



Government
of Canada

Gouvernement
du Canada

[Home](#) → [Canada and the world](#) → [Global issues and international assistance](#)

→ [International human rights, governance and democracy](#)

→ [Rapid Response Mechanism Canada - Protecting Democracy](#)

→ Open data analysis – European Parliamentary Elections: Comprehensive Report

Open data analysis¹ – European Parliamentary Elections: Comprehensive Report

Issue: This open source data report outlines comprehensive findings by the Rapid Response Mechanism Canada (RRM Canada) related to foreign interference during and leading up to the 2019 European Union Parliamentary Elections, May 23-26, 2019. RRM Canada's reporting is informed by in-house analysis and consolidates insights from members of the RRM network. It is important to note that RRM Canada monitors and analyzes all potential cases of foreign interference, regardless of the political party affected or political nature of any given issue.

The objectives of this report are to:

- Shine light on any effort to artificially amplify unsubstantiated or false information challenging the legitimacy and fairness of the UK, Irish or EU democratic and electoral systems; ²
- Identify key issues that were highly divisive and exploited within the context of the EU elections in the UK, Ireland and Italy in order to identify narratives that may transcend borders and be used in other contexts; and
- Identify notable tactics used by malign, foreign actors.

Key Findings

- RRM Canada did not observe significant evidence of state-based foreign interference, or any large-scale, organized and coordinated efforts by non-state actors in any of the case studies examined during the European Parliamentary Elections.
- RRM Canada identified national and transnational actors taking a page out of the Internet Research Agency (IRA) playbook, using the same tactics the IRA used in previous elections, such as the 2016 U.S. Elections.
- The use of foreign interference tactics by national actors makes it difficult to identify foreign interference campaigns with a high degree of certainty.

- The disinformation identified by RRM Canada tended to use authentic information that had been manipulated and distorted by means of misrepresenting its content or context (i.e. “**de-contextualization**”). This tactic allows for the creation of divisive content aimed at undermining social cohesion and reducing trust in democratic institutions by targeting communities susceptible to divisive content, which is based on factual information. This is also in line with a continuing trend where there is a shift from information warfare to manipulation and amplification of divisive narratives through narrative competition.³
- Strategic, inauthentic amplification of divisive and inflammatory content was found around issues related to the following topics: immigration/migration, anti-religious sentiment (Muslim and Jewish), nationalist identity, women’s health, gender-based harassment and climate change. This was likely done by national or international non-state actors.

Challenging the legitimacy and fairness of the UK, EU and Irish democratic system

RRM Canada identified some incidents of coordinated inauthentic behaviour in relation to the artificial amplification of disinformation on social media. However, the available data would appear to indicate that this coordinated inauthentic behaviour does not stem from a foreign state, or large-scale organized non-state actor. Rather, our findings show that national and international non-state actors, likely originating from across Europe and the United States, have most notably (though not exclusively) emulated approaches from the Russian sponsored IRA Playbook used during the 2016 American Presidential Election.

Twitter, Facebook and Reddit⁴ accounts were used to spread divisive and false information to damage and negatively impact social cohesion and trust in democratic processes and institutions. These efforts also included the use of blogs and webpages to host disinformation, as well as coordinated networks of Facebook groups, Reddit accounts and Twitter account networks to disseminate content.

An example of these activities include false and unsubstantiated information on vote rigging, noting Counting Agents with the UK Brexit Party were barred from viewing the vote count. This was amplified through a series of inauthentic and coordinated accounts/networks online⁵ during the voting period to challenge the legitimacy of the electoral process in Nottingham, UK, and the UK more generally.

Use of Divisive Narrative to Undermine Social Cohesion

RRM Canada identified a shift from **information warfare**⁶ to **narrative competition**.⁷ A key trend in the data is the dissemination and amplification of divisive issues such as: immigration, Muslims in Europe, climate change and liberal vs conservative values. What is notable is the strategic pushing of inflammatory and divisive narratives across national borders and global political contexts to engage pan-European, regional and international communities.

