The EU Framework Against Disinformation: What Worked, What Changed and the Way Forward
This report was written by Bruno Lupion. The publication is a result of a project carried out by Democracy Reporting International, with financial support from the German Foreign Office, that encompassed two roundtables in Berlin with civil society organisations and representatives from internet platforms in March and June 2019. The meetings were supported by the Mercator Foundation and organised by Gregor Darmer (Mercator Foundation), Michael Meyer-Resende (Democracy Reporting International) and Rafael Goldzweig (Democracy Reporting International) as the moderator.

The meeting participants included Julia Ebner (Institute for Strategic Dialogue), Darren Hamston (Cardiff University), Naheme Marchal (Oxford Internet Institute), Rachel Levin (Who Targets Me), Jules Darmanin (FactCheckEU), Luca Hammer (independent expert), Armin Rabitsch (Wahlbeobachtung.org), Daniel Fazekas (Bakamo.Social), Curt Benjamin Knüpfel (Weizenbaum-Institut), Semjon Rens (Facebook Germany), Lars Thies (Vodafone Stiftung), Raymond Serrato (Avaaz), Till Eckert (Correctiv), Iskra Kirova (Open Society Foundation), Nina Morschhäuser (Twitter Germany).

30 August 2019
The EU Framework Against Disinformation: What Worked, What Changed and the Way Forward
Table of Contents

1. Executive Summary ................................................. 5
2. European Union's Actions Ahead of the EP Elections .......... 7
3. Civil Society Initiatives on Social Media around EP Elections .... 15
4. Initiatives by social media companies ................................ 18
5. Legal Framework ................................................. 26
6. Recommendations .................................................. 27

Annex: Timeline of activities and initiatives ......................... 29
Before the 2019 European Parliament Elections, many analysts were deeply concerned that these elections could be marred by online disinformation, as seen in the 2016 US Presidential elections, 2016 Brexit campaign and 2018 Brazilian elections. European institutions, civil society organisations and internet platforms took action to reduce the spread of disinformation, increase the cost for anti-democratic actors and raise awareness amongst the public. Disinformation in the EP elections appeared less prevalent than in other elections, but the problem is not solved. Anti-democratic actors, domestic and foreign, have not disappeared and disinformation technology is evolving. In addition, democracy is threatened, not only by hostile actors, but by the unintended consequences of how social media platforms are designed. These threats exist around the clock and not only during elections. Consequently, European actions in the context of the EP elections were only the beginning.

To contribute further on how to reduce online harm to democracy, this report analyses initiatives taken by European institutions ahead the 2019 European Parliament elections. This report is based on desk research and interviews focusing on the European Commission, civil society organisations and internet platforms. What worked? What did not work? What could be further developed and improved?
**What Worked**
The European Commission had four objectives: improving detection, analysis and exposure of disinformation; strengthening coordination and joint responses; mobilising the private sector to tackle disinformation; and raising awareness and improving societal resilience.

It began to build an EU hub to spot and compile disinformation campaigns developed by foreign powers, laid the foundations of a coordinated approach among Member States and pushed internet platforms to improve self-regulation.

**What is Lacking**
Coordination was weakened, because Member States have different capacity and willingness to monitor disinformation within their borders. The self-regulatory approach is also missing enforcement tools and allowed internet platforms to act disproportionately across European countries. Also, the EU does not have the mandate to act against disinformation produced or spread by actors based in the EU.

**What Worked**
Facebook, Twitter and Google, adopted specific policies to raise transparency of political ads and confirm identity of advertisers. They also improved their automated systems and set up dedicated teams to block fake accounts and take down networks engaging in coordinated inauthentic behaviour. Algorithm tweaks and partnerships with fact-checkers were implemented to prioritise credible content and shrink the spread of disinformation.

**What is Lacking**
The companies fell short in several aspects. Their capacity to systematically spot and take down malicious networks was challenged by findings of several civil society organisations. Facebook Ad Library’s interface (API) to allow downloading of political ads data had several bugs that hindered analysis, and Twitter and Google failed to account for issue-based ads in their transparency policy. Moreover, technical improvements were not available in all Member States ahead of the EP elections.

**CIVIL SOCIETY**

**What worked**
Civil society organisations played an important role in understanding the intricacies of this issue, identifying trends and blind spots in strategies to counter disinformation, and locating and reporting coordinated campaigns. This was done by exchanging experiences among organisations, and in a context of scarce resources and with challenges to accessing relevant data.

**What is Lacking**
Absence of coordination between countries and aspects to be monitored led to overlaps and blind spots. There is no common methodology of monitoring social media and quality standards differ widely. Some reports were un-transparent regarding their methodology. Also, some of the findings were not reported to internet platforms in order to act ahead of the EP elections.

**RECOMMENDATIONS**
The European Union should build stronger analytical capacity and coordination among its bodies engaged in monitoring disinformation from foreign-powers, foster coordination and preparedness among Member States and consider co- or normal regulation for internet platforms on political ads and transparency on algorithm choices and ranking systems that affect democratic debate. The discussion of the Digital Service Act, expected to be presented by the European Commission in end of 2020, will be crucial in this regard.

Two current trends on disinformation techniques are: Foreign-born messages being spread via individuals based in the EU that work as proxies, and EU domestic actors learning and reproducing disinformation strategies to achieve political aims. The European Commission faces institutional limitations making it difficult to tackle them directly. It cannot monitor and comment on debates within the EU, so it should leave this task to civil society organisations, that do not face legitimacy constraints to investigate that kind of disinformation and have already demonstrated the capacity to do so. The EU should support civil society organisations in their monitoring efforts between elections and in facilitating activities in all Member States.

**Internet platforms** should improve their APIs to allow researchers and journalists to query data easily from their ad libraries, strengthen partnerships with fact-checkers, develop closer collaboration with civil society organisations and governmental agencies and revamp their self-regulation. Essential to all civil society and academic enquiry is the access to data through Facebook’s API. Privacy concerns are manageable in this context, as the research interest relates to public pages and discussions.

**Civil society** should increase coordination with tech companies to transform findings into actions, develop common reporting standards and increase cooperation among themselves.
2. EU ACTIONS AHEAD OF THE EP ELECTIONS

With concerns about social media disinformation campaigns multiplying and the European Parliament elections approaching, in 2018 the European Commission took several steps to tackle the risks of online disinformation. It

- Convened a High-Level Expert Group to discuss how to address the issue
- Created and financed a task force focused on countering Kremlin-led disinformation campaigns
- Developed a secure online platform for Member States to share data and trends about disinformation campaigns
- Fostered coordination of national electoral networks
- Required internet platforms to develop and sign to a self-regulatory code to fight disinformation and used it to press the companies to do more and better ahead of the EP elections

Fears of a cross-country foreign-born massive campaign did not materialise, but disinformation took place locally in Member States. After the EP elections, the Commission concluded that it did not find a "distinct cross-border disinformation campaign from external sources specifically targeting the European elections", but at the same time collected evidence of "continued and sustained disinformation activity by Russian sources"\(^1\), referring to localised cases documented by the East StratCom Task Force. The initiatives from the European Commission built resilience and raised the cost of developing those campaigns, but disinformation actors are also evolving.

