KEY MESSAGES FOR BILATERAL ENGAGEMENT

G7 RRM – general

- Rapid Response Mechanism Canada (RRM Canada) monitors the digital information environment for foreign information manipulation and disinformation, including during general elections and by-elections. It also supports Canada's international engagement on foreign state sponsored disinformation and leads the G7 Rapid Response Mechanism.
- The G7 Rapid Response Mechanism (G7 RRM) was established by Leaders at the 2018 G7 Summit in Charlevoix.
- It strengthens coordination between G7 countries to identify and respond to diverse and evolving foreign threats to democracy.
- Since its inception, the G7 RRM has focused on countering foreign state-sponsored disinformation and Russia.
- Under German presidency, the focus extended to broader hybrid threats, including foreign information manipulation and interference (FIMI), transnational repression and sub-national interference. Increasing focus on Indo-Pacific, as well.
- The G7 RRM comprises Focal Points from the G7 community, including the EU. It counts Australia, New Zealand, NATO, the Netherlands, and Sweden as observers.

Bilateral issues on FIMI/Dis

- Glad to see that our Strategic Dialogue is producing enhanced cooperation on important issues, among which also the fight against foreign interference.
- Eager to continue working together as Italy takes the helm of the G7 presidency: we share fundamental objectives like defending Ukraine, a theme that encompasses all aspects of international security, economic and energy security, and climate change policy.
- Canada and Italy are aligned strategically on the need to counter foreign interference and disinformation. We hope that we can continue to expand the discussion with you to reflect our evolving interests in that space, including as it relates to transnational repression and raising awareness of this issue globally.
- Disinformation is present in many issues, such as Sahel/Africa and migration, which have significant impacts on the ground. We welcome stronger ITA engagement through G7 RRM on developing practical, coordinated approaches to countering FIMI/Dis.
- Welcome ITA MFA joining [redacted] in 2022. While important, we need to move beyond StratCom and strengthen coordination across all pillars of response through G7 RRM.
- Practical work could include joint monitoring and reports on FIMI/Dis on Presidency topics, leading to public statements, raised awareness, capacity building and strengthened networks.
- Interested in ITA position, plans and state of internal coordination on countering disinformation, including Russian and PRC state and non-state actors.
- To ensure continuity from the Japanese and German presidencies, a strong agenda on FIMI/Dis issues in 2024 and in advance of the Canadian presidency, the G7 RRM Secretariat proposes to establish bi-weekly working calls under RRM – Germany found them very useful.

BACKGROUND

[APG]

1) Italy's participation in the G7 RRM

- Formally, Francesca Santoro, head of Office VI at Italy's MFA (Hybrid Threats) was the FP, [redacted]
- The newly appointed FP is Alberto dal Degan – started on September 15th.
- [redacted]
-

2) TNR Working Group and Italy's position

- The TNR Working Group was launched in July 2023 and is led by the US through G7 RRM.
- Italy (along with the Netherlands and New Zealand participating as observers) supports the WG in principle [redacted]
- One of the key US objectives for this WG is to develop a working definition of TNR and to implement a publicly communicated joint statement on the TNR phenomena.
- [redacted]

3) Recent multilateral efforts

- Two seminars were organized by UK/US/CAN Missions in fall 2022 to engage with civil society and experts to raise awareness of FIMI/Dis. [redacted]
- The concept for Oct 20th event was proposed by G7 RRM Secretariat to the Canadian Embassy, which recommended to organize it as another tri-lateral seminar to ensure alignment in messages to ITA.
- [redacted]
- In 2022, ITA identified capacity building/knowledge sharing, both among government and CS/academic communities as priorities. MFA asked for the US/CAN/UK support in developing government technical and analytical capabilities.
- Increased capacity and capabilities by CS/academic groups to identify, analyze and produce evidence-based public reports on FIMI cases will raise national awareness on threats and the need for a 'whole-of-society' approach to countering FIMI/Dis.

