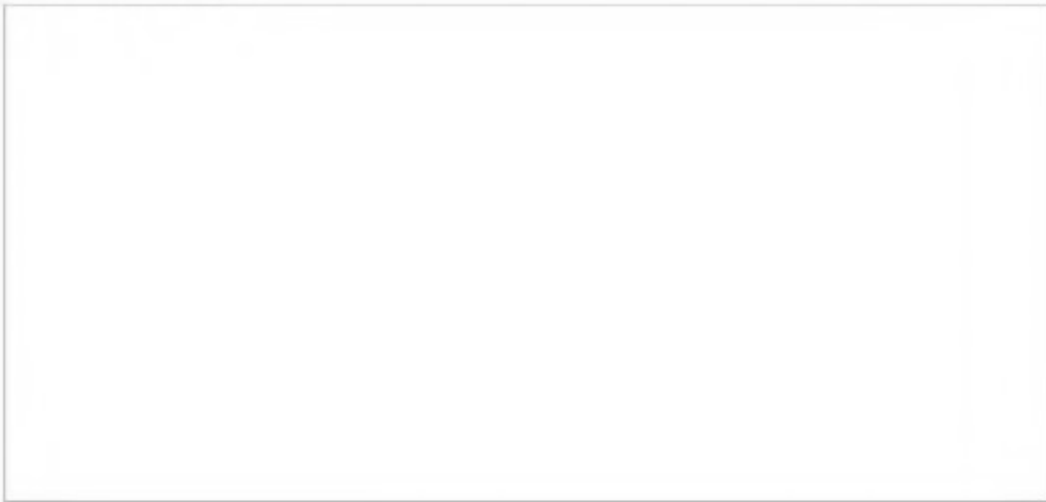
This document is the property of the Canadian Security Intelligence Service and may constitute "*special operational information*" as defined in the *Security of Information Act*. It is loaned to your agency / department in confidence. It must not be reclassified or disseminated, in whole or in part, without the consent of the originator.

For Public Release

SECRET//CEO



Glossary of terms:





Intelligence Report
Bulletin de Renseignements

SECRET//CEO

[Redacted box]

Dissemination: GAC; PCO; CSE; PS; SITE - [Redacted box]

[Redacted box]

China

Synopsis:

[Redacted box]

Source:

Information:

1.

[Redacted box]

2.

For Public Release

SECRET//CEO

[Redacted]

Source comment:

[Redacted]

CSIS comment:

[Redacted]

Your comments are essential to ensure the relevance of CSIS Intelligence Reports being provided to your department/agency.

[Redacted]

For Public Release

SECRET//CEO

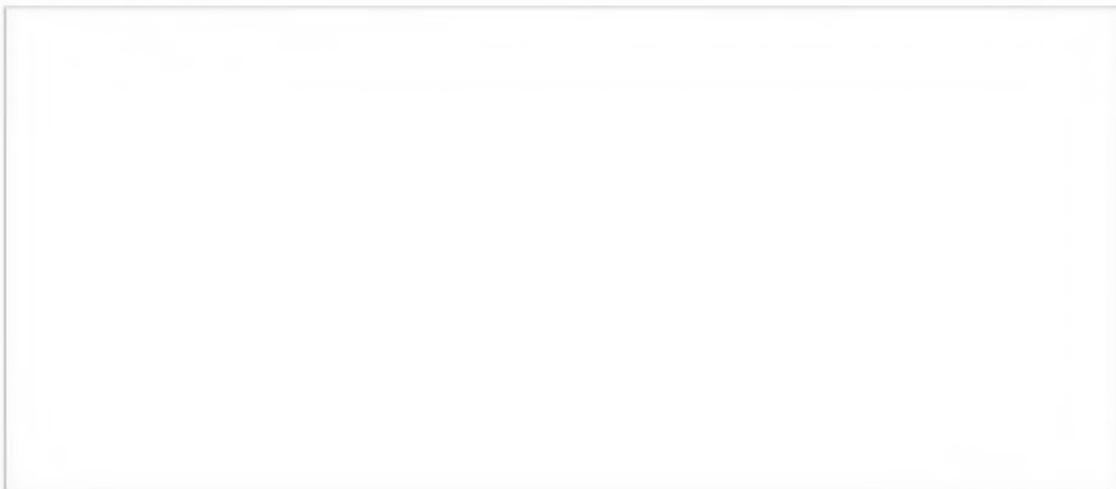
CAVEAT

This document constitutes a record which may be subject to exemption under the *Access to Information Act* or the *Privacy Act*. The information or intelligence must not be disclosed or used as evidence without prior consultation with the Canadian Security Intelligence Service.