Migration/Immigration

An example of this would be the story of “400 African illegal immigrants stormed in the terminal of the Charles de Gaulle Airport in Paris”. This tweet was initially recounted by the NY Post “Footage shows hundreds of migrants occupying French airport terminal”. When this story was picked up by national and transnational alternative and Kremlin-affiliated news sites and blogs, it snow balled, being posted by Voice of Europe, ZeroHedge, Westernjournal, Jihadwatch, Sputnik, Breitbart, TheBlaze, InfoWars, etc. In this instance, a transnational network of actors shared, copied and reproduced divisive content related to a minor local protest with no noted incidents. Suspicious sites picked up this content to reach a broader audience by manipulating what is called Search Engine Optimization or SEO ⁸ and artificially amplified it days before the EU Parliamentary Election by both a network of dubious and unreliable websites, as well as a network of inauthentic accounts on Twitter and Reddit. ⁹ This aided in increasing reach and traction, using near identical, divisive framing of the event, playing on anti-immigrant, anti-African and identity-based sentiment with sensationalized and inflammatory language, and referencing the original content to provide the illusion of validation in reporting.

Health and Reproductive Issues ¹⁰

Another example is an attempt to sow division and further polarize communities around an already highly charged topic. In the Irish context, RRM Canada found national and international non-state actors manipulating and framing authentic information from the public Health Service of Ireland using inflammatory and divisive rhetoric about abortion and pregnancy “remains.” This information was amplified and targeted at susceptible audiences, both local and international through coordinated activity.

This tactic is valuable in transferring a narrative from one community to another, amplifying its significance, and targeting those susceptible to inflammatory and sensationalized content in order to affect discourse around divisive issue across states, Europe and internationally. A narrative may be altered slightly for different audiences, but the core aspects of its framing and messaging are transmitted regardless of the source.

Additional Tactics and Approaches of Note

RRM Canada observed a number of noteworthy tactics employed throughout the EU. One tactic is the use of manipulated authentic information posted on untrustworthy websites, blogs, and by questionable journalists or inauthentic accounts to seed conversations. The information is then picked up and framed using a divisive and inflammatory narrative by a broader network of accounts, websites and blogs ¹¹ referencing the original posting to substantiate their story. Finally, this information is amplified by networks of inauthentic accounts in a coordinated fashion. This information targets susceptible communities and may be translated to various languages to target broader political contexts and audiences. RRM Canada describes this tactic as “de-

contextualization,” as the basis of the information is authentic content that is manipulated and distorted. A version of this tactic has been observed as being used by Kremlin-linked actors and is a known tactic of covert, malicious foreign actors. ¹²

A similar but notable tactic for amplifying content, and strategically translating and pushing it into new communities, was observed in our Italian case study. In this case, the initial content focused on Euroscepticism and anti-globalist sentiment and conspiracy. Using a speech by Italian Deputy Prime Minister Matteo Salvini, content was initially spread and amplified through a set of inauthentic and coordinated accounts. It was then strategically targeted at influential and well-known authentic online actors in order to have it boost engagement. Finally, the content was translated into four different languages and amplified again by systematically pushing it in these four separate communities simultaneously, in order to increase reach and prominence in ideologically similar European discussions and communities.

RRM Canada also noted a small incident of likely inauthentic accounts claiming to be progressive Muslims engaged in discussions with falsely amplified accounts opposed to immigration and multiculturalism ¹³, while also being embedded in an inauthentic network. What was notable about these accounts was that they used hashtags and language characteristic progressive actors, but also prominently displayed their Muslim identity and the intention for a “Muslim takeover” of the west. They were then used as examples of incendiary content by various groups opposed to immigration and multiculturalism. RRM Canada believes these to be experimentation with new tactics meant to provoke and act as a means to further and artificially aid in polarizing societies over wedge issues.

