



Global Affairs  
Canada

Affaires mondiales  
Canada

Canada

# RRM Canada

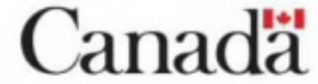
## Government of Canada Efforts to Address Foreign Interference in the National Elections



SECURITY AND INTELLIGENCE  
THREATS TO ELECTIONS TASK FORCE

# Preliminary Assessment

- In January 2019, in recognition of the importance of protecting Canada's electoral process from foreign interference, the Government of Canada announced a number of measures to defend Canadian democracy and further strengthen our electoral systems.
- The [Critical Election Incident Public Protocol](#) was established 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. The Protocol, and its administration, was **overseen by a panel of five senior civil servants who were responsible for determining whether the threshold for informing Canadians had been met, either through a single incident or through an accumulation of separate incidents.**
- In addition, the Security and Intelligence Threats to Elections (SITE) Task Force was established as a fully integrated team to help the Government assess and respond to foreign threats.
- Throughout the election, the Protocol Panel held regular meetings and their discussions were informed by intelligence and analysis provided by the SITE Task Force and from other sources. **The Panel did not observe any activities that met the threshold for public announcement or affected Canada's ability to have a free and fair election.**



Global Affairs  
Canada

Affaires mondiales  
Canada

P R O T É G E R  
L A D É M O C R A T I E

M É C A N I S M E D E  
R É P O N S E R A P I D E D U

**G7**

R A P I D R E S P O N S E  
M E C H A N I S M

P R O T E C T I N G  
D E M O C R A C Y

For Public Release

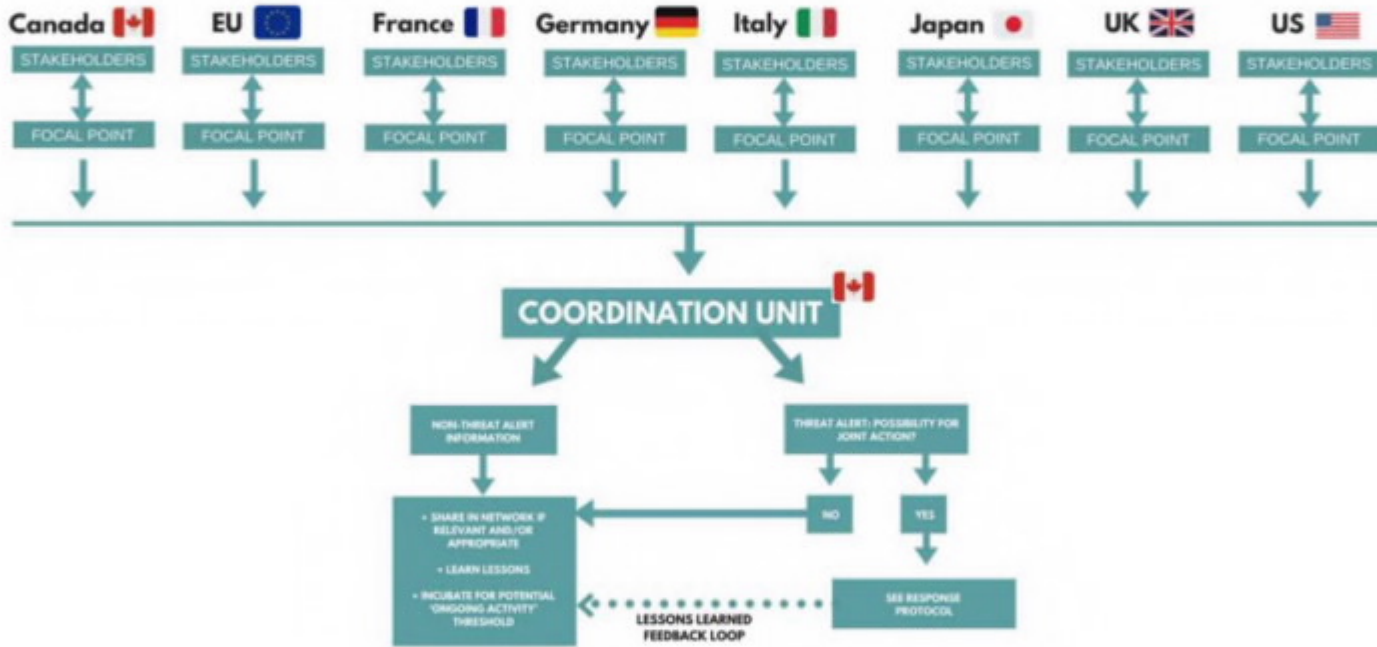


Global Affairs  
Canada

Affaires mondiales  
Canada



# G7 Rapid Response Mechanism



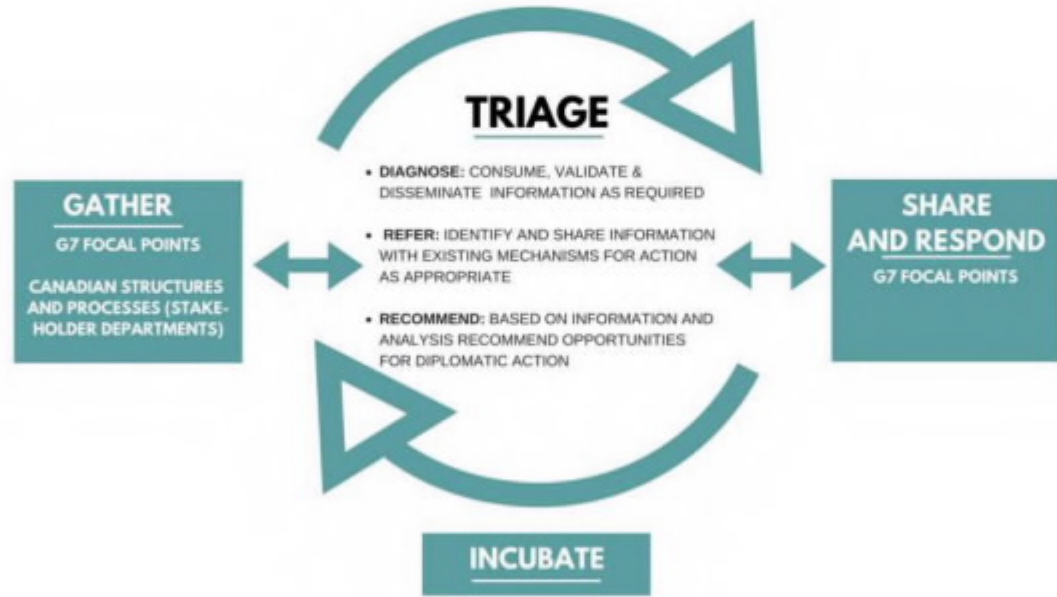


Global Affairs  
Canada

Affaires mondiales  
Canada



# RRM Coordination Unit Key Functions



Global Affairs  
CanadaAffaires mondiales  
Canada

Canada

## RRM Canada

RRM Canada is the network within the Government of Canada (GoC) that the Canadian Focal Point of the G7 RRM has established to coordinate domestic responses to FI and to share GoC initiatives.



Global Affairs  
Canada

Affaires mondiales  
Canada



UNCLASSIFIED//FOR OFFICIAL USE ONLY





### Security and Intelligence Threats to Elections Task Force - Partner Roles Leading to Election 2019



#### SECURITY AND INTELLIGENCE THREATS TO ELECTIONS TASK FORCE

##### WHAT ARE WE TALKING ABOUT?

Covert, clandestine, or criminal activities interfering with or influencing electoral processes in Canada

	MANDATE/ROLE	ACTIVITIES
