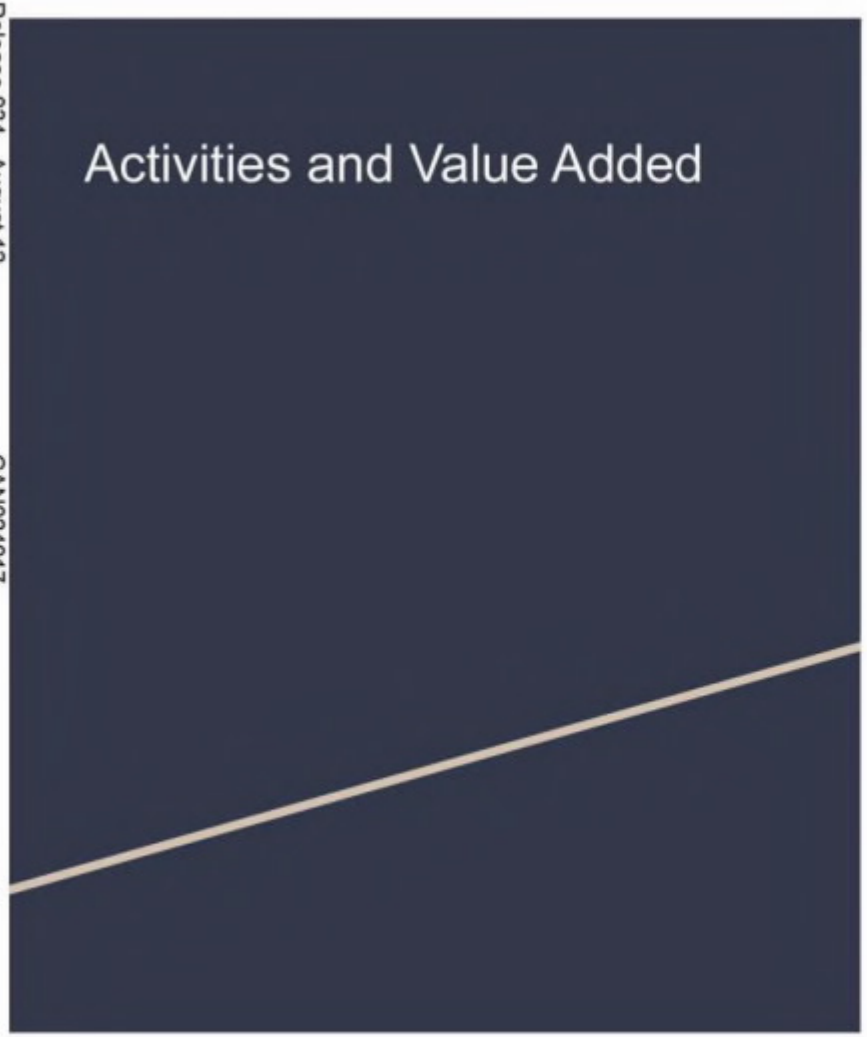
Rapid Response Mechanism Canada
Responding to Information Operations