Table 1, on the next page, gives an overview of initiatives taken by the European Commission:

---

1 To support this claim, the EC cites that "the number of disinformation cases attributed to Russian sources and documented by the East Strategic Communication Task Force since January 2019 (998) doubled as compared to the same period in 2018 (434)\(^7\). It is not possible to conclude, based on that data, that disinformation cases increased, as the leap might have reflected better spotting capabilities of the Task Force."
<table>
<thead>
<tr>
<th>Pillars</th>
<th>Main actions</th>
<th>Results</th>
<th>Weak points</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Improve detection, analysis and exposure of disinformation</td>
<td>Budget and more staff to East StratCom Task Force</td>
<td>Task Force is established as an EU hub to spot and compile pro-Kremlin disinformation and inform EU policymaking.</td>
<td>Restricted to Russia’s campaigns, does not have the mandate to act against domestic disinformation.</td>
<td>Remains active after EP elections.</td>
</tr>
<tr>
<td>Strengthen coordination and joint responses to disinformation</td>
<td>Rapid Alert System</td>
<td>A network of contact points from EU Member States and institutions to exchange reports, trends and findings about disinformation and to send alerts in case of state-sponsored coordinated campaigns.</td>
<td>Participation of Member States heterogeneous, and system might not be able at this point to detect and react to subtle and whitewashed disinformation campaigns</td>
<td>Remains active after EP elections.</td>
</tr>
<tr>
<td></td>
<td>European cooperation network for the EP elections</td>
<td>Convened authorities to cooperate in the preparations for the EP elections and facilitated exchange of information, such as data protection, transparency of political advertising and engagement with social media platforms.</td>
<td>Level of cooperation and formalisation of national networks is heterogenous among Member States</td>
<td>Remains active after EP elections.</td>
</tr>
<tr>
<td>Mobilise private sector to tackle disinformation</td>
<td>EU Code of Practice on Disinformation</td>
<td>First self-regulatory step at the EU level. Process of discussion and implementation was leveraged by the EC as an instrument to put pressure on the internet platforms to do more and faster ahead of the EP elections.</td>
<td>Code of Practice has no key performance indicators to assess compliance of signatories. It also does not establish enforcement and sanction mechanisms.</td>
<td>Will be reviewed by the end of 2019.</td>
</tr>
<tr>
<td>Raise awareness and improve societal resilience</td>
<td>Media literacy initiatives</td>
<td>New directive requires internet platforms and Member States to foster media literacy. EU organised the European Media Literacy Week in March 2019, awareness-raising activities targeting multipliers and distributed material on attempts by Russian sources to interfere in electoral processes</td>
<td>Media literacy is applied on small scale in schools, and implementation of additional policies depend on each Member State</td>
<td>Member States should report on the implementation of the directive by December 2022</td>
</tr>
<tr>
<td></td>
<td>Independent network of fact-checkers</td>
<td>Horizon 2020, an EU Research and Innovation programme, funded initiatives to provide support for European fact-checkers and find alternative solutions to disinformation.</td>
<td>Projects aim at a longer term and did not produce results ahead of the EP elections. There is some overlapping with other initiatives from civil society.</td>
<td>Projects will be developed until the end of 2021.</td>
</tr>
</tbody>
</table>
2.1 EAST STRATCOM TASK FORCE

The East StratCom Task Force, a body of the European External Action Service, was set up in 2015 to address Russia’s disinformation campaigns. It gathers disinformation narratives, exposes trends and methods and publishes findings on the EUvsDisinfo.eu website, in a newsletter and on social media. False and incorrect claims in line with pro-Kremlin disinformation messages are tagged and indexed in a database. It also flags suspicious activities to internet platforms.

The EU has other two similar task forces, the Western Balkans Task Force, for the Balkan States, and the Task Force South, for countries in the Middle East, Northern Africa and the Gulf region. They have begun to counter disinformation also but relying on only one analyst for both task forces.

The East StratCom Task Force became an established hub at the EU level to spot and compile pro-Kremlin disinformation and inform policymaking at EU institutions. It benefits from close cooperation with civil society organisations, that forward disinformation stories to be added to the task force database.

Its mandate is restricted to find and debunk Russia’s disinformation campaigns and therefore does not includes those coming from EU domestic actors. This limitation might leave out of the Task Force’s radar disinformation messages originated in Russia, but that were spread by individuals or organisations in the EU that might act as proxies. Even if it spots those disinformation messages, exposing them carries institutional risks as the Task Force might be accused of interfering in public debates within the EU. Moreover, debunking is reactive and has limited outreach. Debunking messages are often not read by those who were exposed to the disinformation pieces.

Recommendation

Dealing with Russian disinformation spread by individuals and organisations based in the EU, recruited or not by the Kremlin, is a complex issue for the East StratCom Task Force, as it might be accused of acting internally as a “Ministry of Truth”. One workaround would be to put more analytical effort to track if the message originated in Russia, but this would not reduce the institutional risk for the Task Force. Another option is to leave this task to civil society organisations, which face less constraints to investigate this kind of disinformation. Also, there is room for the Task Force to rely more on data analysis to spot disinformation campaigns originated from Russia.

2.2 RAPID ALERT SYSTEM

The Rapid Alert System, launched in March 2019, is a closed online platform for EU institutions and Member States to attribute disinformation campaigns and to respond to them. It is accessed by contact points nominated by each EU Member State and EU institutions and moderated by the StratCom team of the European External Action Service. The system remains active after the EP elections².

The Rapid Alert System fostered a degree of cooperation among some Member States.

Only a few member states participated consistently including France, Germany, the UK and the Baltic States. Around half of the Member States did not add information. This might be due to the absence of monitoring systems at the national level, or a consequence of denying the problem. There was a constant flow of information in the system ahead of the EP elections, but no alert was triggered. This might have happened due to a strict definition of which elements of foreign interference should be identified to trigger an alert, and to the absence of clear cross-EU disinformation campaigns around the election. The system

² The G7 also established in June 2018 a Rapid Response Mechanism, to share data and analysis about threats to democracy, including disinformation campaigns. It is managed by the Canadian Ministry of Foreign Affairs.
might not able at this point to detect and react to more refined, granular disinformation campaigns. Lastly, there are calls for more transparency, to allow researchers and journalists to know the number of incidents shared in the system and the participation of each Member State.