This document is the property of the Canadian Security Intelligence Service (CSIS). It is loaned to your agency / department in confidence, for internal use only. It must not be reclassified or disseminated, in whole or in part, without the consent of the originator. If you are subject to freedom of information or other laws which do not allow you to protect this information from disclosure, notify CSIS immediately and return the document.

This document is the property of the Canadian Security Intelligence Service and may constitute "*special operational information*" as defined in the *Security of Information Act*. It is loaned to your agency / department in confidence. It must not be reclassified or disseminated, in whole or in part, without the consent of the originator.

Since disclosure of information contained in this document might be injurious to national security, the Canadian Security Intelligence Service (CSIS) objects to its disclosure before a court, person or any body with jurisdiction to compel its production or disclosure. The CSIS may take all steps pursuant to the *Canada Evidence Act* or any other legislation to protect this information or intelligence from production or disclosure."

Glossary of terms:

Page 3 of 3

For Public Release

Some intel re: the Gould RITE brief
 + Election Protocol
 brief/TTX

SECRET**McLaughlin, Andrew J (Andy)****Subject:** FW: New Heads up - threat briefing for the Panel - June 20**Classification: SECRET**

From: Tayyeb, Alia C [mailto: [redacted]@pco-bcp.gc.ca]
Sent: June-17-19 5:30 PM
To: Wilczynski, Artur; [redacted]; [redacted]; King, Lyall; [redacted]
 [redacted]; Denham, Tara
Cc: [redacted] (PCO); [redacted] (PCO); [redacted] (PCO); Xavier
 Caroline 47627418646 (PCO); [redacted]; McLaughlin, Andrew J
Subject: RE: New Heads up - threat briefing for the Panel - June 20
Importance: High

Classification: SECRET//CANADIAN EYES ONLY

Hello,

Further to the email below and my conversation with some of you today.

Panel Retreat – Threat Brief

June 20 8:30-11:30

1. CSE / CSIS Threat Brief – similar to that delivered to Minister Goodale.
 - a. CSIS will provide CIRs as background reading material. (please provide asap)
 - b. CSIS will table drop a placemat
 - c. CSIS will provide the placemat and or script with Goodale for me to brief NSIA wrt content (please provide asap)
 - d. I'm told CSIS DIR is not requesting a plus 1

2. RCMP Threat Brief (please provide a contact person so I can get a sense of content)

3. GAC Threat Brief (TBC – just verifying with NSIAO)
 - e. GAC has provided background docs (thank you!)

Minister Gould – Threat Brief

June 20 3:30 (TBC)

1. CSE / CSIS Threat Brief – updates from last time, new reporting, new engagement

SECRET**1**

For Public Release

SECRET

- a. No placemat required
- b. Australian Elections update
- c. News article about Russia/US power grid

- 2. GAC Country Updates
- d. Ukraine, EU, Alberta

Please advise if you have any questions and grateful for your responses to the above.
 Thanks.
 Alia

From: Tayyeb, Alia C
Sent: June 6, 2019 6:16 PM
To: Wilczynski, Artur; King, Lyall
 @rcmp-grc.gc.ic.ca>; Denham, Tara
 <denhamt@international.gc.ic.ca>
Cc: @pco-bcp.gc.ic.ca>; @pco-bcp.gc.ic.ca>;
 pco-bcp.gc.ic.ca>; Xavier, Caroline M. <cmxavie@pco-bcp.gc.ic.ca>;
 >; McLaughlin, Andrew J
Subject: New Heads up - threat briefing for the Panel - June 21

Classification: SECRET//CANADIAN EYES ONLY

- 1. Further to the below, please consider this an additional heads up that the Panel itself will be meeting on June 21 and an important agenda item will be the overall threat briefing for the Panel. CSIS, CSE and RCMP Deputies will be expected to deliver this and should have already received the invitation. Briefing can be TS/SI in this case.

Please confirm the leads for each of your agencies and I will set up a call to ensure we are all on the same page. DD by COB tomorrow.