RRM Canada

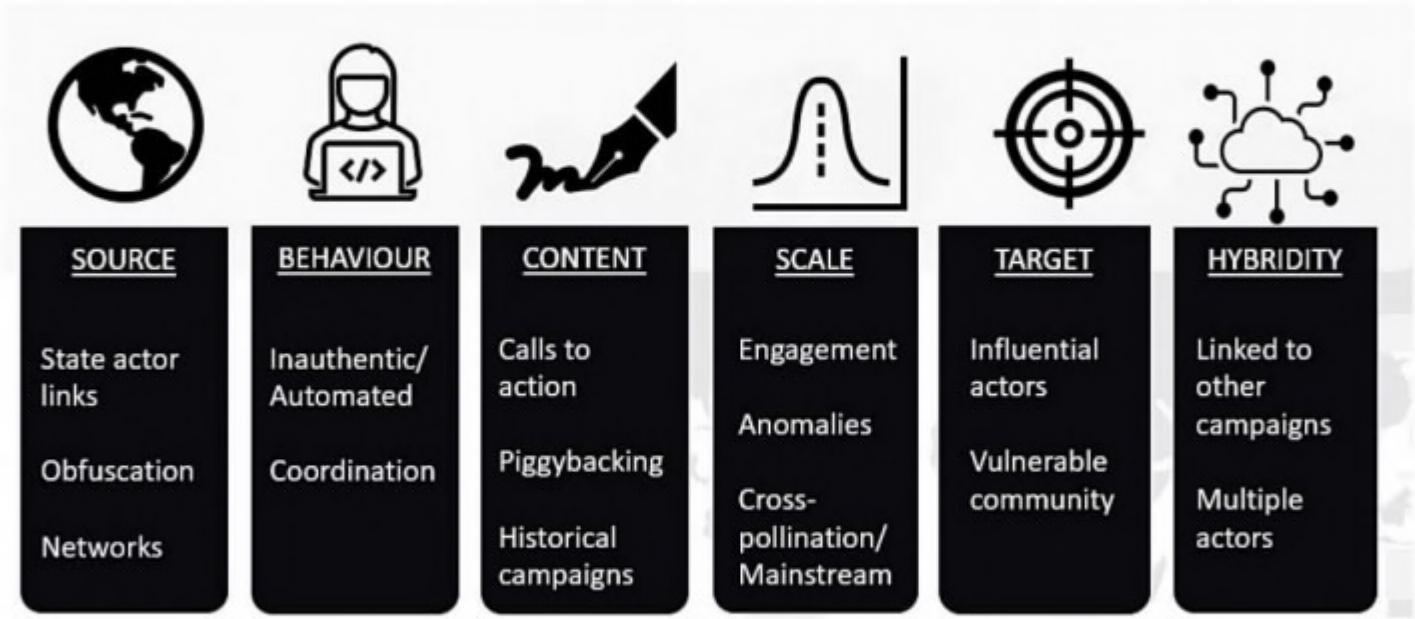
- Set up in 2018
- Housed within Global Affairs Canada, Centre for International Digital Policy
- Comprised of policy and data analysts, divided into three teams: Policy, Russia, and Global Threats/Indo-Pacific
- Mandate:
  - Monitor & detect foreign information operations online
  - Support Canada's electoral integrity
  - Lead multilateral engagement on countering foreign information operations and coordinate G7 RRM



- Open-source methods
- All source situational awareness on priority files (complements traditional intelligence and security reporting)
- Early warning mechanism during election cycles and crises
- Information sharing in unclassified contexts, including with non-state actors
- **Informs and coordinates response to information operations – at home and internationally**

Framework for Open-Source Analysis

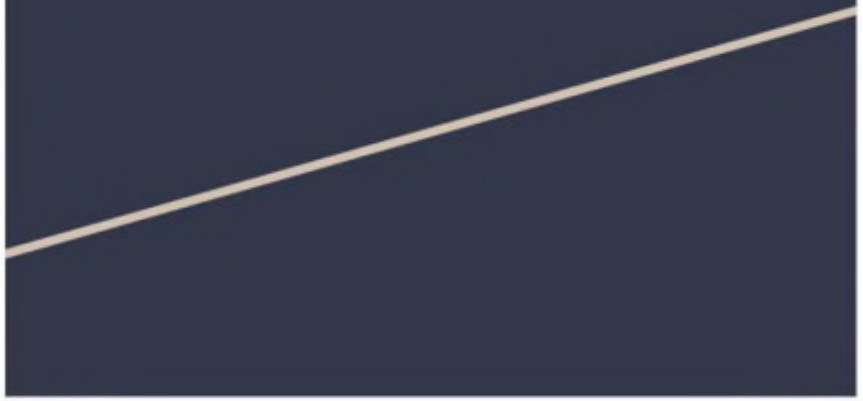
Global Affairs Canada / Affaires mondiales Canada