Recommendation

The EU should persuade and support Member States to establish or improve their national monitoring systems, such as a national StratCom, which in turn would strengthen the inputs received by the Rapid Alert System. Demand for more transparency could be partially fulfilled by regular reports with figures and statistics on the use of the system.

2.3 EUROPEAN COOPERATION NETWORK FOR THE EP ELECTIONS

The EP elections are organised by Member States, which have different types of election management bodies. In February 2018, the EC asked these national authorities to identify best practices to spot and manage risks to the electoral process from cyber-attacks and disinformation.

In September 2018, the EC recommended that each Member State should establish a national election network, to secure exchange of information on threats and findings and the liaison on the enforcement of rules in the online environment. It also asked Member States to appoint contact points to take part in a European cooperation network for the EP elections.

This network was supported by the EC, which convened meetings of the contact points for practical exchanges on how to protect elections. The network remains active after the EP elections and contact points will be convened in bi-annual meetings. The outcome of the work of the Rapid Alert System is shared with the network, and for some Member States, the contact points for the Rapid Alert System and the network on elections are the same.

The network helped authorities to collaborate in the preparation for the EP elections and facilitated exchange of information on things like data protection, transparency of political advertising, engagement with social media platforms and the role of media regulators.

Recommendation

The level of cooperation and formalisation in national networks is different among Member States, influencing their participation in the European network.

Recommendation

Members States that do not have well-established national cooperation networks should engage in such initiatives.

2.4 CODE OF PRACTICE

The EU Code of Practice on Disinformation is a list of commitments to tackle online disinformation signed by internet platforms and the advertising industry, that came into force in January 2019 and presented as a self-regulatory instrument. Facebook, Twitter and Google participated since the beginning, and Microsoft joined them in May 2019. The Code was initiated by the EC.

The Code of Practice includes commitments on five areas:

- **Scrutiny of ad placements**: to hinder monetisation of financially driven disinformation
- **Political and issue-based advertising**: to increase transparency related to political and issue ads and block malicious actors from using ads for disinformation campaigns
- **Integrity of services**: to remove fake accounts, block or expose bots, and identify and take down networks engaging in coordinated inauthentic behaviour
- **Empowering consumers**: to reduce the outreach of disinformation, raise the outreach of trustworthy content and increase transparency on who runs pages and accounts

---

• **Empowering the research community:** to enable privacy-compliant access to data held by internet platforms

The EC required the internet platforms to submit monthly reports from January 2019 to May 2019 on the implementation of the code, that were made public by the Commission together with calls for the platforms to step up action.

The signatories will evaluate the effectiveness of the Code and discuss and propose follow-up actions on a report expected to be released in October 2019. The EC will provide an independent assessment about the code, carried out with the help of the European Regulators Group for Audio-visual Media Services (ERGA), expected to be released by the end of 2019. Should the EC conclude that the Code of Practice is not sufficient, it may propose normal regulation to address the issue.

The Code of Practice was the first self-regulatory instrument in the world to tackle online disinformation. The process of discussion and implementation of the code was used by the EC to push internet platforms to do more and better ahead of the EP elections. It was faster than regulation would have been and brought results before the EP elections.

The Code of Practice has neither key performance indicators nor monitoring tools to assess compliance of signatories. It also does not establish enforcement and sanction mechanisms against non-compliance. For that reason, it does not fulfil the requirements for self-regulation that are in place at EU level for the media sector. Implementation of the code across platforms varied: for instance, while Facebook included issue-based ads in their transparency policy, Twitter and Google did not. Moreover, platforms have been implementing the commitments at different paces among Member States, sometimes influenced by PR strategies and leaving several countries behind.

**Recommendation**

Internet platforms and the advertising industry should use the one-year assessment to discuss a revamp of the text, for instance harmonising standards for political ads, and to satisfy requirements of self-regulation. The European Union should consider possible co-regulation or normal regulation to set procedural standards for content regulation such as appeal bodies, to increase transparency on algorithmic ranking choices, to harmonise political and issue-based ads rules and to level the capacity the platforms put in place in each country. That seems to be under discussion by the European Commission as it draws up the Digital Services Act, expected to be presented by the end of 2020.

### 2.5 MEDIA LITERACY

Media literacy aims at the demand-side of the disinformation dynamic — at citizens who consume information. The EC organised a European Media Literacy Week in March 2019, with more than 320 events throughout Europe, ran awareness-raising activities targeting multipliers and distributed material on attempts by Russian sources to interfere in electoral processes.

The new Audio-Visual Media Service Directive (AVMSD), adopted in November 2018, establishes that Member States shall promote and take measures for the development of media literacy skills and report on implementation by December 2022. It also requires media service providers and video-sharing platforms providers to promote the development of media literacy in all sections of society.

Investments from the EC in media literacy go in the right direction and are complemented with more funding and initiatives from platforms and civil society organisations, detailed further in this report. The new AVMSD says that media literacy should target citizens of all ages, which is welcome since there is growing evidence that media literacy should not focus only on children and teenagers, but also on older demographics, who are more
inclined to believe in and spread disinformation⁴.

Projects to teach media literacy to students, adults and elderly must be broadened. Nowadays, such projects are applied on a small scale, mostly at schools. They are not built systematically into school curricula. Also, there is lack of systematic monitoring of digital literacy skills among the population. And the implementation of the AVMSD depends on the political environment and resources of Member States.

Recommendation

The EC should support the inclusion of media literacy in school curricula and other educational institutions, including for the elderly across the EU. Likewise, it should support the inclusion of an assessment of students’ media literacy competences in the next round of the OECD PISA test.

2.6 INDEPENDENT NETWORK OF FACT-CHECKERS

The EC announced in April 2018 that it would support the creation of an independent European network of fact-checkers “to establish common working methods, exchange best practices, achieve the broadest possible coverage across the EU, and participate in joint fact-checking and related activities”⁵.

Horizon 2020, an EU research programme, funded some initiatives within that remit. One of them is the Social Observatory for Disinformation and Social Media Analysis (SOMA), launched in November 2018 with a grant of € 1 million and an additional € 2.5 million from the Connecting Europe Facility.

The project aims to provide support and tools to the European community of fact-checkers, media organisations and researchers. In July 2019, it had 16 independent members. SOMA went through a test period until end of June 2019 and currently offers to its partners the verification platform Truly Media, that allows crawling through social media content and assessing its trustworthiness.