4) G7 RRM objectives and activities in 2023

- Topics for consideration based on continuing efforts and group consultations:
  - AI & Disinfo (need to identify points of collaboration with G7 GPAI & OECD),
  - Transnational Repression (through G7 RRM WG) – [redacted]
  - Weapons of Mass Destruction disinformation (in collaboration with GP on non-proliferation of WMD)

[APG]

  - Development of response frameworks for countering disinformation (through the G7 Collective Response WG)
  - Development of the G7 RRM Indo-Pacific pillar (analytics-to-StratComm)
- Strengthen coordination inside the group through existing and emerging activities in:
  - FIMI/Disinfo persists across all topics, incl those that may be on Italy's agenda in 2023. Strengthening collective OSINT monitoring/reporting on Africa, food/energy security, migration and others will boost collective awareness and responses.
  - Collective Response WG (EEAS/CAN) – in '23-25 -- develop a collective response framework and operational principles as guidelines for developing national capabilities and processes on countering FIMI (incl. alignment with the GEC Framework).
  - Transnational Repression WG (the US) – in '23-24 -- map existing terminologies and approaches; strengthen coordination and information sharing across foreign/domestic mandates; identify opportunities for coordinated communiques and outline a shared approach.
  - Sub-national interference WG (GER) – in '23-24 – map existing approaches to identifying SNI across sub-federal levels of government; strengthen coordination and information sharing across foreign/domestic mandates; develop a compilation of best practices.
  - Analytics WG (the US) – in '24 -- continue the development of analytical inter-operability through Open CTI platform & DISARM framework to advance shared threat understanding; continue developing tools and methodologies for monitoring, including exercises; support [redacted] campaigns development; facilitate analytics coordination on Indo-Pacific (with CAN).
  - Capacity Building WG (the US/EEAS/CAN) – in '24 -- will be constituted in early 2024 to take stock of existing CB modules/capabilities across the community; survey CB needs across G7 RRM and third parties; develop a joint CB action plan, including offerings, to support the evolution of collective responses and whole-of-democracies countering efforts.
- Ensure that countering FIMI, including disinformation, remains a high priority topic in Leaders' and relevant Ministerial discussions and statements.
- Develop 2024 G7 RRM Action Plan based on the above activities and priorities – Italy's leadership is welcome to move coordinated actions beyond StratComm.

5) [redacted]

[APG]

[redacted]

Responsive lines on related issues:

FI in Canada/electoral interference

- **Foreign information manipulation and interference undermines Canada's democracy and Canadians' ability to exercise their rights and freedoms**.
- GAC, through RRM Canada) supports the work of the Security and Intelligence Threats to Elections Task Force (SITE), whose role it is to prevent covert, clandestine, or criminal activities from influencing or interfering in the Canadian electoral process. The SITE also includes CSE, CSIS and the RCMP.
- As a member of SITE, GAC supports the Critical Election Incident Public Protocol with regular security briefings. Canada is also committed to working with international partners to stop the spread of disinformation that undermines democracies.
- RRM Canada uses OSINT techniques only to identify potential tactics or campaigns. The RRM Canada methodology is available on-line, outlining key protocols and principles. The RRM-related work continues outside the writ period of a general election.
- RRM Canada provides information and updates to the SITE Task Force, and during writ periods, to the Panel as part of Public Protocol. The Panel is empowered to make a public announcement, in case which was not necessary during the 43rd and 44th general elections.
- To counter foreign interference, Canada has been working to update its foreign interference toolkit which includes, among other things, a Foreign Influence Transparency Registry (FITR).
- Canada continues to review the tools and authorities at its disposal to ensure our approach keeps pace with the evolving threat environment and is adapted to the Canadian context.

Foreign interference/TNR

- One of the objectives of the recently created G7 RRM transnational repression (TNR) working group, chaired by the US, is to agree on a working definition of TNR, and eventually to raise awareness of the issue and its different manifestations (extrajudicial killings, cyber threats, coercion, etc.) through public diplomacy initiatives.

[APG]

- Recent incident in Canada involving India is a strong example of transnational repression, and demonstrates importance of collaboration in tackling it. This follows on a number of incidents on which Canada reported publicly, including PRC targeting one of our MPs - Michael Chong – as well as Police Stations and monitoring during GE 44 (2021).

- While the investigation in some cases will have to run its course, hope to build on the momentum created by these incidents to bring our international partners closer together on countering TNR, including as it relates to digital threats and spyware.

- This issue is of central importance for us, and we hope Italy, especially given your role holding the Presidency in 2024, will consider joining the working group as a means to move forward.

- From Canadian perspective, we are looking into ways to demonstrate successes for the RRM, for 2024 and as we start building towards our own presidency in 2025. A publicly communicated joint statement under the TNR WG would be one way to send a strong message and would be a nice deliverable in that sense, possibly under your Presidency.

- Would be pleased to invite our political coordinators to discuss this possibility further.