 <b>CSE</b> Communications Security Establishment	<b>Information Technology Security</b> <ul style="list-style-type: none"> <li>Providing advice, guidance, and services to help ensure the protection of electronic information and of systems of importance</li> </ul> <b>Foreign Intelligence</b> <ul style="list-style-type: none"> <li>Collection of foreign intelligence for Government of Canada on threat actors</li> </ul> <b>Supporting CSIS and RCMP</b> <ul style="list-style-type: none"> <li>Providing assistance on technical operations</li> </ul>	<ul style="list-style-type: none"> <li>Providing intelligence and cyber assessments on the intentions, activities, and capabilities of foreign threat actors</li> <li>Protecting Government systems and networks related to elections through cyber defence measures</li> <li>Providing cyber security advice and guidance to political parties, provinces and other institutions involved in democratic processes</li> </ul>
 <b>CSIS</b> Canadian Security Intelligence Service	<b>Intelligence and Threat Reduction</b> <ul style="list-style-type: none"> <li>Collection of information about foreign influential activities that are detrimental to the interest of Canada and are clandestine or deceptive or involve a threat to any person</li> <li>Countering such activities through threat reduction measures</li> </ul> <b>Intelligence Assessment</b> <ul style="list-style-type: none"> <li>Providing advice, intelligence reporting and intelligence assessments to Government of Canada about foreign influential activities</li> </ul>	<ul style="list-style-type: none"> <li>Providing threat briefings and intelligence reporting to Elections Canada and the Commissioner of Elections</li> <li>Providing an assessment of hostile state activity methodologies and capabilities to Government of Canada decision makers</li> </ul>
 <b>GAC</b> Global Affairs Canada	<b>G7 Rapid Response Mechanism</b> <ul style="list-style-type: none"> <li>Open source research on global trends and data on threats to democracy</li> <li>Partnership with G7 countries to share information and coordinate responses to threats as appropriate</li> </ul>	<ul style="list-style-type: none"> <li>Providing research on disinformation campaigns targeting Canada by foreign actors</li> <li>Reporting on global trends, metrics, and incidents</li> <li>Coordinating attribution of incidents</li> </ul>
 <b>RCMP</b> Royal Canadian Mounted Police	<b>National Security</b> <ul style="list-style-type: none"> <li>The primary responsibility for preventing, detecting, denying and responding to national security-related criminal threats in Canada</li> <li>Investigates criminal offenses arising from terrorism, espionage, cyber attacks, and foreign influenced activities</li> <li>The key investigatory body for Elections Canada if criminal activity is suspected</li> </ul>	<ul style="list-style-type: none"> <li>Investigates any criminal activity related to interference or influence of Canada's electoral process</li> <li>Works closely in partnership with intelligence, law enforcement and regulatory agencies</li> </ul>



