Election
Monitoring

May 2019

# Disrupted: Evidence of Widespread Digital Disruption of the 2019 European Parliament Elections

Compiled by

AVAAZ

ISD | Powering solutions to extremism and polarisation

With support from Digital Action

## This briefing brings together the observations of a coalition of organisations who monitored the digital environment during the 2019 European Parliament Elections to identify disinformation, disruption or interference campaigns, as well as the technology platforms' responses to it.

This briefing includes:

# 1. Introduction

Disinformation, inauthentic activity, and online attacks were widespread. For instance:

- Networks of Facebook pages in Germany, France, Italy, Poland, Spain, and the UK that were using disinformation tactics gathered over 750 million views in 3 months across the EU before they were taken down by Facebook
- 200,000 fake accounts were found supporting the far-right AfD right up to the elections
- In the UK alone, 42% of the most active accounts supporting official party Twitter handles showed signs of bot-like behaviour

It is likely that the evidence we, as a small number of users, have gathered on disinformation, inauthentic activity, and online abuse is only the tip of the iceberg, compared to what the companies have the responsibility and the means to reveal, but didn't.

As set out below, this is an illustration of how platforms' responses in a number of areas fell far short of their commitments in the self-regulatory Code of Practice, which was intended to protect European democracy.

We stand ready to work with the Commission on more effective policy measures, including regulation, to protect democracy and freedoms in Europe.

The Evidence: Part 1

# Disinformation and Inauthentic Accounts

The digital disruption techniques deployed in these elections were more sophisticated than previous so-called 'fake news' efforts, instead with a longer arc 'culture war' dynamic around issues like migration, Muslims in Europe, family vs. progressive values and increasingly climate policy.

The information here is just what small teams of civil society actors with limited resources have been finding in a selection of countries, *without* the transparency that platforms enjoy. This suggests there is a sea of disinformation which is not being identified or acted upon.

In-authentic and coordinated amplification:[1]

- Professor Trevor Davis, George Washington University, uncovered 200,000 pro-AfD fake accounts in Germany spreading electoral content.
- In Spain, ISD reported a network of over 2,000 accounts to Twitter, which were boosting Anti-Islam hashtags and amplifying support for Vox, including a mixture of bots and inauthentic accounts (see report here, p. 4).
- Almost 700 suspect pages and groups reported to Facebook by Avaaz, which were followed by over 35 million people and generated over 76 million "interactions" (comments, likes, shares) in the last three months (see initial report here). Facebook has taken down 132 of the pages and groups reported, accounting for almost 30% of all interactions across the reported networks.
- In the UK, ISD demonstrated that support for most major parties on Twitter was boosted by suspected bots. 42% of the most active accounts supporting official party Twitter handles showed signs of bot-like, hyperactive behaviour (see report here, p. 5).

Disinformation and illegal content:

- Avaaz uncovered mainly far-right disinformation networks in France, UK, Germany, Spain, Italy and Poland, posting content that was viewed an estimated 763 million times over the past three months, before finally being removed by Facebook. That is an average of 6 million views per day.
- In Poland, ISD identified a suspected coordinated network of pages, accounts and groups on Facebook used to promote nationalist party Konfederacja and to amplify anti-Semitic and pro-Kremlin content. This network included 60 pages with a total of 194,675 followers and 5 groups with a total of 23,187 members.
- An estimated 9.6 million Spanish voters saw disinformation on Whatsapp, as revealed in a study by Avaaz.

Attacks on public figures:

- In Germany, Spain, Italy and France, ISD evidenced online attacks on public figures, particularly female public figures, including hate speech campaigns, disinformation campaigns and physical threats against political figures in France, Spain and Germany. These attacks threaten the rights of women to safely participate in democratic processes.
- A website attacking an Irish gay, female MEP candidate was promoted via Google ads. It was only removed when highlighted by her party (party press release)

[1] More country-specific information is available in the reports (hyperlinked) from Avaaz and ISD.

The Evidence: Part 2

# Platform Response

The platforms' actions and procedures ahead of the elections were ineffective in preventing digital disruption. The limited self-regulatory commitments made to transparency and integrity of services were not only poorly and sporadically enforced, but also by design focused on paid content and not enough on (much more common) organic content, networks and accounts.

In some cases platforms took steps that were even counterproductive, giving malicious actors an electoral advantage over those respecting European laws. In Germany, Twitter's attempts to enable speedy reporting of disinformation was gamed by far-right networks, resulting in overzealous takedowns of legitimate political and media content. This included removal or suspension of the accounts of anti-AfD activists and Jewish-interest newspapers, as well as of victims of harassment (rather than the perpetrators).

**Ad transparency: issues with the platforms' responses**

In March, scores of experts from across Europe set out what an ideal ad archive Application Programmable Interface ("API") should look like. The practices of Facebook and Google fell well short. The main issues are below, with more detail from Mozilla on Facebook's API here.

**Problems with design:**

- Lack of engagement data, which means you can't tell whether an ad is particularly viral (and therefore gaining significant free reach). The hunt for virality encourages speech at the edges of acceptability, and therefore polarises politics.
- Lack of targeting data: users can't understand how they're being reached and why
- Irregularities in the search results
- Limits to bulk-access: a user is allocated on average 171 API requests per country per day (there were, for instance 300 candidates in the Netherlands alone). The API returns only 25 ads per page by default, and each request for an additional page counts against a user's limit of API requests.
- No guarantee of completeness: without knowing ahead of time the complete and precise set of words and variations used by all advertisers in all countries in all languages, a user cannot retrieve the full set of political ads from the Facebook Ad Library API.
- Google didn't specify which ads were on YouTube or which ones were displayed next to search results
- Sharing political ads on Facebook removes the 'paid for' line
- Google didn't include issue-based ads. Facebook did but decided themselves what to flag as 'political' - resulting in lots of false positives

**Problems with implementation:**

- False positives
  - Mainly commercial ads: Ikea, cosmetics, games etc
- False negatives: adverts from AfD support pages and Identitarian groups were missing from the German political ads library
- Late timing for roll-out and inconsistent state, demanding constant adjustments by users
- Mandatory registration process (that should have prevented foreign forces to buy ads in an EU country) have failed (Bits of Freedom story).
- Long delays were reported for legitimate candidates to have their ads processed. Facebook said in an email that a 72 hour delay should be expected
- Weak format/presentation of the data: it's hard to deduplicate what you see, impossible to know what you're looking for unless you know you're looking for it, and you can't request back data (i.e. if a regulator wanted to know levels of spend during a regulated period, they couldn't get that information)

For more information contact:

Nick Martlew
info@digitalaction.co
digitalaction.co