For Public Release

G7 RAPID RESPONSE MECHANISM (RRM): FACTS AND FINDINGS

G7 RRM – announced at Charlevoix Summit in 2018, is fully operational

- Focal Points identified and met twice; Terms of Reference and information-sharing protocols agreed upon; communications principles and action plan for 2019 developed; progress report endorsed by Ministers in Dinard (France) in April, 2019 (attached); information-sharing infrastructure in place; US State Department-based Global Engagement Center finalising an information-sharing and collaboration platform for RRM use.
- Community of practice on open source data monitoring and analytical activities launched in June, 2019. In addition to G7, interest from Australia, New Zealand, Poland, Lithuania and others. US to host next meeting.
- The RRM Coordination Unit stood up at Global Affairs Canada and incorporated its activities within the broader Government of Canada efforts aimed at safeguarding the Canadian 2019 Federal Elections; serving as an "early warning system" by identifying potential foreign threats though open source data monitoring and analysis (Security and Intelligence Threats to Elections Task Force).

Global RRM Network is growing

- RRM core network comprised of G7 members (guided by foundational documents listed above).
- In recognition of the global nature of the threat, RRM information-sharing network is wider and growing. The close to 400 members include:
  - Like-minded countries: Australia, Lithuania, Netherlands and New Zealand
  - Over 100 specialists

RRM Open Source Data Analysis and Reports

- RRM mandated to address diverse and evolving threats to democracy, but disinformation in focus over the past year.
- RRM Coordination Unit has a limited open source data monitoring and analytical capacity to identify potential foreign interference activity in the digital context, producing the following reports:
  - 9 monthly Canada digital trends reports
  - 6 reports on the Ukrainian elections
  - 1 comprehensive report on the European Parliamentary Elections
  - Several reports on the foreign interference tactics and strategies
- Open source data monitoring and analytical activities subject to a publically available ethical and methodological framework.
- Since January 2019, RRM Coordination Unit producing the RRM Wire – a monthly newsletter which highlights original insight, shines light on new developments and projects, and draws attention to potential partners working in defence of democracy **.**

Outreach, Engagement and Recognition

- RRM Coordination Unit organized 4 speaker series and two training opportunities for GoC employee**s**, including two-day training on hybrid threats delivered by the European Centre of

[APG]

Excellence for Countering Hybrid Threats and a single day workshop focussed on communications implications.

- The work of the RRM is increasingly recognized, within the Government of Canada as well as outside. It has received favourable mentions in the following reports: June 2019 Report of the Standing Committee on Foreign Affairs and International Development; the Atlantic Council's report titled "Democratic Defense Against Disinformation 2.0;" and a report by the Centre for International Governance Innovation (CIGI) and the Alliance of Democracies, titled "Election Risk Monitor: Canada."

Key Foreign Interference Trends Observed by RRM Canada

Based on its open source data monitoring and analytical reports, RRM Canada discerned the following trends in foreign interference:

- **"Meta-trolling"** - seen in US mid-term elections and Ukraine: 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 was designed to call into question the legitimacy of an election or any given piece of information by deliberately associating it with "Russian Trolls."
- **Use of foreign interference tactics by domestic actors -** seen in EU elections: evidence of coordinated inauthentic behavior undertaken by domestic actors – more challenging to identify foreign interference.
- **Narrative Competition** - seen in EU Parliamentary elections: 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 issues (mostly far-right community). Again, increased complexity to identify foreign interference.
- **Account Purchasing** – seen in Ukrainian elections: buying social media accounts of authentic users to leverage for foreign interference activities.

[APG]