Gouvernement  
du Canada

Government  
of Canada



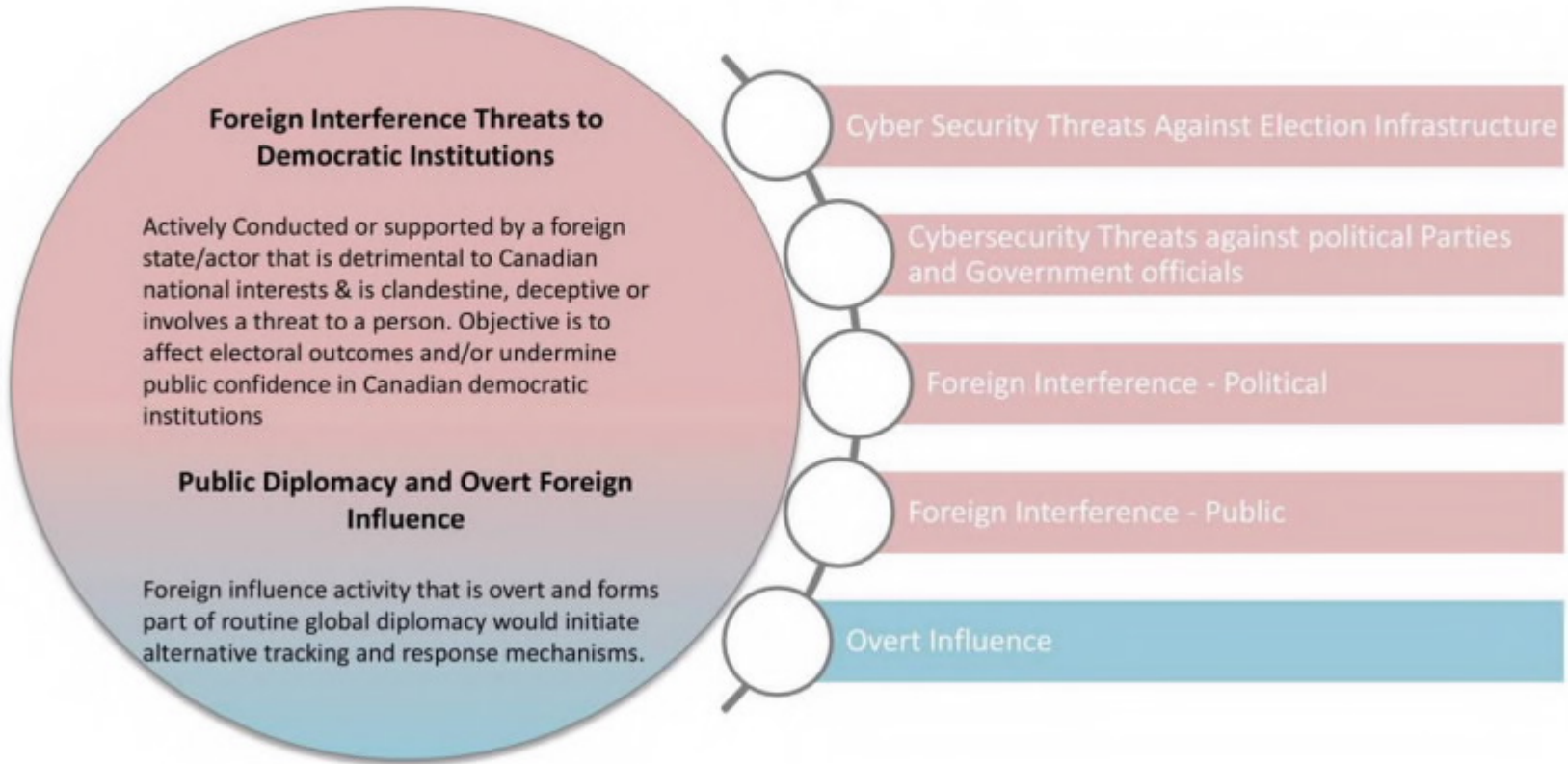


Global Affairs  
Canada

Affaires mondiales  
Canada

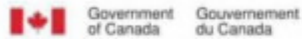


# SITE Playbook





# Improving Organisational Readiness

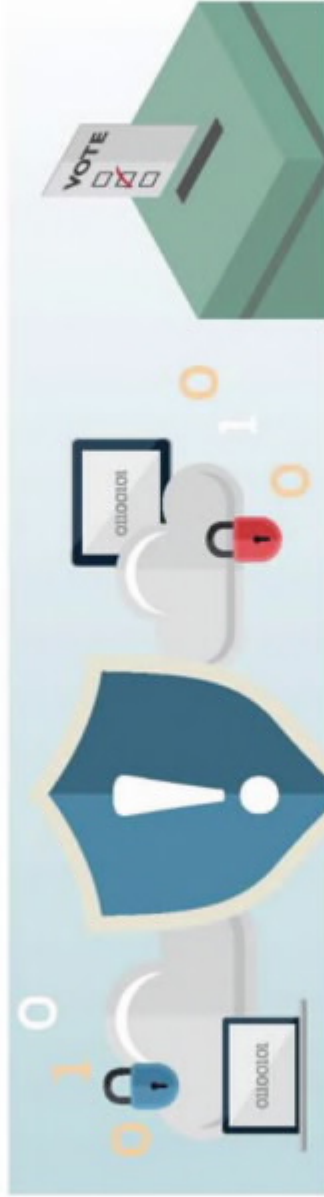


- Sensitising decision makers about the threat
- Providing political parties with clearances to receive threat briefings
- Offering political parties technical advice to protect their cyber systems



For Public Release

# Government of Canada's Plan to Safeguard Canada's 2019 Election





# Enhancing Citizen Preparedness

- *Digital Citizen Initiative* to support digital, news and civic literacy programming
- *Get Cyber Safe* public awareness campaign
- 2019 update to *Cyber Threats to Canada's Democratic Processes Report*
- Canada's *Elections Modernization Act*
- The *Critical Election Incident Public Protocol*

# The North American house hippo is back — and ready to tackle fake news



'We think the house hippo is more important than ever,' says MediaSmarts executive director Kathryn Ann Hill

CBC Radio - Posted: Oct 04, 2019 5:57 PM ET | Last Updated: October 4

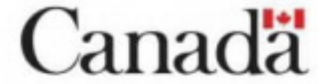


The beloved North American house hippo is back in a new ad to promote Canadian media literacy. (MediaSmarts)



Global Affairs  
Canada

Affaires mondiales  
Canada



# Open Data Analysis

@JustinTrudeau	74,000+
