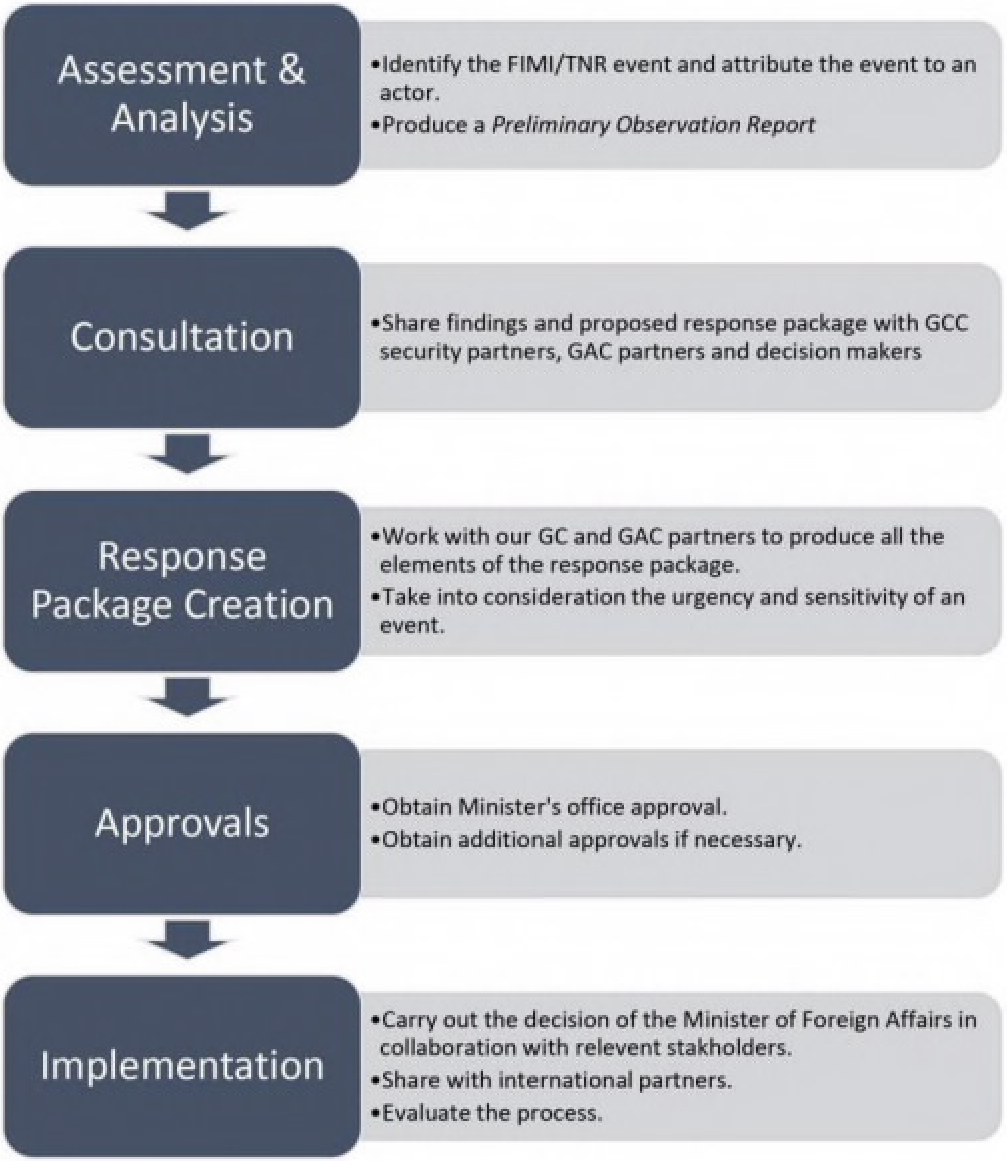
RRM Canada Response Framework to Foreign Information Manipulation and Interference

The purpose of this framework is to outline the process on how RRM Canada responds to foreign information manipulation and interference (FIMI) and transnational repression (TNR) threats to Canada, its strategic interests, and allies. The process is divided in 5 steps that allows for a whole-of-government response package to responsible actors.