- 2. With respect to the SECRET briefing of political parties (TBC sometime later in June), we should be able to give them points of contact for CSIS, CSE and the RCMP. Please discuss how you wish to do that, i.e. a person, an email, a singular SITE email...? Happy to further discuss if you like.

Thank you.
 Alia

From: Tayyeb, Alia C

SECRET

2

For Public Release

SECRET

Sent: June 3, 2019 12:04 PM

To: Wilczynski, Artur [redacted]

; King, Lyall

[redacted]; [redacted]@rcmp-grc.gc.ca; Denham, Tara

<[redacted]@international.gc.ca>

Cc: [redacted]@pco-bcp.gc.ca; [redacted]@pco-bcp.gc.ca; [redacted]

[redacted]@pco-bcp.gc.ca; Xavier, Caroline M. <[redacted]@pco-bcp.gc.ca>

Subject: Heads up - SECRET briefing to political parties

Classification: SECRET//CANADIAN EYES ONLY

Good morning,

As was noted at the first Critical Election Incident Panel (aka Panel of 5) meeting on Friday (your Deputies were in attendance), I wanted to give you an early heads up that we are looking to schedule our first SECRET level briefing of cleared political party representatives – likely the third week of June (TBC).

The rough agenda I would envisage would be something along the lines of:

1. Intro to each of your agencies and SITE overview
2. Trends overview – similar to what was done for Min Gould but at SECRET level
3. Specific Cyber trends + overview of the unclass briefs CSE has been doing with parties
4. Work plan for political party engagement (PCO will lead this with your and DI input)

I will revert with more information once we have a firm date. Happy for your comments / feedback / suggestions.

Thanks very much.

Alia

SECRET**3**

For Public Release

Background: Lyall's Readout from briefing to cleared party members.

TOP SECRET/[REDACTED]/CANADIAN EYES ONLY

McLaughlin, Andrew J (Andy)

From: King, Lyall
Sent: June-19-19 12:18 PM
To: McLaughlin, Andrew J (Andy); Wilczynski, Artur
Cc: [REDACTED]
Subject: Briefings to Cleared political party members and Elections Canada Excom

Classification: TOP SECRET/[REDACTED]/CANADIAN EYES ONLY

Andy,

Here is a brief summary of the presentations made to cleared political party members on 17 June and to the Excom of Elections Canada on 18 June:

SECRET Briefing to Cleared members of Political parties, 17 June, 1130-1300

Chair: Caroline Xavier

Briefers: PCO, CSE, CSIS, GAC, RCMP

Agenda

1. Introduction (PCO- Security Intelligence) – 2 min
2. Security Briefing (PCO-Security Ops) – 3 min
 - Overview of rules of info management of SECRET intelligence
3. CSE's 'Cyber Security Guide for Campaign Teams (CCCS/[REDACTED]) – 10 min
 - Discussion on cyber guide and TDP2 highlights
4. Intro to SITE TF (CSE/CSIS/GAC/RCMP) – 20 min
 - Intro to SITE– referring to [SITE Brief](#) and [Roles/Responsibilities](#) documents (CSE/Lyall King)
 - Each agency to provide quick 2 min overview of authorities/mandates – what we bring to the SITE table (CSE, CSIS, GAC, RCMP)
5. Preliminary Threat Briefing (SITE TF – CSIS Lead/[REDACTED]) – 30 min
 - Baseline info - verbal (what is foreign interference, what we see, general trends, key concerns – RU/CH, provide reassurance of coverage)
6. Way Forward (PCO-Sec Int) – 5 min
 - Proposal for upcoming briefs, contact information, etc

Comments

- Members from PC, Liberal, NDP and Green parties present (8 total), plus Min DI CoS
- Briefing was well-received – a couple of follow-on questions:
 - How do you spot/prevent influence at the local level?
 - CSIS discussed difficulties in this space as candidates are not always aware; suspicions, particularly involving financing, should be reported so Security and Law Enforcement are aware (and can take action should thresholds be met).
 - How are we doing compared to our allies wrt securing our democratic processes?
 - I discussed general lessons learned from [REDACTED] – explained how we put lessons into practice for defence; referred to good work done by CCCS with EC, [REDACTED]
 - How are platforms like Wechat playing into interference?
 - General comment back that [REDACTED] given press in BC on use of Wechat to encourage voters.
- MinDI CoS asked a few questions – more in line with follow-up later:

TOP SECRET/[REDACTED]/CANADIAN EYES ONLY

1

For Public Release

TOP SECRET// [] /CANADIAN EYES ONLY

- o What are the thresholds for going public with material?
- o Do we have updated information from recent Australian elections?
- o How will info flow work between ministers, social media and CSE (for example if Min Gould's FB account is hacked)?
- o He also commented on the fact that not everyone is starting from the same level of understanding, so more information is good.
- Caroline closed the session while indicating the intent to hold another session in late July (availability pending), with a focus on some scenarios, establishing clear contact points for party reps, and a threat brief.