@liberal_party	25,000+
@AndrewScheer	19,000+
@CPC_HQ	14,000+
@gmbutts	6,900+
@MaximeBernier	5,600+
@cathmckenna	4,500+
@CBCNews	2,800+
@manny_ottawa	2,300+
@Danbalkwill1	2,200+



#TrudeauMustGo	310,000+
#cdnpoli	110,000+
#elxn43	94,000+
#TrudeauBlackface	31,000+
#Scheer4PM	26,000+
#TrudeauCorruption	22,000+
#TrudeauWorstPM	16,000+
#Trudeau	9,700+
#TrudeauMustResign	8,900+
#DefundCBC	8,900+





Global Affairs  
Canada

Affaires mondiales  
Canada

Canada

# Open Data Analysis

```

In [1]: import praw

reddit = praw.Reddit(client_id='[REDACTED]',
                    client_secret=[REDACTED],
                    user_agent='[REDACTED]')

print(reddit.read_only)
submissions = reddit.subreddit('[REDACTED]')

True

In [3]: import os
import sys
import time
import requests
from py2neo import Graph, Node, Relationship

In [4]: [REDACTED]

graph.run("CREATE CONSTRAINT ON (r:Rredditor) ASSERT r.id IS UNIQUE")
graph.run("CREATE CONSTRAINT ON (s:Post) ASSERT s.id IS UNIQUE")
graph.run("CREATE CONSTRAINT ON (c:Comment) ASSERT c.id IS UNIQUE")

Out[4]: <py2neo.database.Cursor at 0x23a4f429198>

In [8]: a = reddit.submission(id='cw3fni')

post=Node("Post",id=a.id)
post["title"]=a.title
post["name"]=a.name
post["selftext"]=a.selftext
post["num_comments"]=a.num_comments
post["score"]=a.score
post["upvote_ratio"]=a.upvote_ratio
post["url"]=a.url
post["is_self"]=a.is_self
post["created_at"]=a.created_utc