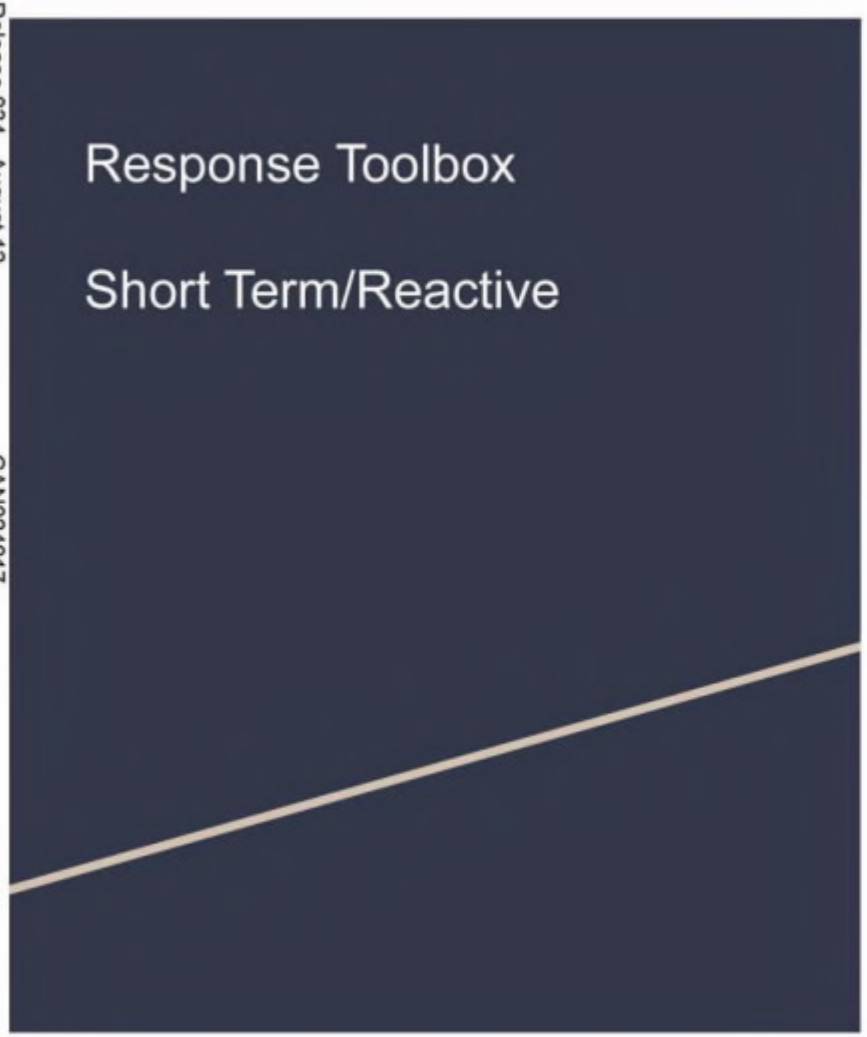
PROTÉGER LA DÉMOCRATIE
MÉCANISME DE RÉPONSE RAPIDE DU G7
RAPID RESPONSE MECHANISM
PROTECTING DEMOCRACY

Response Toolbox

Crisis-driven
Complex
Short and Long-term
Evolving



- Learned from countering COVID 19 and Ukraine-related information operations
- Whole of Government coordination
- Across mandates and silos
  - domestic & international
  - open & classified
  - hard (security) & soft (society, economy)
  - technical & qualitative
- Short & long-term approaches
- Evolution of threats driven by technology (AI)



- Detection & Attribution
- Communications
- Active Cyber
- Platform Engagement
- Diplomatic Engagement
- Sanctions
- Crisis Programming (Funding)
- International Coordinated Response

Response Toolbox

Long Term/Proactive

- Monitoring & Detecting
- Capacity Building
  - Supporting Independent Media & Journalism
- Strategic Communications
- Leveraging international instruments and building norms
  - Declaration on Information Integrity
- Building societal resilience
- Legislative and regulatory frameworks

Ongoing and proactive activities

Reactive activities

Stakeholders

Security and Intelligence Threats to Elections Task Force (SITE)

- Key Mechanism: SITE
- Focussed on electoral integrity – but coordinates outside of elections
- Comprised of:
  - Global Affairs Canada
  - Canadian Security Intelligence Services
  - Communications Security Establishment
  - Royal Canadian Mounted Police

- Privy Council Office
- Public Safety Canada
- Canadian Heritage
- Elections Canada
- Commissioner of Canada Elections