SECRET Briefing to Elections Canada Executive Committee, 18 June, 1120-1200

Briefers: CSE/Lyall King, CSIS/[]

- I gave a brief overview of SITE TF, roles and responsibilities (5 min)
- CSIS led on the threat brief – covering same basic points detailed in the attached (below)
- Briefing was well received
- Some questions/discussion on:
 - o types of information targeted by adversaries (i.e. looking for voter lists – what use is this? Are they more likely to target individuals/politicians?)
 - I noted that this is often opportunistic – []
 - o Special ballots and other points of vulnerability (i.e. 300k+ Canadians in Hong Kong) – general notion that we need to better understand risk around this.
 - o Discussion on financing violations and how intelligence can feed into this
 - We emphasized existing relationships with RCMP, CSIS, FINTRAC and Commissioner of Canada Elections; also noted that intelligence/investigations can take time – long outlasting election cycle.

CSIS speaking points used for Threat Brief (political parties); similar message to EC Excom, but not word for word (ignore first page on CSIS mandate....)



Classified Briefing to Politic...

Lyall King

[]

TOP SECRET// [] /CANADIAN EYES ONLY

SECRET

EXERCISE EXERCISE EXERCISE

media/comm

CRITICAL ELECTION INCIDENT PROTOCOL PANEL
TABLETOP EXERCISE #1 - CYBER INCIDENT

website
public
comms.

Element 1:

On October 6, 2019, Returning Officers (ROs) and Assistant Return Officers (AROs) in some ridings across Canada fall prey to a series of sophisticated spear phishing attacks.

300k

EC - Action on DMOC/BSC info

Element 2:

On October 8th, the Elections Canada's (EC) IT system is successfully breached by a cyber-attack targeting the National Register of Electors. While the source of the attack cannot be immediately identified, CSE notes that the technical signatures of the attack point to a sophisticated actor.

party

Element 3:

On October 9th, the media starts reporting an observable volume of internet traffic is being directed to the IP addresses of Canadians in 15 ridings across Canada. The traffic appears to be emanating from computer servers in Bulgaria and mostly consists of social media posts generated by botnets. The social media posts contain information meant to discredit the incumbent candidates. The commonality between the 15 targeted ridings is that they are known to be swing ridings where the typical margin of victory for previously elected officials was been quite small.

party

*• RFA
• BAC
• Same party?
• leader
India
Liberals*

[Redacted boxes]

Actions Taken

- CSE has been working with EC to investigate and contain the breach.
- As per established incident response procedures, DGs, ADMs and DMs (DMOC) have been briefed. EC and the Office of the Commissioner of Canada Elections (CCE) have also been informed of the available intelligence.
- [Relevant Ministers and the PM have been briefed. ?] *panel first*
- Elections Canada has been providing reassuring public messaging regarding the integrity of the election and have not publicly discussed the breach of their systems. They do not assess this incident as having an impact on the integrity of the election process.

Questions

1. Should the Panel be formally convened to consider the issue?
2. As per the CEIPP, does the accumulation of incidents described above meet the threshold for informing the public?
3. Will the Panel consult with the Chief Electoral Officer and the Commissioner of Canada Elections? What considerations should be raised?
4. What response options, if any, will the Panel consider if this threshold for informing the public?
5. Would the Panel provide any guidance to the security and
6. What is the public communications response from the P intelligence community if the threshold is met? If it is r
7. What, if any, is the Panel's engagement strategy with informing the public is met? If it is not met?

For Public Release



For Public Release

SECRET

Annex BQuestions and Consideration Towards Determining Threshold (Meeting Two)

Determining whether the threshold for a public announcement has been met will require considerable judgement and there are different considerations that could be included in making this decision:

- the degree to which the incident(s) undermine(s) Canadians' ability to have a free and fair election;
- the potential of the incident(s) to undermine the credibility of the election; and
- the degree of confidence officials have in the intelligence or information.