```

Global Affairs  
CanadaAffaires mondiales  
Canada

Canada

# RRM Canada Ethical and Methodological Framework

- RRM Canada has developed a framework that highlights our legal and ethical responsibility, while providing insight into our analytical work
- The purpose of the framework is to emphasize:  
**The protection of human rights, accountability, and a principled approach to open data analytics**

Global Affairs  
CanadaAffaires mondiales  
Canada

Canada

# Tactics & Trends: Global

- “Meta-trolling”
- Use of foreign interference tactics by domestic actors
- Narrative Competition and Reframing
- Decontextualisation and Hyperlocalization
- Account Purchasing





Global Affairs  
Canada

Affaires mondiales  
Canada

Canada

# Tactics & Trends: Canada

- More disinfo about disinfo and foreign interference than actual foreign interference or disinfo
- Increasingly crowded space



Global Affairs  
Canada

Affaires mondiales  
Canada

Canada

# Outreach Initiatives

- Engaging with Community of Experts across government and civil society
  - Sharing methodologies and best practices
  - Encouraging elections monitoring and open source data analysis.



Global Affairs  
Canada

Affaires mondiales  
Canada

Canada

# Global Community of Practice for Open Source Analysis

- Developing working-level collaborative relationships across G7 partners + Likeminded

For Public Release



Global Affairs  
Canada

Affaires mondiales  
Canada

Canada

# Outreach: Hackathon

- Post Elections: 4-13 Nov 2019
- Partnership with CSE to develop new tools to analyze social media data for FI
- Focus on Reddit data related to Canadian Elections

# Reddit: What is it

Front Page of the Internet

Reddit is a social news aggregation, web content rating, and discussion website.

Members, AKA Redditors, submit content to the site such as links, text posts, and images, which are then voted up or down by other Redditors.



**9%**  
 OF ONLINE  
 CANADIAN  
 ADULTS HAVE A  
**Reddit**  
 ACCOUNT



An amazon.com company

For Marketers For A

Top Sites in Canada

Global By Country By Category

Showing 50 of 500 results

	Site	Daily Time on Site	Daily Pageviews per Visitor
1	<a href="https://www.google.com">Google.com</a> Enables users to search the world's information, including webpages, images, and videos. Offers...More	8:14	10.75
2	<a href="https://www.youtube.com">Youtube.com</a> YouTube is a way to get your videos to the people who matter to you. Upload, tag and share your...More	8:40	4.99
3	<a href="https://www.facebook.com">Facebook.com</a> A social utility that connects people, to keep up with friends, upload photos, share links and ...More	9:24	3.92
4	<a href="https://www.google.ca">Google.ca</a>	4:31	5.82
5	<a href="https://www.reddit.com">Reddit.com</a> User-generated news links. Votes promote stories to the front page.	11:09	7.10



# Battleground

## Nearly 1,000 Russian trolls were banned from Reddit — here's what they were posting about

Kaylee Fagan Apr. 12, 2018, 3:58 PM



Shutterstock.com

## Volunteers found Iran's propaganda effort on Reddit — but their warnings were ignored

More than a year before the announcement from Facebook and Twitter, a group of moderators on Reddit noticed a peculiar pattern of submissions.



Iranian President Hassan Rouhani, top center, reviews army troops marching during the 37th anniversary of Iraq's 1960 invasion of Iran, in front of the shrine of the late revolutionary founder, Ayatollah Khomeini, just outside Tehran, Iran on Sept. 22, 2017. Shiran Nourouzi / AP Photo

## Reddit Has Become A Battleground Of Alleged Chinese Trolls

"Bad enough to have to deal with Russian Ops and the Alt-Right, but now we have to deal with Chinabots as well."



**Craig Silverman**  
BuzzFeed News Reporter



**Jane Lytvynenko**  
BuzzFeed News Reporter

Posted on March 14, 2019, at 2:54 p.m. ET

# Hackathon

Results: over a dozen new tools and methodologies to be shared with G7 and likeminded Governments as well as trusted partners in academia and civil society

Connection to [REDACTED]

Commitment to share code and back end analytic techniques

GECIQ: common analytic, development and reporting platform.