The EC supports third parties from civil society and academia towards building a network of fact-checkers, instead of engaging itself in this endeavour. Positively, SOMA states that the Commission does not have power to intervene in the work of partner fact-checkers.

SOMA did not build a consistent network of fact-checkers ahead of the EP elections, as it was still in its test period. Also, there might be overlaps with other initiatives at this point. For instance, European members of the International Fact-Checking Network joined forces in an initiative ahead of the EP Elections called FactCheck EU, encompassing 19 European media outlets from 13 countries. Also, the organisation First Draft launched CrossCheck Europe, a collaborative platform to fact-check with more than 50 partners covering 19 countries.

Recommendation

Initiatives to build a network of fact-checkers, such as SOMA and others, should connect fact-checkers with other organisations from civil society devoted to analysing social media dynamics. Also, the network of fact-checkers should have an interface with official monitoring mechanisms, such as warnings from the Rapid Alert System and internet platforms. The EU should keep refraining from getting involved directly with fact-checking.


2.7 FUNDING FOR INNOVATION

The EC has funded different research and projects combatting disinformation in innovative ways. Since 2016, it has approved grants of € 27.9 million to 13 initiatives via the research programme Horizon 2020. Table 2 provides details on these programs.

This report does not offer a comprehensive analysis of these innovative projects, but instead a brief description of some of them:

- **Eunomia**: A platform to help determine the source of a piece of information, how it has been modified and its trustworthiness with a blockchain-based infrastructure.
- **WeVerify**: A verification platform for digital content, that has already launched a verification plugin to help fact-checking and debunking tasks on social platforms, especially videos and images.
- **Provenance**: A system for digital content verification that will register original works in a blockchain ledger to track how it spreads and to identify manipulations.
- **SocialTruth**: A system that enables easy access to various verification services, ensuring scalability and trust in a decentralised environment.

A share of Horizon 2020’s total budget, estimated at nearly € 80 billion over seven years (2014 to 2020), has been invested in initiatives related to disinformation. Even if the final output is not immediately applicable to European citizens, the knowledge developed might be integrated into future projects in the public and private sectors.

The commitment to innovative research has not been matched by a commitment to action. For example, the East StratCom Task Force worked its first three years without any budget.

**Recommendation**

The EC’s funding of innovative projects to counter disinformation is a positive start, but it is also important to fund EU bodies and civil society organisations’ projects aimed at understanding, detecting and exposing disinformation in real time.

### TABLE 2

**PROJECTS FUNDED BY THE RESEARCH PROGRAMME HORIZON 2020**

<table>
<thead>
<tr>
<th>Name</th>
<th>EU contribution (€ M)</th>
<th>Start</th>
<th>End</th>
</tr>
</thead>
<tbody>
<tr>
<td>Comprop</td>
<td>2</td>
<td>Jan.16</td>
<td>Dec.20</td>
</tr>
<tr>
<td>Botfind</td>
<td>0.15</td>
<td>Aug.17</td>
<td>Jan.19</td>
</tr>
<tr>
<td>Debunker</td>
<td>2</td>
<td>Sep.16</td>
<td>Aug.20</td>
</tr>
<tr>
<td>ELHO</td>
<td>2.5</td>
<td>Apr.19</td>
<td>Mar.24</td>
</tr>
<tr>
<td>GoodNews</td>
<td>0.15</td>
<td>Sep.18</td>
<td>Feb.20</td>
</tr>
<tr>
<td>Invid</td>
<td>3.1</td>
<td>Jan.16</td>
<td>Dec.18</td>
</tr>
<tr>
<td>Fandango</td>
<td>2.9</td>
<td>Jan.18</td>
<td>Dec.20</td>
</tr>
<tr>
<td>Co-inform</td>
<td>4.1</td>
<td>Apr.18</td>
<td>Mar.21</td>
</tr>
<tr>
<td>Eunomia</td>
<td>2.5</td>
<td>Dec.18</td>
<td>Nov.21</td>
</tr>
<tr>
<td>SocialTruth</td>
<td>2.5</td>
<td>Dec.18</td>
<td>Nov.21</td>
</tr>
<tr>
<td>Provenance</td>
<td>2.5</td>
<td>Dec.18</td>
<td>Nov.21</td>
</tr>
<tr>
<td>WeVerify</td>
<td>2.5</td>
<td>Dec.18</td>
<td>Dec.21</td>
</tr>
<tr>
<td>SOMA</td>
<td>1</td>
<td>Nov.18</td>
<td>Apr.21</td>
</tr>
<tr>
<td><strong>Total</strong></td>
<td><strong>27.9</strong></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Source: EC report “Towards European Media Sovereignty”
2.8 PARALLEL INITIATIVES

In the long-run, two other initiatives at the EU level may impact digital threats to democracy such as disinformation:

2.8.1 GENERAL DATA PROTECTION REGULATION (GDPR)

The new European data protection framework, in place since May 2018, establishes stricter rules for handling of personal data, which makes it harder for malicious actors to abuse personal data for micro-targeting purposes, including in electoral contexts. National data protection authorities are able to investigate and address infringements.

Additionally, in March 2019, the EP approved amendments to the statute of European political parties and established specific prohibitions for those parties in relation to personal data use in online campaigning.

2.8.2 EU COPYRIGHT REFORM

The new Directive on Copyright in the Digital Single Market, approved by the Council in April 2019, enhances the position of news publishers to negotiate copyright payments for the use of news articles by internet platforms. The EC claims that, in the long run, it will help to rebalance the relation between media and online platforms, strengthening news media outlets and journalists to produce high-quality journalism.

---

6 Regulation (EU, EURATOM) No 1141/2014 of 22 October 2014
3. CIVIL SOCIETY INITIATIVES ON SOCIAL MEDIA AROUND EP ELECTIONS

Civil society organisations (CSOs) played a critical role in identifying disinformation campaigns and extremist discourse ahead of the EP elections. Many efforts combined data and qualitative analysis.

Also, some CSOs spotted extremist pages that had not been previously identified by internet platforms, showcasing the need for cooperation and multi-stakeholder approaches to tackle disinformation. They were able to find patterns and trends, and in some cases measure the spread of disinformation or extremist content.

However, most cross-country projects from civil society focused on the same few Member States, such as France, Germany, Italy, Poland, Spain and the UK, leaving several countries off the radar.

Also, they are limited in their capacity of monitoring systematically. What was exposed may only be a small part of campaigns aimed at manipulating elections. There is no comprehensive approach to monitoring extremist online campaigns.

Lastly, much of the funding of these organisations is limited to monitor electoral periods, while manipulation of public discourse happens all year long. Those organisations should be able to retain their capacity to analyse threats over time.

Table 3 shows the Member States monitored by civil society cross-country projects.