*factually / actually**(perceived)**unhelpful*

One prevailing principle is that a public announcement would be an extraordinary event that could in itself, significantly influence the overall results of the election and possibly undermine the credibility of the electoral process. There are risks associated with making an announcement (i.e. not being seen as impartial or serving the interest of a particular party) and not making an announcement if clear evidence of an attack or other incident emerges after the election.

Recognizing that these decisions require nuanced judgement and are highly dependent on context, some questions to possibly consider when assessing if the threshold has been met may include:

- To what extent is the incident(s) vote changing?
- To what extent has disinformation been disseminated beyond specific interest groups, i.e. picked up and reported on by the mainstream media? (Exposure and Reach)
- Has the incident created fear or intimidation among segments of the population in terms of ability to vote? Does this have a significant impact on the election?
- Has the incident disproportionately affected parties or candidates? To what extent has it interfered in the level electoral playing field?
- Is this a matter for referral to the Commissioner of Canada Elections?
- To what extent is it believed that the interference is related to foreign actors?
- Is the disinformation around something that would affect the election?
- What is the scale/scope of the incident?
- Are there other remedies to the incident? For example, is this something traditional media is best positioned to weigh in on? To what extent is the incident(s) self-correcting?

For Public Release

Background: CSIS talking points for the threat
brief to cleared party members.

SECRET
2019 06 17

Classified Briefing to Political Parties: CSIS Mandate & Threat Landscape

CSIS Mandate on FI

- At CSIS, we collect intelligence on threats to the security of Canada and foreign intelligence using a variety of investigative methods.
- CSIS investigates threats which may, on reasonable grounds, be suspected of posing a threat to the security of Canada.
- We also have the authority, in certain circumstances, to take reasonable and proportionate measures to reduce the threats we detect.
- We collect and analyze information and we produce intelligence reports, including threat assessments and security assessments, to various departments of the federal government and law enforcement authorities.
- CSIS is not a law enforcement agency like a police force or the RCMP. We have no authority to arrest or detain people.
- At CSIS, accountability is at the centre of everything we do. The Security Intelligence Review Committee reviews all our activities. We are also subject to judicial oversight. A warrant from the Federal Court is required for any intrusive investigative measure we use.
- Since the Service's inception, it has been mandated to investigate espionage, sabotage and foreign interference threat activities. In the CSIS Act, foreign influenced activities or foreign interference are defined as any activities within or relating to Canada that:
 - are detrimental to the interests in Canada, and
 - are clandestine or deceptive or involve a threat to any person.
- As a member of the SITE taskforce, CSIS collects information about foreign interference and provides advice, intelligence reporting and intelligence assessments to the Government about these activities, as well as other hostile state activities.

1

SECRET
2019 06 17

Threat Overview

- FI activities are long-standing, ongoing, systematic, and deeply rooted threats. While foreign interference differs from traditional espionage, FI and espionage activities are often conducted simultaneously via similar tradecraft and threat networks.
- Foreign states continue to engage in extensive and aggressive foreign interference against Canadians and Canadian institutions. Foreign interference in the Canadian political system is motivated by foreign governments' political, economic and security agendas.
- The main goals of foreign state actor FI activity in Canada are:
 - strategic and economic gain (notably, influencing elections and their outcomes or pressuring Canadian officials into taking specific stances on key issues);
 - regime preservation; and,
 - discrediting liberal-democratic institutions with the aim of advancing their own regime interests.
- Foreign threat actors use a range of levers in their influence and interference activities: cyber operations can be used together with traditional human intelligence operations to undermine democratic processes
- FI activities are conducted by foreign diplomats, intelligence officers, state proxies and co-optees including key members of diaspora communities.
- All levels of political power in Canada have been targeted: federal, provincial, territorial and municipal. Political office-holders, candidates, office personnel and other persons with perceived access or influence have been the main targets.
- As a multicultural society, diaspora communities in Canada are vulnerable to FI activities, and in some cases, are the targets of state-directed threats of violence or other punitive measures.
- Tactics may include threatening, harassing and even detaining family members outside of Canada or refusing to issue travel documents or visas without cooperation.