AI & Dis (from USS notes)

- **Canada is concerned about the use of generative A.I. in the production of state-backed disinformation.** Threat actors like China are increasingly comfortable with generative A.I. to produce deep fakes – i.e. A.I. generated photos and videos that seek to dupe audiences in believing it's the genuine article. As the cost of using and creating these tools goes down, we are worried more threat actors – like Russia and Iran – will use generative A.I. to target Canadians on a regular basis.
- **Social media companies are capricious partners in the fight against A.I. generated disinformation.** Tech titans in Silicon Valley have all signalled that they want a responsible roll-out of generative A.I. technologies to the public. The White House Summit where A.I. top seven companies made a series of voluntary promises to protect users was a positive sign. However, a previous call from some of these tech leaders to pause A.I. development for "6 months" while guard rails could be put in place seems to have gone unheeded; all of these companies are racing to bring A.I. tools – sometimes free ones – to the market.
- **Global Affairs Canada lacks the tools to quickly and definitively identify generated A.I. content.** Global Affairs Canada's disinformation research unit – the Rapid Response Mechanism – is looking for tools to investigate and assess A.I. generated imagery and videos. However, the RRM's assessment is that many market providers of A.I. detection tools are inconsistent, and still leave credible room for doubt. GAC is looking at internal solutions, but producing A.I. detection tools is inherently expensive, and may prove futile as the technology improves.

India Killing

- The PM has stated publicly that Canada is not seeking to escalate or provoke, but is seeking India's cooperation.

[APG]

- As noted by the Prime Minister in the House of Commons, Canadian security agencies have been actively pursuing credible allegations of a potential link between agents of the government of India and the killing of a Canadian citizen.
- Canada is a rule of law country. The protection of our citizens and the defense of our sovereignty are fundamental.
- Canada has relayed its deep concerns to senior officials of the Indian government, including the Prime Minister having raised this personally and directly to Prime Minister Modi at the G20.
- Any involvement of a foreign government in the killing of a Canadian citizen on Canadian soil is an unacceptable violation of our sovereignty.
- We have been working closely and coordinating with our allies on this very serious matter.

MP Chong Report

- In Summer 2023, the Rapid Response Mechanism (RRM) Canada team detected an information operation on the WeChat platform targeting Michael Chong.
- We took action to alert Mr. Chong, raise concerns with PRC officials in Ottawa, and publish our findings to enhance Canadians' knowledge of information manipulation.
- Once we became aware of the activity in June, we conducted our analysis and validated our findings within the Government of Canada, including with members of the Security and Intelligence Threats to Elections (SITE) Task Force.
- The activity sought to spread false and misleading narratives about Mr. Michael Chong, and displayed several indicators of FIMI, including:
  - coordinated content and timing;
  - highly suspicious and abnormal shifts in the volume and scope of engagement; and,
  - the concealment of state involvement.
- We also brought the activity to the attention of the Deputy Ministers Committee on Intelligence Response, which provided advice for how to scope our response.
- While the RRM Canada team discovered the activity while monitoring to support the SITE Task Force during the June 2023 by-elections, the information operation itself was not related to the by-elections.

Police stations

- RRM Canada began looking into the issue following the release of two reports by the NGO Safeguard Defenders (SD) in September 2022 that identified "102 overseas police service stations" run by the PRC in 53 countries.
- RRM Canada solely looked at open-source and publicly available resources to assess the extent that the PRC leverages this network as part of its global influence operations.
- We learned that PRC government entities are using WeChat – a popular messaging and social media service in China – to publicize overseas station services to diaspora communities in Canada, G7 countries, and beyond.
- RRM Canada assesses that Beijing's active publicity of these stations on WeChat may serve as a deterrent to members of the diaspora who disagree with Beijing's domestic and international policies, infringing on their freedom of expression within democracies.
- We recognize this issue is an international problem and therefore studied and shared our findings with our international and domestic partners. We continue to discuss the issue with

[APG]

our partners in the pursuit of a collective response to foreign interference, in particular through the Transnational Repression WG.

- RRM Canada did not find any evidence of overseas police stations operating in Canada beyond what Safeguard Defenders have reported.
- This is a file which is continuing to evolve. We are closely working with partner departments to determine whether there are still police stations operating in G7 countries.

Global Declaration on Information integrity

- [redacted]
- Declaration is a set of high-level international commitments by participating States to protect information integrity online.
- Grounded in international law, human rights treaties.
- Sets out participant States' expectations that industry and online platforms adopt a human rights-respecting approach.
- Builds on the work of the Summit for Democracy Cohort on Information Integrity, the work of civil society (Forum on Information & Democracy) and its reports on the reliability of information
- Complement UN efforts underway such as the Code of Conduct for Information Integrity on Digital Platforms.
- Strengthens existing multilateral and multi-stakeholder efforts to protect the information ecosystem.

[APG]