Here are main trends that civil society organisations identified:

- Shift from pure disinformation to what is called narrative warfare. Instead of spreading falsehoods, many fake news sites (unclear affiliation, no editorial information) focus on propagandistic activity such as only reporting on crimes committed by Muslims.
- Increased disinformation by domestic non-state actors
- Some disinformation spreading networks are resilient despite of platforms’ interventions.
- Domestic extreme right, disinformation organisations are building international networks with similar organisations from other countries.
- No massive increase of disinformation ahead of the EP elections.

Table 4, on the next page, summarises the cross-country initiatives.

TABLE 3
Member States Monitored by Civil Society Cross-Country Projects

<table>
<thead>
<tr>
<th>Country</th>
<th>Number of projects</th>
<th>Country</th>
<th>Number of projects</th>
</tr>
</thead>
<tbody>
<tr>
<td>France</td>
<td>6</td>
<td>Sweden</td>
<td>2</td>
</tr>
<tr>
<td>Germany</td>
<td>5</td>
<td>Hungary</td>
<td>2</td>
</tr>
<tr>
<td>Italy</td>
<td>5</td>
<td>Slovakia</td>
<td>2</td>
</tr>
<tr>
<td>Poland</td>
<td>5</td>
<td>Austria</td>
<td>1</td>
</tr>
<tr>
<td>Spain</td>
<td>4</td>
<td>Denmark</td>
<td>1</td>
</tr>
<tr>
<td>UK</td>
<td>4</td>
<td>Ireland</td>
<td>1</td>
</tr>
<tr>
<td>Czech Republic</td>
<td>3</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

7 For more details on this, see DRI Briefing Paper 100: Online Threats to Democratic Debate: A Framework for a Discussion on Challenges and Responses. Available at https://democracy-reporting.org/dri_publications/bp100-online-threats-to-democratic-debate/
<table>
<thead>
<tr>
<th>CSO</th>
<th>Monitoring period</th>
<th>Tools used</th>
<th>Countries</th>
<th>Target</th>
<th>Results</th>
<th>Methodology</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alto Data Analytics</td>
<td>From mid-December 2018 to end of May 2019</td>
<td>Alto Analyzer</td>
<td>France, Germany, Italy, Poland and Spain</td>
<td>Internet platforms, public forums and blogs</td>
<td>Identified a small number of highly active social media profiles sympathetic to right- and left-leaning nationalist and “populist” parties.</td>
<td>Collected data points from varied digital sources. Time period and keywords researched varied by country. Details not disclosed.</td>
</tr>
<tr>
<td>Avaaz</td>
<td>From January to May 2019, with more intensity from March on.</td>
<td>Scrapping codes, CrowdTangle</td>
<td>Germany, France, Italy, UK, Poland and Spain</td>
<td>Facebook</td>
<td>Reported 550 pages and groups to FB suspected to violate terms of use and engage in inauthentic behaviour, of which 77 were taken down. Spotted page names changes, coordinated sharing of content and other malicious behaviours.</td>
<td>Compiled stories debunked by fact-checkers. Looked for FB pages and groups sharing those stories and its networks. Mapped 9,000 pages. Extracted the last three months of activity and investigated it. Details not disclosed.</td>
</tr>
<tr>
<td>Cardiff University</td>
<td>End-January up to May 2019.</td>
<td>Built-in tool and Babel Street</td>
<td>Multiple, including Twitter, FB, Instagram and news sources.</td>
<td>27 EU countries</td>
<td>Found more propaganda than pure disinformation. Platform interventions affect prevalence and distribution, but networks prove to be resilient. Domestic authors and amplifiers have learnt the techniques.</td>
<td>Used data and social science. Analysed audiences receptive to disinformation and interactions between different users and did content analysis. Looked into who was buying followers, followers fishing and narrative switching.</td>
</tr>
<tr>
<td>GLOBSEC</td>
<td>10 April to 10 May 2019.</td>
<td>Zoomsphere</td>
<td>Czech Republic, Hungary, Poland and Slovakia</td>
<td>Facebook</td>
<td>In Hungary, disinformation was promoted by pro-government media, whereas in the Czech Republic was spread by fringe channels. In the three countries, “immigrants as a threat” was a common narrative.</td>
<td>Collected data from 15 relevant FB pages per country that publish disinformation or pro-Kremlin narratives, filtered by keywords “election” and “euro&quot;, identified sentiments toward parties and most prevalent narratives.</td>
</tr>
<tr>
<td>Institute for Strategic Dialogue</td>
<td>From mid-February to May 2019.</td>
<td>Crimson Hexagon for Twitter, CrowdTangle for FB, Graphika for network mapping.</td>
<td>Germany, France, Italy, Spain, Poland, and the UK.</td>
<td>Twitter, Facebook, Telegram, WhatsApp and others.</td>
<td>Found a shift from information warfare towards narrative warfare, and non-state actors adopting techniques. Migration, climate change denial and misogyny were prominent topics. Increasing transnational cooperation among nationalist groups/parties.</td>
<td>Used digital tools and digital ethnographic research, also looking into Telegram, WhatsApp and fringe platforms. Coupled research on social media with on the ground know-how from investigative journalists and one specialist in digital forensic.</td>
</tr>
<tr>
<td>CSO</td>
<td>Monitoring period</td>
<td>Tools used</td>
<td>Countries</td>
<td>Target</td>
<td>Results</td>
<td>Methodology</td>
</tr>
<tr>
<td>------------------------------------------</td>
<td>---------------------------</td>
<td>------------------------------------------</td>
<td>------------------------------------------------</td>
<td>---------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Oxford Internet Institute</td>
<td>April to May 2019</td>
<td>NewsWhip</td>
<td>Seven language spheres: English, French, German, Italian, Polish, Spanish, and Swedish.</td>
<td>Twitter and Facebook</td>
<td>Twitter users shared far more links to mainstream news than to junk news, except in the Polish sphere. On Facebook, individual junk news stories can outperform mainstream media stories. Anti-immigration and Islamophobic sentiment were predominant topics.</td>
<td>Collected tweets related that used EP elections-related hashtags. From this sample, extracted those containing a URL link. Sources shared five times or more across collection period were manually classified by a team of nine multi-lingual coders.</td>
</tr>
<tr>
<td>Political Capital and Friedrich Naumann Foundation</td>
<td>15 March to 15 April 2019</td>
<td>Versus</td>
<td>Czech Republic, Hungary, Poland and Slovakia</td>
<td>Pro-Kremlin news outlets</td>
<td>In Hungary, migration and Euroscepticism were central topics. In Slovakia, monitored media cultivated negative perception of the EU. In Czech Republic, there was appraisal for far-right leaders. In Poland, information operations portrayed anti-EU politicians as solution for the country.</td>
<td>Monitored English-language versions of RT and Sputnik International and eight local pro-Kremlin media outlets in each country, with keywords and looked into narratives. Subsequently, carried out a narrative analysis of the monitored content and narratives.</td>
</tr>
<tr>
<td>Prague Security Studies Institute</td>
<td>15 April to 25 May 2019</td>
<td>Versus</td>
<td>Czech Republic</td>
<td>Disinformation-prone news websites</td>
<td>Disinformation did not increase significantly ahead of the EP elections. Migration and supposedly economic damage of EU were central topics. Right-wing party Freedom and Direct Democracy benefited from disinformation-prone websites.</td>
<td>Monitored disinformation-prone news websites. First, how 31 disinformation platforms were framing EU topics, and then how the 8 most influential were reporting EP elections. Manual coders analysed sentiment towards parties.</td>
</tr>
<tr>
<td>Weizenbaum Institut</td>
<td>January to end of June 2019</td>
<td>Crimson Hexagon, Facebook scraping technologies, Netvizz, MediaCloud.</td>
<td>Germany, Austria, Denmark, Sweden, Poland, France, Italy</td>
<td>Internet platforms and news websites</td>
<td>Alt-news sites are building networks integrated on the national scale, with hubs that connect them to other countries’ networks. Suggests that to locate disinformation sources, one should also look to the West (US) and domestic actors. Right-wing actors shifted away from EU-scepticism.</td>
<td>Monitored parties and organisations on the right and investigated how topics intersect in each country. Monitored right-wing news outlets and their social media activity, checking if they linked to each other and formed networks. Compared narratives within ecosystems and with mainstream media.</td>
</tr>
<tr>
<td>Who targets me</td>
<td>Began to analyse data three weeks before EP elections but gathered data before that.</td>
<td>Facebook Ad Library API</td>
<td>Ireland, UK and France</td>
<td>Facebook</td>
<td>Sometimes media, non-political groups or commercial ads can be caught up in the political classification. Facebook is taking a confusing approach when it comes to issue ads. Research is ongoing and will be shared by the end of the Summer.</td>
<td>Gathered the data using API.</td>
</tr>
</tbody>
</table>
4. INITIATIVES BY SOCIAL MEDIA COMPANIES