For Public Release

SECRET
2019 06 17

- Coerced, or even sympathetic, community members are then used as proxies by foreign threat actors to engage with Canadian decision-makers or undertake activities that would not be appropriate for official representatives in Canada.
- State-sponsored cyber information operations against democratic institutions are on the rise globally and will continue to impact democratic institutions worldwide.
- A small number of nation-states (notably, Russia) have undertaken the majority of the cyber activity against electoral processes worldwide. Other Western democracies have been targeted by cyber actors.
- While Canada is not immune to this threat, we are not aware of any significant cyber threat to Canadian elections posed by state actors at this time. Furthermore, we have no information to indicate that non-state actors are actively conducting, or plan to conduct, cyber-based influence operations.
- The rise of social media and web platforms creates new risks and enables influence activity at unprecedented scale and sophistication. These new systems have generated unintended threats to the democratic process, depriving the public of true and relevant information, informed political commentary, and the means to identify and ignore fraudulent information.
- We are almost certainly not aware of the full extent of the FI activities of hostile states in Canada.

Main actors in Canada that carry out FI activities – China and Russia

The People's Republic of China and the Russian Federation are the top-tier FI threats. Based on the observed FI activities, we assess these states believe they can operate in Canada with relative impunity. FI activities tend to increase leading up to and following elections.

Election 2019: Trends

- Current threat landscape in Canada is consistent with past practice from threat actors: Little discernable increase in overall interference activities at this time.
- Cyber threat activity has been directed against other Western elections. [redacted]
[redacted] -We are not aware of any significant cyber threat to Canadian elections at this time.

3

For Public Release

SECRET
2019 06 17

- HUMINT threat activity remains the most prominent form of foreign interference in Canada. We assess this is unlikely to change ahead of Election 2019.
- Use of social media platforms by foreign state actors to conduct disinformation and amplification activity has increased globally. This trend likely to be a factor in the Canadian electoral context. At present, discernable FI activity in the social media space is limited.

China

Strategic Points:

- Most significant foreign interference actor – the threat emanates [redacted] through [redacted] *Chinese officials* in Canada, uses Chinese Canadian Community groups, social media tools, trusted contacts, co-optees and cut-outs (business people, Canadian permanent residents and citizens), staff members of elected officials, and China media language outlets, to advance Communist Party of China objectives.
- Covert influence on key individuals is long-standing, occurs Canada-wide, directed toward all major political parties. China seeks to clandestinely and/or deceptively support Canadian candidates, parties, and policies perceived to further the Communist Party of China's (CPC) strategic interests.
- Targets of China's threat activities are often unaware of the Chinese government's interest in them – though some targets willingly cooperate with China's threat actors.
- China is currently consolidating its strategic approach, which involves selecting preferred political candidates across federal party lines, aligning community-influence groups to promote Chinese political objectives, and arranging financial support to be funneled to preferred candidates. Local priorities may take precedence over national-level preferences
- Elected officials and candidates across all levels of government targeted – China covertly directs financial and voting support for favorable candidates, parties, and policies perceived to further the China's strategic interests.
- There is a general trend towards China interfering with Canadian officials at all levels of Canadian Government. [redacted] preferred supporters at municipal levels of government and then direct them upwards to provincial and federal levels for long term cultivation.

4

SECRET
2019 06 17

- China's intelligence capabilities are advanced, and its intent to utilize its range of levers is high. [redacted] China remains an active cyber player with interests in many Canadian entities and sectors, [redacted]

[redacted]

- Based on historical patterns of Chinese interference activity in the lead-up periods to Canadian elections, [redacted] we assess that Chinese activities will increase closer to the October election.

Russia

Strategic Points:

- Globally, Russia is a significant foreign interference threat actor and this is particularly true for threats to democratic institutions. Notwithstanding the latter, to date, [redacted] Russian activity against Canada's 2019 Election and Canadian democratic institutions has been minimal.
- Canada's electoral processes will be targeted if Russia sees disruption and interference as strategically beneficial. [redacted]

[redacted]

- [redacted]

- [redacted] that Canada's election is not a priority target for Russia. Given Russian FI efforts in other countries, we will remain watchful for similar levels of Russian preparatory actions undertaken prior to the Canadian election that may lead to Russian interference activity.

- [redacted]

- [redacted]

SECRET
2019 06 17

While Canada does face other state-based threat actors that could potentially interfere in electoral areas, these states' intent and capability remain low compared to the threat Canada faces from China and Russia.