Global Affairs  
CanadaAffaires mondiales  
Canada

Canada

# Challenges

- Limits to open and publicly available data in attribution
- Twitter doesn't matter...
- Identifying and responding to evolving tactics of malignant actors.
- Disentangling the foreign and domestic and the legacy of digital foreign interference campaigns
- Protecting the very principles, rights and democratic society that are being exploited by malign actors

For Public Release

# Threat Landscape and RRM Canada Programming

## Slide Notes

### Slide 1:

#### Introduction

Our govt, as I imagine most of yours, ramped up our thinking about threats to our democracy, after US elections in 2016 and French elections in 2017.

The government's plan to Safeguard Canada's 2019 election similarly was an initiative that developed in an environment that required a dedicated, coordinated and multi-dimensional response to these emerging and complex challenges.

While it's early days for lessons learned just after this week's vote, I'd like to talk about some of the architecture we put in place to guard against foreign interference, including disinformation.

### Slide 3:

The RRM is a concrete and demonstrable effort by the G7 to respond to emerging threats to democracies

It will be led by Canada on an ongoing basis

At it's core – it's about open-source/unclassified information sharing and analysis across the G7, to understand emerging threats to democracies and

identify opportunities for coordinated response

This is the more operational team within the Centre

The two main capacities within the Unit include our:

Policy analysts, who are the 'experts' when it comes to understanding the various threats to our democratic processes and institutions – and who articulate these threats through that lens, i.e. in defence of democracy, openness, and transparency.

Data analysts, who are experts at analysing big data, and increase our capacity to do open-source social medial analysis, in order to map and understand what some of these threat vectors look like (we're currently focused on disinformation campaigns and amplification tactics)

### Slide 4:

Formed of 8 Focal Points, and each is supported by national structures.

The Focal Points share and consume information, meant to be fast, does not have to be formal reports – can be real time.

The Coord Unit is where we triage, assess, and share info. Should a call to action be initiated by a by member, the coord unit would be responsible for devising the formal response.

**Slide 5:**

How does the RRM Coordination Unit add value?

Consume all of the information shared by G7 members and the wider network we are establishing (including leading academics, institutions, and other governments interested in sharing information)

We are working to understand how these various issues and trends impact democracy, and are watching for key tactics and techniques that should be highlighted via the RRM

We also leverage our data and analytic backgrounds to increase our understanding of the threat environment

For social media analysis, we have an ethical and methodological framework to guide our work

NOTE: this is a new capacity for GAC and the GoC

Our policy coverage is from the G7 commitments, and our mandate is to monitor for coercive, corrupt, covert or malicious activities by foreign actors we focus on identifying overarching trends and tactics – not the message/content

We don't monitor for individuals (individuals may appear in searches – as it would do if a person was looking through openly available data), but we don't monitor or focus on individuals when reporting on trends or tactics

We only access openly available information (information anyone else could see)

We have diverse linguistic capacity to support the use of our data analysis tools

We bring these capacities together to support the G7 RRM. In the immediate term, this means:

An annual workplan for the RRM (outlining key events, elections, and trends to monitor) that G7 members commit to share info on (i.e. Ukraine elections, EU elections, our federal election)

We also share the results of research we have commissioned from leading experts, on topics such as Effective Methodologies for Addressing Foreign Interference in Digital Contexts, and The Gender Dimensions of Computational Propaganda and Foreign Interference Operations.

**Slide 6:**

How does the RRM Coordination Unit add value?

Consume all of the information shared by G7 members and the wider network we are establishing (including leading academics, institutions, and other governments interested in sharing information)

We are working to understand how these various issues and trends impact democracy, and are watching for key tactics and techniques that should be highlighted via the RRM

We also leverage our data and analytic backgrounds to increase our understanding of the threat environment

For social media analysis, we have an ethical and methodological framework to guide our work

NOTE: this is a new capacity for GAC and the GoC

Our policy coverage is from the G7 commitments, and our mandate is to monitor for coercive, corrupt, covert or malicious activities by foreign actors we focus on identifying overarching trends and tactics – not the message/content

We don't monitor for individuals (individuals may appear in searches – as it would do if a person was looking through openly available data), but we don't monitor or focus on individuals when reporting on trends or tactics

We only access openly available information (information anyone else could see)

We have diverse linguistic capacity to support the use of our data analysis tools

We bring these capacities together to support the G7 RRM. In the immediate term, this means:

An annual workplan for the RRM (outlining key events, elections, and trends to monitor) that G7 members commit to share info on (i.e. Ukraine elections, EU elections, our federal election)

We also share the results of research we have commissioned from leading experts, on topics such as Effective Methodologies for Addressing Foreign Interference in Digital Contexts, and The Gender Dimensions of Computational Propaganda and Foreign Interference Operations.