Facebook, Twitter and Google took the heat ahead of the EP elections due to widespread apprehension that large disinformation campaigns on their platforms could sway voters. They were pressed by EU institutions, civil society and media to take more action to fight disinformation. In response, the tech companies developed initiatives that made it more difficult to spread disinformation and raised the cost for malicious actors. However, the issue is far from being solved and manipulation techniques are evolving. They have built on transparency tools developed to the U.S. 2018 midterm elections, improved and expanded to the EP elections.

The three companies established transparency policies for political ads related to the EP elections. They adopted stricter rules, submitted advertisers to document checks, labelled political ads as such and compiled them on libraries accessible publicly and via API.

However, only Google’s API seemed to work well, while Twitter’s had minor problems and Facebook’s had serious bugs. Also, some political ads were not labelled as such, while others were deleted from libraries. Twitter and Google did not develop policies to raise transparency and label issue ads, contrary to a commitment of the Code of Practice on Disinformation.

Table 5 provides the definitions adopted by the platforms to frame ads as political or issue-based:

The companies deployed initiatives to increase integrity, using automated systems and human reviewers. This resulted in companies blocking or deleting fake accounts, users that violate terms of services and ads that do not fulfil policies and taking down networks engaged in coordinated inauthentic behaviour. It is hard to independently assess the result of these initiatives, as the companies do not publish detailed information and there is little independent data on disinformation actors that could be used as a benchmark.

Facebook partnered with fact-checkers to review and rate the accuracy of posts deemed or reported as false is a good example of how a multi-stakeholder approach benefits initiative to tackle disinformation. However, it covered only 14 European languages, leaving 10 out. Platforms claimed to have changed algorithms to prioritise authoritative content over disinformation, but not evenly across the 28 EU countries. The following section gives an abstract of each platforms’ initiatives (Table 6).

| TABLE 5 | Definition of Political/issue Ads |
|-----------------|-----------------|-----------------|
| **Political Ads** | **Facebook** | **Google** | **Twitter** |
| Ads that make reference to political figures, political parties and the EP elections. | Ads that mention a political party, a candidate or a current officeholder. | Ads purchased by a European or national political party or by a candidate registered with their corresponding national electoral authority, or ads that advocate for or against a clearly identified candidate or party for European elections. |
| **Issue Ads** | Ads that make reference to six issues of importance within the EU: immigration, political values, civil and social rights, security and foreign policy, economy and environmental politics. | - | - |

18
<table>
<thead>
<tr>
<th>TABLE 6</th>
<th>Initiatives by Social Media Companies Ahead of the 2019 EP Elections</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Facebook</strong></td>
<td><strong>Google</strong></td>
</tr>
<tr>
<td><strong>Political Ads Policy and hindering Monetization of Disinformation Actors</strong></td>
<td>Confirmed identity of advertisers and increase transparency on spending and statistics of political and issue ads, enforced from mid-April 2019.</td>
</tr>
<tr>
<td>Ad library API had serious technical issues.</td>
<td></td>
</tr>
<tr>
<td><strong>Integrity of Services</strong></td>
<td>Automated system blocks most attempts to create fake accounts. Company works to detect and take down networks of coordinated inauthentic behaviour, but it’s hard to measure the rate of success. Civil society organisations reported numerous pages violating terms of service that had not been identified by the tech company.</td>
</tr>
<tr>
<td><strong>Fact-checking</strong></td>
<td>By May 2019, it had partnership with 21 fact-checking organisations to review and rate the accuracy of posts deemed or reported as false. But it covered only 14 European languages, leaving 10 of them behind.</td>
</tr>
<tr>
<td><strong>Empowering the Research Community</strong></td>
<td>Partnered with selected researchers to allow privacy-compliant access to data, covering academic institutions from six EU Member States, but system was not yet function by mid-August 2019. At the same time, company is making harder to access public pages and posts via API.</td>
</tr>
</tbody>
</table>
4.1 FACEBOOK

4.1.1 POLITICAL AND ISSUE ADS

Facebook was the only platform to include issue ads in their transparency policy, as required by the Code of Practice on Disinformation. The company also explained the methodology used to define which political issues would be considered in the policy.

Sometimes media, non-political groups or commercial ads were caught up in the political classification. Also, brackets on the amount spent were not precise and reduced the accuracy of independent reports, as pointed out by an analysis of Who Targets Me.