[Redacted]

India

- [Redacted] the Sikh extremist threat, and monitoring the Sikh community in Canada, is a priority for Indian officials in Canada, [Redacted]
[Redacted]
- Indian officials have utilized a network of contacts, which includes politicians, academics, businesspersons, media personalities and community leaders, to monitor Canadian-based individuals that are of interest to the Government of India.
- [Redacted]
[Redacted] Some of this activity has been conducted in either a clandestine or deceptive manner making it foreign interference.
- Furthermore, Indian interference activities targeted at Canadian Members of Parliament, Provincial Legislative Members, [Redacted], outside the scope of regular diplomatic norms, has been observed.
- [Redacted]

Pakistan

- [Redacted], Pakistani officials in Canada have likely tried to clandestinely influence and support Canadian politicians of Pakistani descent, with the aim of furthering Pakistani interests in Canada.
- [Redacted]

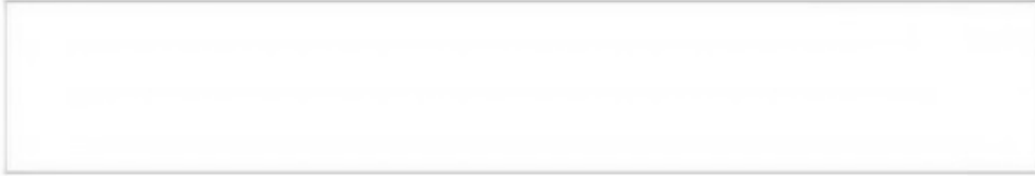
[Redacted]

[Redacted]

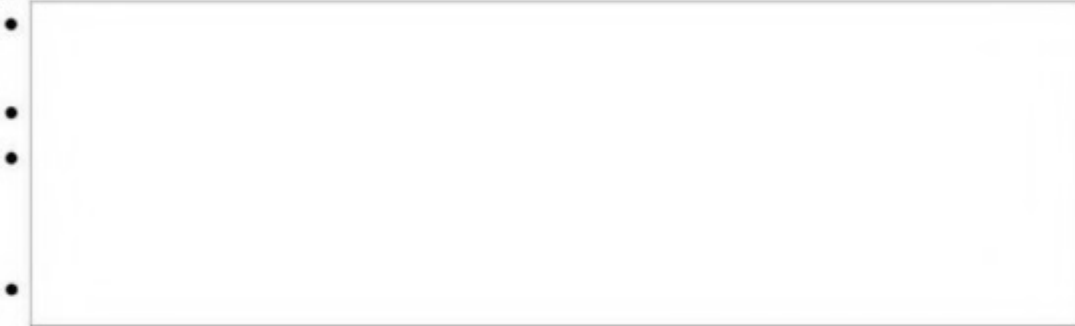
For Public Release

• • •

SECRET
2019 06 17



Iran



For Public Release

Cabinet Directive on the Critical Election Incident Public Protocol

1.0 Introduction

The protection and preservation of Canada's democratic institutions and practices is one of the core responsibilities of the federal government.

National security threat and risk assessments, along with the experience of key international allies, underscore that Canada's 2019 General Election may be vulnerable to foreign interference in a number of areas. Recognizing this, significant work has been undertaken within the federal government to protect and defend electoral systems and processes. As part of this work, the Government of Canada has established the Critical Election Incident Public Protocol (CEIPP) in order to ensure coherence and consistency in Canada's approach to publicly informing Canadians during the writ period about incidents that threaten Canada's ability to have a free and fair election.

2.0 Purpose

The *Cabinet Directive on the Critical Election Incident Public Protocol* sets out the ministers' expectations with respect to the general directions and the principles to guide the process for informing the public during the writ period of an incident that threatens Canada's ability to have a free and fair election.

The Protocol is an application reflective of the caretaker convention. The caretaker convention puts into practice the principle that the government is expected to exercise restraint in its activities and "restrict itself" in matters of policy, spending and appointments during the election period, except where action is "urgent" and "in the national interest".

During the caretaker period, announcements that must proceed are to be made in the name of the department to ensure a distinction between official government business and partisan activity.

3.0 Scope of Application

The Critical Election Incident Public Protocol will have a limited mandate. It will only be initiated to respond to incidents that occur within the writ period and that do not fall within Elections Canada's areas of responsibility (i.e., with regard to the administration

For Public Release

of the election, as identified in the *Canada Elections Act*). Incidents that occur prior to the writ period will be addressed through regular Government of Canada operations.