Concluding Remarks

Our findings are consistent in a number of ways with other experts in this field. Notable findings from published reports illustrate the impact of tactics like narrative competition, and the emergence of new actors using well-known information operation tactics, particularly non-state actors. ¹⁴ Some experts found instances of state-based foreign interference, including on platforms like Facebook, Reddit and Medium, while noting amongst the various findings the emergence of the tactic of planting, seeding and systematically amplifying false information across platforms and other information sources. ¹⁵ In relation to the EU Parliamentary Elections, a key insight from RRM Canada is that while no significant evidence of state-based foreign interference was observed, the digital ecosystem is ripe and ideal for exploitation by foreign malign actors. ¹⁶

Released: 18 July 2019

Disclaimer: Rapid Response Mechanism Canada monitors and shares information consistent with Canada’s privacy laws and the Ministerial Direction for Avoiding Complicity in Mistreatment by Foreign Entities. The information sharing practices of Global Affairs Canada are subject to review by the Privacy Commissioner, the Information Commissioner of Canada, the Office of the Auditor

General and the National Security and Intelligence Committee of Parliamentarians, among others. Nothing in the present document shall be construed as adding any obligation or normative commitment under international or national law for any G7 member.

Footnotes

- 1 The purpose of Open Source Data reporting is to assist in charting trends, strategies and tactics in foreign interference. Prepared by RRM Canada, this work supports the G7 RRM – an initiative announced in 2018 in Charlevoix, mandated to strengthen coordination to identify and respond to diverse and evolving threats to G7 democracies, including through sharing information and analysis, and identifying opportunities for coordinated response
- 2 RRM Canada has selected 3 cases (UK, Ireland and Italy) based on initial research, linguistic limitations, and most importantly, it is an attempt to fill in gaps in the RRM networks coverage and support cases looked at by partner organizations. This approach was meant to ensure a more complete understanding of foreign interference within the context of the EU Parliamentary Elections.
- 3 Also noted by partner organizations, including a recent report from the Institute for Strategic Dialogue (2019).
- 4 Focus on these specific platforms was due to limitations in access, and indicators of key points of engagement.
- 5 This incident showed no evidence of being linked to a foreign actor, according to information available to RRM Canada.
- 6 Please see: New Knowledge. 2019. “Tactics and Tropes of the Internet Research Agency,” for further information.
- 7 Competition for the way an issue is framed within public discourse, with each framing looking to become the dominant method of conceptualizing said issue, is referred to as “narrative competition”. Please see the Institute for Strategic Design (2019). “2019 EU Elections Information Operations Analysis” for further explanation.

- 8 Search engine optimization is the process of affecting the online visibility of a website or a web page in a web search engine's unpaid results. It is a measurable, repeatable process that is used to send signals to search engines that a webpage is worth showing in Google's index. Though this process should occur organically by users visiting a website, this can be manipulated by multiple tactics to give an inauthentic SEO score thus artificially amplifying content.
- 9 The Twitter network of inauthentic accounts was observed as central to various attempts at amplification. Reddit posts targeted ideologically similar groups, such as *The_Donald*, *New Right* and *The_Europe*.
- 10 According to Ireland Health Services Executive this falls under: Unplanned Pregnancy Support Services.
- 11 This includes several pro-Kremlin sites including, Zerohedge, RT, and Sputnik, as well as other alternative media sites.
- 12 See DRF Lab's work on the EU Parliamentary Elections.
- 13 Only two accounts were observed exhibiting this inauthentic and dubious behaviour, and were taken down in advance of the election period. RRM Canada assesses that this is representative of the potential testing of a new tactic.
- 14 Please see the Institute for Strategic Design (2019). "2019 EU Elections Information Operations Analysis."
- 15 Please See: Digital Forensics Research Lab. 2019. "Top Takes: Suspected Russian Intelligence Operations." June 22, 2019.
- 16 It must be noted that the findings of this report may differ from other reports that have used or have access to other source data and information, had different objectives or monitored for a longer period of time.
-

Date Modified:

2019-09-03