RRM Canada Highlights

Responding to Russian Information Operations

- Dedicated Russia team
- Enhanced RRM Canada
  - Monitoring & Reporting on Ukraine
  - International engagement (G7 RRM and)
  - Concrete initiatives to bolster response - especially in Eastern Europe
- Supported sanctions against disinformation actors
- Supported strategic communications
- Need for expanded focus (e.g., in Africa & the MENA region)

RRM Canada Highlights

Responding to Chinese Information Operations

- Dedicated China/Indo Pacific team
- Monitors PRC information operations
- Uncovered information operations targeting Canada
- Led response to aggressive targeting of a Canadian Parliamentarian
  - Public attribution, including a statement in Chinese
  - Diplomatic engagement
  - Outreach to Tencent
- Spamouflage

Gaps & Challenges

- Whole of government coordination a challenge
- Political sensitivities – occasional bureaucratic paralysis
- Multilateral responses difficult to muster - need to strengthen the G7 RRM response muscle

Slide Notes

Slide 4:

The team is collecting and assessing open-source data along the following indicators. The sum total of all available indicators leads analysts to certain conclusions, with varying degrees of certainty. There are no clear cut thresholds.

My colleague, Alexa Pavliuc, will provide additional information on how RRM Canada conducts its activities during her presentation.

Source:
State actor links
Obfuscation
Networks

Behaviour:
Inauthentic/Automated
Coordination

Content:
Calls to action
Piggybacking
Historical campaigns

Scale:
Engagement
Anomalies
Cross-pollination/ Mainstream

Target:
Influential actors
Vulnerable Community

Hybridity:
Linked to other campaigns
Multiple actors

Slide 5:

Our current national level response framework incorporate a whole of government approach and therefore includes our national-level partners.
Many agencies and departments are involved in combatting foreign threats to Canada
They all have their own mandates but also own expertise
Need to address both long term challenges (resilience) and short term challenges (harmful narrative targetting individuals)

Slide 6:

Monitoring and detecting: includes OSINT reporting, including during Ges; Mission reporting; Classified material
Communications: StratComms and public messaging (incl); G7 RRM Annual Reports; G7 Communiqués and Statements
Diplomatic engagements: range in severity, from condemning to démarching, to denying entry to Canada and expelling diplomats; Leveraging broader multilateral organizations (OECD Mis/Dis Hub); Building alliances of like-minded countries and isolating culprits in multilateral contexts
International coordinated responses: Leveraging leadership of G7 RRM; coordinating with other like-minded groups, such as and
Platform engagements: to support open societies (e.g. G7 RRM Pilot in support of Ukraine integrity); exchange threat intelligence or discuss countering FI (w.e. Tencent)
Crisis programming (funding): GAC funded the G7 RRM-supported Multi-stakeholder Partnership to protect the integrity of Ukrainian information environment
Active cyber: Alignment with CSE's active cyber operation mandate, to ensure efforts reflect Canada's foreign policy priorities.

Building capacity of partners: Programming ; Training; Initiatives to support vulnerable or front-line democracies
Leveraging International Instruments: UN Human Rights Charter; Global Declaration on Information Integrity
Work with Non-State Partners to build societal resilience: work with Civil Society Organizations and industry
Legislative and regulatory frameworks: GAC's engagement with GOC partners who lead on domestic policy developments;

Supporting media and journalism: Supporting the work of journalists and media in countering disinformation

Slide 8:

This chart represents GAC's emerging Response Toolbox on countering FIMI. In the following two slides I will explain these proactive and reactive activities which span across short-, medium- and long-term work.

Ongoing and proactive activities, including the work of RRM Canada, support GAC's foreign policy strategy. These activities are proactive and continuous, but can vary in attention paid to them and usefulness depending on the situation. These activities inform and support the reactive activities that may also be undertaken in the event of an incident.

Reactive activities can be undertaken in response to specific disinformation activities or occurrences. Reactive responses range greatly in scope and severity, depending on the exact circumstances.