4.0 Panel

The CEIPP will be administered by a group of senior civil servants who will, working with the national security agencies within the agencies' existing mandates, be responsible for determining whether the threshold for informing Canadians has been met, either through a single incident or an accumulation of separate incidents.

This Panel will be comprised of:

- the Clerk of the Privy Council;
- the National Security and Intelligence Advisor to the Prime Minister;
- the Deputy Minister of Justice and Deputy Attorney General;
- the Deputy Minister of Public Safety; and
- the Deputy Minister of Foreign Affairs.

5.0 Process

The protocol lays out a process through which Canadians would be notified of an incident that threatens Canada's ability to have a free and fair election, should notification be necessary.

During the writ period, the protocol for a public announcement would be:

1. The national security agencies will provide regular briefings to the Panel on emerging national security developments and potential threats to the integrity of the election.
2. If the head of a national security agency (i.e., the Communications Security Establishment, the Canadian Security Intelligence Service, the Royal Canadian Mounted Police or Global Affairs Canada) become aware of interference in the 2019 General Election, they will, in consultation with each other, consider all options to effectively address the interference. Barring any overriding national security/public security reasons, the agencies will inform the affected party (e.g., a candidate; a political party; Elections Canada) of the incident directly.
3. The Panel will evaluate incidents to determine if the threshold (as set out in Section 6 below) for informing the public has been met. The Panel will operate on a consensus basis and will draw on expertise from across government, including national security agencies working within their existing mandates.

For Public Release

4. If a public announcement is deemed necessary, the Panel will inform the Prime Minister, the other major party leaders (or designated senior party officials who have received their security clearances sponsored by the Privy Council Office) and Elections Canada that a public announcement will be made. These leaders would all receive the same briefing information.
5. Immediately after having informed the Prime Minister, the other political parties and Elections Canada, the Clerk of the Privy Council, on behalf of the Panel, would ask the relevant agency head(s) to issue a statement to notify Canadians of the incident(s).

6.0 Threshold for Informing the Public

A public announcement during the writ period would only occur if the Panel determines that an incident or an accumulation of incidents has occurred that threatens Canada's ability to have a free and fair election.

Determining whether the threshold has been met will require considerable judgement. There are different considerations that could be included in making this judgement:

- the degree to which the incident(s) undermine(s) Canadians' ability to have a free and fair election;
- the potential of the incident(s) to undermine the credibility of the election; and
- the degree of confidence officials have in the intelligence or information.

The Panel brings together unique national security, foreign affairs, democratic governance and legal perspectives, including a clear view of the democratic rights enshrined in the *Canadian Charter of Rights and Freedoms*.

Although a disruptive event or interference may emanate from domestic and/or foreign actors, as a starting point, the focus should be on foreign interference. That being said, attribution of foreign interference attempts may be challenging or not possible within the timelines permitted by events, given that attempts to unduly influence the election may involve misdirection and disinformation. Further, it is possible that foreign actors could be working in collaboration with, or through, domestic actors. Ultimately, it is the impact of the incident on Canada's ability to have a free and fair election that is at issue in the determination of whether the threshold has been met, and if a public announcement is required. For clarity, Canadians – and democracy – are best served by election campaigns that offer a full range of debate and dissent. The Protocol is not intended to, and will not, be used to respond to that democratic discourse.

For Public Release

7.0 Announcement

The announcement would focus on:

- a) notification of the incident;
- b) what is known about the incident (as deemed appropriate); and
- c) steps Canadians should take to protect themselves (e.g., ensure that they are well informed; cyber hygiene), if relevant.

8.0 Existing Authorities

Nothing in this Directive in any way alters or expands the mandates of the national security agencies or any other department or agency. Specifically, nothing in this Protocol supersedes the RCMP's independence.

9.0 Assessment

Following the 2019 election, an independent report will be prepared, assessing the implementation of the Critical Election Incident Public Protocol and its effectiveness in addressing threats to the 2019 election. This report will be presented to the Prime Minister and to the National Security and Intelligence Committee of Parliamentarians. A public version will also be developed. The report is intended to help inform whether the Protocol should be established on a permanent basis going forward to help protect the integrity of future elections or what adjustments to the Protocol should be made to strengthen it.