Assessment & Analysis

- Identify the FIMI/TNR event and attribute the event to an actor.
- Produce a *Preliminary Observation Report*

Consultation

- Share findings and proposed response package with GCC security partners, GAC partners and decision makers

Response Package Creation

- Work with our GC and GAC partners to produce all the elements of the response package.
- Take into consideration the urgency and sensitivity of an event.

Approvals

- Obtain Minister's office approval.
- Obtain additional approvals if necessary.

Implementation

- Carry out the decision of the Minister of Foreign Affairs in collaboration with relevent stakholders.
- Share with international partners.
- Evaluate the process.

A. Current understanding of the national level response

Part I: Assessment & Analysis

Step 1: Data team alert team of incoming event/incident and its target(s)

- Alert respective IOL deputy director that relays the information to policy team.
- Data team completes the production of a *Preliminary Observation* report.

Step 2: Obtain approval from IOL director to engage response mechanism

- Using the *Preliminary Observation* report, obtain approval from Director of IOL to launch the response process.

Step 3: State actor attribution

- Determine who we can attribute the event/incident to and with what degree of certainty.

Step 4: Release of data team's *Preliminary Observation* report for internal use

- Launch the writing process of the full report for the data team.

Part II: Consultation

Step 5: Obtain validation for findings / receive support to go forward

- Use SITE+ to confirm data and conclusions.
- Share with ADM for awareness.

Step 6: Select response package

- Qualify and determine the urgency and sensitivity of the incident to select the appropriate response package.
- Use the *Targeted response country risk matrix* to choose the appropriate reactive or diplomatic responses to the incident.
- If needed, include civil society, academia or other internal and/or external partners that could contribute to the response package.

Step 7: Alert internal and GoC partners of incident, recommended response package and expected product from stakeholders involved

- Define who needs to be either informed, consulted, or involved to contribute to the package based on how the incident was qualified and rated in terms of urgency and sensitivity.
- Share the *Preliminary Observation* report.
- Book meetings with stakeholders that need to be consulted or contribute.
- Always inform:
  - SITE Task Force members (CSIS, CSE, RCMP)
  - PCO Security and Intelligence and Democratic Institutions
  - Public Safety
- Offer consulted and involved partners a deadline to offer comments and recommendations.

Step 8: Consider and integrate comments and suggestions in the response package

Step 9: Obtain IFM approval with deputy minister

- Obtain confirmation of the response package chosen, deadlines established, and stakeholders involved.

Part III: Response Package Creation

Step 10: Establish a deadline and expectations for implicated teams to produce their parts of the response package

- Deadline would vary depending on the qualifying, urgency and sensitivity of the incident.

(If applicable) Step 11: Engage international partners for coordinated response

- Use approved coordinated response mechanism with international partners.

Part IV: Approvals

Step 12: Share information package for DMCIR

- Provide a complete package of all products and proposed responses for approval.
- Ensure each product in the package is accurately dated.

Step 13: Obtain Ministry's office approval

- Send a complete and DMCIR approved package to the communications branch of oMINA for final approval.

Part V: Implementation

(If applicable) Step 16: Go public and put into action the response package

- For proactive responses/high urgency incidents, put in place response that can be activated early (démarching, statements, denouncing, announcements)
- For non-urgent/proactive, wait for full report and full package of responses that are longer term (sanctions, PNG, website creation)
- Only go public if necessary or possible. Some response package won't allow it.

Step 17: Share our internal documents/findings with our G7RRM partners

- Share findings in our mailing list as soon (at the same time?) as published.
- Adress in more detail in the next Focal Points meeting.
- Which document is shared depends on the sensitivity of the issue.
  - If sensitive (related to MPs, high risk, high secrecy) share only public facing reporting.
  - If judged less sensitive, can share internal documents with partners.
- Ask of them to share and/or support our reporting and statements:
  - Public statements
  - Retweet/tweet
  - Denouncing
- Share with academia and think tanks

Step 19: Reflect and improve

- Have members of the team who took part in any step of the process reflect on the success and challenges of the most recent response process.
- Use lessons learned to improve the process.