**Slide 7:**

We work to ensure that the knowledge gained by the RRM is integrated into our national structures – and in particular, is leveraged to protect our national elections.

Participate in the Security and Intelligence Threats to Elections (SITE) Task Force, in order to share our reports/newsletters/analysis (weekly basis)

Operate as an 'early warning' system given our mandate to understand the broad threat landscape related to potential foreign interference in the social media landscape.

Established a 'tech table' with SITE and the RRM Canadian network to align data expertise across the GoC - and clarify mandates, capacities, thresholds, and methodologies related to social media analysis.

RRM Canada has established indicators for reviewing information in the social media environment to determine the extent to which we may suspect foreign interference. Any initial monitoring done via RRM Canada that identifies suspected foreignness (such as unnatural amplification or evolving tactics noted by other G7 members) – is shared with SITE, and if of significance and within mandates, can be investigated further.

We brief various government departments (and communications teams) on the work of the RRM, as there is increased focus on understanding the threat posed by disinformation and other covert and overt influence activities – and how other countries have/are responding

**Slide 8:**

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

**Bin 1: Cybersecurity threats against election infrastructure**

Threats that are malicious and deliberate attempts directed, subsidized or undertaken by – or on behalf of - a foreign state/actor targeting Canadian election infrastructure.

Threats to Canada's elections infrastructure targeting information technology (IT) systems supporting the election; the owners and operators of electoral IT systems; individuals accountable for the election (i.e. electoral officials); and, the vendors of hardware and/or software that is used within the elections infrastructure.

**Bin 2: Cybersecurity threats against government officials, political parties or electoral candidates.**

Malicious and deliberate attempts directed, subsidized or undertaken by - or on behalf of – a foreign state/actor that targets Canadian government officials, Canadian political parties or electoral candidates.

In these instances, the IT systems of a Canadian political party, candidate or government official would be threatened.

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

**Bin 3: Foreign Interference ~ Political**

Foreign interference activity that targets Canadian government officials, political organizations or electoral candidates with the goal of impacting electoral outcomes, and/or undermining their policies, positions and opinions.

This threat activity is conducted in a clandestine, deceptive or coercive manner and is directed, subsidized, or undertaken by - or on behalf of - a foreign state/actor.

#### Bin 4: Foreign Interference – Public

Foreign interference activity that targets the Canadian public and/or discrete populations, such as local diaspora communities.

The objective of this type of activity is to impact electoral outcomes, sow societal discord, sway public sentiment within Canada to undermine Canadians' confidence in the electoral system and processes and/or support the foreign states/actors own national interests and agenda.

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

#### Bin 5: Overt Influence

Overt influence refers to the use of public diplomacy and other means whereby a foreign state openly attempts to influence Canadian policy, the political landscape and/or electoral processes. Similar to the other Bins, one goal of overt influence activity can be to affect electoral outcomes within Canada but because it is overt and transparent, it initiates alternative diplomacy response mechanisms.

Given the overt and often political nature of this activity, GAC is best positioned to respond to concerns within Bin 5.

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

#### **Slide 9:**

This is all about improving the government's ability to identify, prevent and respond to the threats to our democracy

Sensitising decision makers about the threat  
 Providing political parties with clearances to receive threat briefings  
 Offering political parties technical advice to protect their cyber systems

**Slide 10:**

A series of actions across a number of areas were taken to further strengthen our electoral system. The plan includes four pillars

**Slide 11:**

An engaged and informed public is perhaps the best line of defence against disinformation. With this in a core pillar was to think about how to enhance Canadians preparedness through various initiatives

Digital Citizen Initiative to support digital, news and civic literacy programming;  
 Get Cyber Safe public awareness campaign;  
 2019 update on Cyber Threats to Cda's Democratic Process rpt;  
 Elections Modernization Act expanded the education mandate of Canada's Chief Electoral Officer, clarified prohibitions related to false statements and foreign interference, and prohibited the use of foreign funds by third parties for partisan advertising and activities.  
 Critical Election Incident Public Protocol: impartial process to inform Cdns of threat to integrity of 2019 election  
 Panel of 5 senior public servants – natl security, foreign affairs, democratic governance, justice – charged with monitoring threats to elections and determining if and when to communicate threats to Cdns.  
 Protocol has a narrow scope – FI only – and a high threshold for reaching out to Cdns

Together, these measures aim to foster a more informed public, better equipped to think critically about what they read and share online.