Several reports have described technical constraints, bugs and limitations of the Facebook Ad Library API that hindered the possibility to develop meaningful analysis based on the data available. An assessment by the French government highlighted some of the API failures: lack of information of ad funders, incomplete documentation, bugs, a pagination system that requires numerous requests and makes it hard to download the entirety of the Ad Library for every country, and ads removed from the library, in contradiction with Facebook’s pledge to keep active and inactive ads for seven years.

Mozilla also published a report describing that their methods to scan and discover political and issue ads on Facebook had to be adapted on a daily and sometimes hourly basis to deal with “design limitations, data issues, and numerous software bugs in the Facebook Ad Library API”. Mozilla said it tried to help the company to debug their system, but most issues was not solved. According to the report, the API “delivered incomplete data on most days from its release through May 16, when Facebook fixed a critical bug”. Also, “the API was broken again from May 18 through May 26, the last day of the elections”.

Additionally, a news report by Politico found several paid posts from the German far-right party AfD that were ran on Facebook without being labelled as political ads.

Lastly, Facebook began to enforce its transparency policy only from mid-April onwards, barely one month ahead of the EP elections, while Twitter and Google began to enforce their policies in March.

Recommendation

Facebook should debug its API and make it easier and more consistent to query data from the Ad Library. It should not have been a major challenge for a company used to deal with huge amounts of data and technical challenges to put in place a functional API to access data of political and issue ads. Facebook should also maintain and improve its transparency and verification policy for political and issue ads in the future, adding more granularity on paid values.

4.1.2 INTEGRITY OF SERVICES

Beyond blocking fake accounts, Facebook tries to detect and stop networks engaged in coordinated inauthentic behaviour.

For example, in March 2019, the company announced it had removed 137 Facebook and Instagram accounts, pages and groups that were part of a domestic-focused network in the UK. Individuals behind fake accounts represented themselves as far-right and anti-far-right activists, engaged in hate speech and spread divisive comments on both sides of the political debate.

In May 2019, Facebook removed two separate networks comprised of 118 pages, groups and accounts originated in

---

Russia. The first network posted about local and political news including topics like the military conflict in Eastern Ukraine and political news in Europe, while the second focused on Austria, Baltic countries, Germany, Spain, Ukraine and the UK, posting about topics like local politics and migration.

It is positive that the company worked to detect and remove networks engaged in coordinated inauthentic behaviour and made those decisions public. Some of those actions benefited from reporting by law enforcement agencies, and Facebook claimed it also shared information with law enforcement agencies, policymakers and industry partners, showing a degree of coordination and a multi-stakeholder approach.

It is hard to assess the success of Facebook actions against coordinated inauthentic behaviour and other disinformation strategies, as one cannot know about actors and networks that were not identified. Research by Avaaz found 550 pages and groups suspected to be involved in spreading disinformation, 77 of which were taken down only after the organisation reported them to Facebook.

**Recommendation**

Facebook could make the datasets of networks engaged in information operations taken down by the company publicly available to help the research community understand the dynamics of these networks. Consequently, researchers could identify strategies and propose ideas and policies to improve responses. Also, Facebook should improve its capacity to detect violations of terms of use and information operations. Civil society organisations with far less resources were able to spot disinformation activity not identified by the company.

### 4.1.3 COOPERATION WITH STAKEHOLDERS

Facebook launched two ‘escalation channels’ to receive information from selected partners and users. The *Election Security Escalation Channel* allowed trusted security and intelligence partners to report potential cybersecurity and information operations threats. By the end of May 2019, it had partners from ten EU countries. The *Government, Political and Advocacy Concierge* allowed administrators of government and political pages to report tech issues, bugs, imposter accounts, violating and suspicious content, among other issues.¹¹

**4.1.4 FACT-CHECKING**

Facebook has a partnership with fact-checking organisations to review and rate the accuracy of posts suspected to be false. By May 2019, it encompassed 21 organisations in the EU covering 14 European languages: Croatian, Danish, Dutch, English, French, German, Greek, Italian, Lithuanian, Norwegian, Polish, Portuguese, Spanish and Swedish. The company claims to have reduced the distribution of content marked as false by partner organisations by an average of 80%. Once content is marked as false, the company alerts users who have shared this false content.

Partnerships with fact-checking organisations certified by the International Fact-Checking Network (IFCN) are an effective strategy to help Facebook improve the accuracy of content shared on its platform. External, third party fact checking organisations provide a level of legitimacy to classifying posts as disinformation or misinformation, rather than Facebook making this classification itself. Also, as Facebook pays fact-checkers for their services, it contributes to strengthen the fact-check environment.

The company began to send fact-checkers quarterly reports with statistics about their work, but some of them complain they would like to receive more feedback. Also, there is no public library with posts deemed false and ranked down by the platform.

---

¹¹ Facebook May report on implementation of the Code of Practice on Disinformation
Ten official European languages were not covered by Facebook partnership with fact-checking organisations.

**Recommendation**

The partnership should be expanded to allow more fact-checkers to analyse content on Facebook and to reach all 28 EU countries. Facebook should provide better and more frequent feedback. The initiative should be extended to Instagram to check disinformation spread via photos and memes. The company already began to test it on Instagram in May 2019. A public library with posts deemed false and ranked down would increase transparency.

### 4.1.5 MEDIA CAMPAIGN

From early April until late May 2019, Facebook ran a campaign in selected EU countries — Belgium, Denmark, France, Germany, Ireland, Italy, the Netherlands, Poland, Spain, Sweden and the UK — about the company’s integrity efforts ahead of the EP elections. Ads appeared on Facebook and Instagram timelines, print newspapers and digital billboards.

Ads ran on its own platforms were concentrated in only six Member States, with most of them on Germany, France and the UK, according to an analysis by Who Targets Me\(^{12}\), leaving out the other 22 Member States.

**Recommendation**

Media efforts from Facebook regarding disinformation should address all 28 EU countries.

### 4.1.6 EMPOWERING THE RESEARCH COMMUNITY

In April 2019, Facebook announced the first researchers that would be allowed to access to privacy-protected Facebook data to study the platform’s impact on democracy, via a partnership with Social Science One and the Social Science Research Council. It selected academic institutions from six EU Member: Denmark, France, Germany, Italy, the Netherlands and Poland.

The disclosure of the names of the researchers selected in the first round of applications signalled that the cooperation scheme was going forward. Facebook does not have the right to review or approve their research findings prior to publication.

There have been delays in implementing the partnership. The scheme was announced by Facebook in April 2018 and researchers were supposed to have access to data from June 2019 on, but by mid-August 2019 it was yet not effective. Initially, the company considered to deliver aggregated data to researchers, but later realised that the data could be deanonymized, breaching user privacy. The company then decided that it would use a technique known as *differential privacy* to increase protection of user data, but its implementation is facing technical issues. Since June 2019, researchers can use a test platform with fake data to run queries, but the test platform has bugs.