B. Proactive response – Mitigate & Enable

Situational Awareness

- OSINT monitoring
- Whole-of-government cooperation
- Work with GAC's intelligence policy teamCollect & save evidence
- Threat assessment

Information Sharing

- Share ad hoc reports on specific incidents
- Share recurring reports
- Focal point meetings
- Report on emerging threats
- Participate in events and collaborative work to publicize and exchange information
- Share information (data, research, assessment, etc.) with civil society and academia
- Share assessments with

Expertise Sharing

- Share training documents/procedures/technical expertise
- Give presentations on best practice or lessons learned
- Give workshop-type training sessions

Public Resilience Building

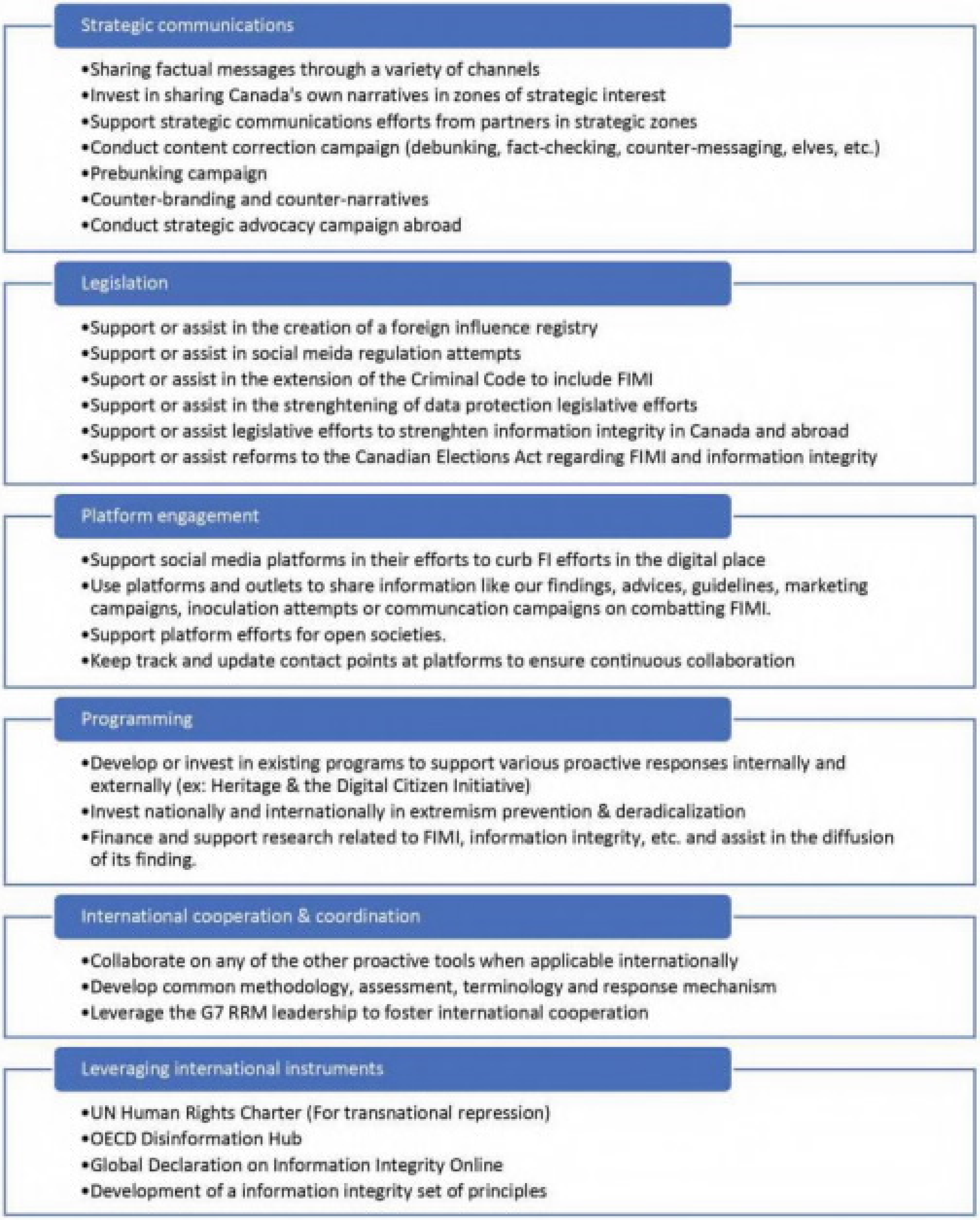
- Support independant media & journalism here and abroad
- Support development of an international journalism program like BBC Media Action (UK)
- Support civil society and local communities of experts to conduct fact checking
- Support/develop national and international level programs to develop digital literacy and public engagement in and out of the education system
- Support public inoculation to inaccurate information and FIMI attempts
- Develop cybersecurity and resilience training for politicians and policital parties
- Work with GoC partners to develop resources for specific targeted groups (LGBTQ, refugees, etc.)
- Work with GoC partners to develop a whole-of-society approach to media literacy, resilience and digital hygiene