**Slide 15:**

What the RRM's work is bounded by:  
 Canadian Charter, Privacy Laws, Ministerial Direction for Avoiding Complicity in Mistreatment by Foreign Entities, Safeguarding Elections Protocols  
 Principles Approach and Clear Protocols:  
 Information sharing is determined by external and internal protocols



### Gender Equality and Awareness of Harms

GBA+; Privacy Training; Considerations of fundamental rights and freedoms; awareness of context and differentiated impacts to communities

#### **Slide 16:**

Over the last 6 months, through information exchange via the RRM, and our focused social media analytics and analysis of recent elections (EU, Ukraine), RRM Canada has identified the following key tactics related to foreign interference in democratic processes and institutions:

“Meta-trolling” - Openly claiming disinformation campaigns or designing content to be detected and called out as propaganda in order to discredit the information it contains. In both cases, this tactic is designed to call into question the legitimacy of an election or any given piece of information by deliberately associating it with “foreign Trolls.”

Use of foreign interference tactics by domestic actors - evidence of coordinated inauthentic behavior undertaken by domestic actors – more challenging to identify foreign interference.

Narrative Competition - transnational narratives on divisive issues (climate change, immigration, LGBTQ, religious intolerance) being amplified across borders, with a mix of national and international actors involved. Attempts to reproduce and repurpose narratives in regional/international context, promoting similar narratives and sentiments around divisive. Again, increased complexity to identify foreign interference.

#### Decontextualisation

We consider decontextualisation as the use of authentic information that is manipulated and distorted through the misrepresentation of its content or context. Decontextualisation is generally a bad-faith representation of information, whereby the authentic information is taken out of context, misaligned with unrelated events or actors, and generally meant to re-shape the meaning of the content with the aim of achieving a particular, disingenuous or deceptive goal.

Account Purchasing – seen in Ukraine elections: buying social media accounts of authentic users to leverage for foreign interference activities.

**Slide 17:**

Over the last 6 months, through information exchange via the RRM, and our focused social media analytics and analysis of recent elections (EU, Ukraine), RRM Canada has identified the following key tactics related to foreign interference in democratic processes and institutions:

“Meta-trolling” - Openly claiming disinformation campaigns or designing content to be detected and called out as propaganda in order to discredit the information it contains. In both cases, this tactic is designed to call into question the legitimacy of an election or any given piece of information by deliberately associating it with “foreign Trolls.”

Use of foreign interference tactics by domestic actors - evidence of coordinated inauthentic behavior undertaken by domestic actors – more challenging to identify foreign interference.

Narrative Competition - transnational narratives on divisive issues (climate change, immigration, LGBTQ, religious intolerance) being amplified across borders, with a mix of national and international actors involved. Attempts to reproduce and repurpose narratives in regional/international context, promoting similar narratives and sentiments around divisive. Again, increased complexity to identify foreign interference.

**Decontextualisation**

We consider decontextualisation as the use of authentic information that is manipulated and distorted through the misrepresentation of its content or context. Decontextualisation is generally a bad-faith representation of information, whereby the authentic information is taken out of context, misaligned with unrelated events or actors, and generally meant to re-shape the meaning of the content with the aim of achieving a particular, disingenuous or deceptive goal.

Account Purchasing – seen in Ukraine elections: buying social media accounts of authentic users to leverage for foreign interference activities.

**Slide 18:**

Key partners in Atlantic Council’s DFR Lab, German Marshall Fund’s Alliance for Securing Democracy, Oxford Internet Institute’s Computational Propaganda Project and McGill’s Digital Democracy Project

**Slide 19:**

Building infrastructures to facilitate sharing of best practices and knowledge amongst analysts and experts.

**Slide 20:**

Invite sent out global community of practice

**Slide 21:**

Reddit bills itself as the front page of the internet and is one of the most popular websites worldwide.

Popular for it's communities of interest or "Subreddits" in which users submit content for discussion.

Has been as an area for political activity for a relatively long time. US President Obama held an "Ask me Anything" as part of his 2012 re-election campaign.

Political and worldnews subreddits have existed default subreddits automatically subscribed by new accounts since the sites beginnings circa 2005

Subreddits relating to Canada and Canadian politics have existed for

**Slide 22:**

Although the number of Canadians with actual reddit accounts may be relatively small compared to the larger sites like FB the engagement metrics are huge.

Reddit is the 4th or 5th most visited website in Canada depending on how you measure

Visitors on average spend more time on the site and visit more often than both Facebook or Google

Good platform for social search. Ie asking where are is the best Pub in Ottawa on r/Ottawa

Nearly 500K Redditors subscribe to r/Canada and many describe it as their primary source of news

Unk, but probably larger, number of “Lurkers” who brows r/Canada and other Canadian political subreddits without an account.

**Slide 23:**

Just some recent headlines