Monitoring and attribution: includes OSINT reporting, including during GEs; Mission reporting; Classified material – we strive to achieve attribution based on available data
Communications: StratComms and public messaging (incl); G7 RRM Annual Reports; G7 Communiqués and Statements
Diplomatic engagements: range in severity, from condemning to démarching, to denying entry to Canada and expelling diplomats; Leveraging broader multilateral organizations (OECD Mis/Dis Hub); Building alliances of like-minded countries and isolating culprits in multilateral contexts
International coordinated responses: Leveraging leadership of G7 RRM; coordinating with other like-minded groups, such as and
Platform engagements: to support open societies (e.g. G7 RRM Pilot in support of Ukraine integrity); exchange threat intelligence or discuss countering FI (w.e. Tencent)
Crisis programming (funding): GAC funded the G7 RRM-supported Multi-stakeholder Partnership to protect the integrity of Ukrainian information environment
Active cyber: Alignment with CSE's active cyber operation mandate, to ensure efforts reflect Canada's foreign policy priorities.

Building capacity of partners: Programming ; Training; Initiatives to support vulnerable or front-line democracies
Leveraging International Instruments: UN Human Rights Charter; Global Declaration on Information Integrity

Work with Non-State Partners to build societal resilience: work with Civil Society Organizations and industry
Legislative and regulatory frameworks: GAC's engagement with GOC partners who lead on domestic policy developments;
Supporting media and journalism: Supporting the work of journalists and media in countering disinformation

Slide 9:
- Work closely through SITE during election time to combat foreign interference in our electoral process.

Extended notes on rôle of each agencies:

Privy Council Office
Coordinate work of departments
Leads committees to favour a whole of government approach on foreign interference

Royal Canadian Mounted Police
Investigates incidents of foreign actor interference
Prevent threats and harassment from foreign entities

Canadian Security Intelligence Services
Investigate activities that may cause a threat to the security of Canada, including foreign interference
May take actions to reduce threats

Global Affairs Canada
Contributes to drafting legislation on foreign interference
Monitors and report on the digital environment through RRM Canada
Leads the G7 RRM

Public Safety
Houses a coordination unit focusing on foreign interference
Works at enhancing partnership between federal, non-federal and non-government partners to counter foreign interference
Represents Canada at the

Communications Security Establishment
Responsible for cybersecurity and defensive cyber operations
Provides assessment on foreign threat actors

Slide 11:
GAC dedicated website: https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/response_conflict-reponse_conflits/crisis-crises/ukraine-disinfo-desinfo.aspx?lang=eng

Slide 13:
Working with whole of government means aligning different mandates.
For good reasons, in democratic countries, the government is made of a complex structure of agencies with different mandates.
Can lead to slow change and slow action
Can lead to silo work and duplication of work
Need for commonly shared threat intelligence picture to facilitate shared understanding of threats and, thus, decisions and response

Responding to FIMI threats implies political sensitivities.
Responding to foreign actions involves political risks and sensitives (e.g. does it makes sense for Gov to intervene or should it be civil society-driven response?)
Canada has large diasporas and a diverse population
Directly affects the type of response deemed suitable

Technical limitations: monitoring tools changing, size of data to analyze, etc.
Tools we use evolve alongside social media platforms in sometimes diverging ways.
Constant need to re-assess our capacity and the tools we use
Always need to learn new tactics and methods to monitor the environment
Deplatforming led to multiplication of platforms

Evolving threats and actors: language capacity and cultural expertise required to monitor efficiently.
New threats and the complexity of the digital environment means the need for a diverse workforce
Need to be familiar with the language but also the cultural sensitivities to monitor properly, leading to HR challenges
Constantly evolving adversarial tactics, techniques and procedures (TTPs)

Developing a collective response with partners multiplies the national level challenges of each partner.
Each country has its own complex web of agencies and departments.
If getting things moving in a single country is complex, making it move across multiple settings is exponentially more.
Need to work closely and over the long term to build collective response mechanism:
Common threat intelligence awareness
Common terminology
Clear processes and procedures
Capacity building and reguar exercising, esp due to rotations
Governments must involve CSOs due to trust and transparency issues

Different visions: difficult to establish attribution, thresholds and appropriate tool selection.
For a variety of reasons, it is hard to come to a unanimous agreement on thresholds and/or attribution criteria amongst partners.
Nonetheless vital that we try – this is what G7 RRM established practical working groups (TNR, SNI, Capacity) and on framework/principles (Collective Response)
Deciding what response tools will be appropriate for what threat is also difficult, but based on our respective experiences, it should be possible.