Enhanced Transparency

- Declassification and public disclosure of intelligence and reports
- Regular briefing and presentation to the HoC
- Wide publication of OSINT findings
- Promote third party observers in elections and other high suspicion/impact areas

Threat Disruption

- Expose Campaigns
- Tactical information operations
- Active cyber



Strategic communications

- Sharing factual messages through a variety of channels
- Invest in sharing Canada's own narratives in zones of strategic interest
- Support strategic communications efforts from partners in strategic zones
- Conduct content correction campaign (debunking, fact-checking, counter-messaging, elves, etc.)
- Prebunking campaign
- Counter-branding and counter-narratives
- Conduct strategic advocacy campaign abroad

Legislation

- Support or assist in the creation of a foreign influence registry
- Support or assist in social meida regulation attempts
- Suport or assist in the extension of the Criminal Code to include FIMI
- Support or assist in the strenghtening of data protection legislative efforts
- Support or assist legislative efforts to strenghten information integrity in Canada and abroad
- Support or assist reforms to the Canadian Elections Act regarding FIMI and information integrity

Platform engagement

- Support social media platforms in their efforts to curb FI efforts in the digital place
- Use platforms and outlets to share information like our findings, advices, guidelines, marketing campaigns, inoculation attempts or communcation campaigns on combatting FIMI.
- Support platform efforts for open societies.
- Keep track and update contact points at platforms to ensure continuous collaboration

Programming

- Develop or invest in existing programs to support various proactive responses internally and externally (ex: Heritage & the Digital Citizen Initiative)
- Invest nationally and internationally in extremism prevention & deradicalization
- Finance and support research related to FIMI, information integrity, etc. and assist in the diffusion of its finding.

International cooperation & coordination

- Collaborate on any of the other proactive tools when applicable internationally
- Develop common methodology, assessment, terminology and response mechanism
- Leverage the G7 RRM leadership to foster international cooperation

Leveraging international instruments

- UN Human Rights Charter (For transnational repression)
- OECD Disinformation Hub
- Global Declaration on Information Integrity Online
- Development of a information integrity set of principles

C. Targeted reactive response country risk matrix

Potential consequence of response Current state of relations	Low	High
Low	**Strong diplomatic responses** (Sanctions, PNG, limited entry to the country, summoning foreign diplomats for reproaching, bring back diplomatic staff, travel ban) **Public communications** (Name and shame, public statements, speeches, condemning. attribution) **Strong coordinated response** (Seek support from partners in condemning) **Engage in StratComms** (Create or update disinformation databases, push counter narrative, engage civil society) *Ex: Russia*	**Mild diplomatic responses** (Summoning foreign diplomats for reproaching, démarching) **Public communications** (Name and shame, public statements, speeches, condemning. attribution) **Mild coordinated response** (Seek support from partners in condemning (if related to them) or propagate our message through their channels) **Engage in StratComms** (Create or update disinformation database, push counter narrative, engage civil society) *Ex: PRC*
High	**Mild diplomatic responses** (Summoning foreign diplomats for reproaching, démarching) **Public communications** (Name and shame, public statements, speeches, condemning) **No coordinated response** **Engage in StratComms** (Create or update disinformation database, push counter narrative, engage civil society) *Ex: Smaller country with neutral/cordial relations*	**Minimal diplomatic responses** (Summoning foreign diplomats to seek explanations, démarching) **No public communications** (Instead focus on private communications) **No coordinated response** **No StratComms** *Ex: G7 Partner*