At the same time Facebook is allowing a few selected researchers to tap into its data, the company is restricting access to public posts and pages data via its API. Tools to extract public data are facing a growing number of limitations by Facebook’s API and privacy policies. Netvizz, a tool widely used by researchers, is expected to be blocked in September 2019.

**Recommendation**

Facebook should invest more resources to solve technical problems that are delaying the implementation of the partnership. Also, the company should refrain from blocking access via its API to public pages and posts, which is used by numerous researchers to understand political, social and disinformation patterns within the platform without the need of privileged access to private pages and posts that the

---

partnership with Social Science One offers. Public data and posts do not raise critical privacy issues.

### 4.2 Google

Google’s approach towards advertising differs from Facebook and Twitter. Beyond earning money from placing ads spaces in its own products, such as Search and YouTube, it also allows websites owners around the world to earn money placing ads via the service AdSense in their website, charging a percentage of the revenue.

#### 4.2.1 General Ads

Google AdSense policy bans websites that misrepresent, misstate or conceal information about themselves, such as a website that impersonates a political party or a government agency. It also blocks websites based on mirroring, scraping or rewriting of content from other sources. Those policies apply globally and may impact also disinformation actors.

Also, the company prohibits ads in its products, such as Search and YouTube, that intend to deceive users with false statements about identity, false claims and misleading information. Google rates ads and websites with algorithms and human evaluators.

In their monthly reports ahead of the EP elections, Google released data on the number of Google Ads or AdSense accounts blocked due to violation of their policies, broken down by each EU Member State, considering the billing country.

Google did not specify which percentage of blocked ads or accounts were related to disinformation.

#### 4.2.1 Political Ads

Google began to enforce its policy for political ads in March 2019, without accounting for issue ads. In May 2019, the company stressed “the difficult nature of identifying issue ads and the technical requirements for implementing any such solution”.  

Google policies may be applied to hinder monetisation of malicious actors that create websites with disinformation to attract audience and raise revenue from online ads. The Ad Library includes also the ads that violated the policy, flagged as such, and the API worked well. Research by Mozilla experienced no technical issue with the dataset or the download process.

The company failed to include issue ad in its policy, contrary to the commitment in the Code of Practice on Disinformation.

**Recommendation**

Google should maintain and improve its transparency and verification policy for political ads in the future and add issue ads to it.

#### 4.2.2 Fact-Checking

Google launched a search tool that allows users to find fact checked articles by topic. Additionally, fact-checkers can now label articles that they have checked within a mark-up platform. These labels are included in search results for users, so users are made aware of whether an article was checked and what the fact checker concluded.

Google also improved its Search algorithm to put more emphasis on fact-checked article results in searches related to breaking news events.

#### 4.2.3 YouTube

Breaking news events are an opportunity to malicious actors to direct traffic to their content. To reduce tides of misinformation on YouTube during those events, Google implemented two features to prioritise authoritative and verified news channels, the Top News shelf, that appears in YouTube search, and the Breaking News shelf, on the YouTube homepage. Another serious problem of YouTube, the recommendation of extremist content was not addressed in the EU.

Those features were available in only 18 EU countries ahead of the EP election: Germany,

---

13 Google May 2019 report to the European Commission.
France, UK, Italy, Spain, Poland, Netherlands, Sweden, Ireland, Romania, Belgium, Czech Republic, Lithuania, Greece, Portugal, Hungary, Austria and Slovakia.

In January 2019, Google announced it would reduce recommendations of borderline content and content on YouTube that could misinform users in harmful ways. However, the algorithm change worked initially only in the U.S. and the company only says it is working to bring it to more countries by the end of 2019.

Also, YouTube polices do not address specifically disinformation or inauthentic coordinated behaviour, only impersonation.

Recommendation

YouTube should explicitly include downgrading disinformation in its policy and prohibit inauthentic coordinated behaviour in its policies' rules, as Google News’ policy does. Also, algorithm improvements, such as the Top News and Breaking News shelves and excluding extremist content from recommendations should be implemented across Europe.

4.3 TWITTER

4.3.1 POLITICAL ADS

Twitter began to enforce its ad policy related the EP elections in March 2019. By the end of May 2019, there were 27 EU certified political campaign accounts, 21 of which were running ads.

There was no specific policy for issue ads around the EP elections, although Twitter began to enforce a policy for issue ads in the U.S. in October 2018.

An assessment by the French government\(^4\) found weaknesses in the Ads Transparency Center – “In-Stream Video” political campaigning ads were not included, the API returned frequent errors and data integrity was not guaranteed since both the advertiser and Twitter may decide to halt the exposure of ads in the library. Also, information provided by the Ads Transparency Center could not be downloaded as a file.

Recommendation

Twitter should improve its transparency and verification policy for political ads in the future and expand it to include issue ads. Also, the company should solve technical issues and improve accessibility via its API.

4.3.2 INTEGRITY

According to its own reports, the company challenges ten spam-like accounts per second. Around 75% of these challenged accounts do not pass the company’s tests and are removed.

In April 2019, the company announced a new election integrity policy that forbid posting or sharing content that may suppress voter turnout or mislead people about when, where or how to vote, and created a new channel for users to report such content. From 1 to 20 May 2019, Twitter received 28,456 reports via this new dedicated function.

The company’s automated system has positive effects to block malicious accounts that may be linked to disinformation operations. Also, its integrity team is capable of identifying and taking down state-sponsored information operations to undermine political discourse.

Automated systems might not be able to spot and act against impersonators and more refined disinformation campaigns. Civil society organisations spotted fake accounts, disinformation actors and campaigns that had not been identified previously by the tech company.

Recommendation

Twitter should strengthen its automated system and integrity team to be able to spot more information operations and to respond more quickly to reports by users on issues such as impersonation.

4.3.2 FACT-CHECKING

Twitter does not have partnerships with fact-checking organisations to review and rate posts deemed or reported as false.

Recommendation

Twitter should consider establishing partnerships with fact-checking organisations in a similar way to Facebook.

4.3.3 EMPOWERING THE RESEARCH COMMUNITY

Twitter has a more open stance to allowing access to public tweets via its API in comparison to Facebook, allowing researchers significant access to analyse posts.

Also, the platform has released data packages with accounts and content associated with potential state-sponsored disinformation operations to undermine political discourse found by its integrity team since 2016. By July 2019, 13 datasets had been released, covering operations from Russia, Iran, Venezuela, Bangladesh and Catalonia.

Twitter’s approach to its API provides significant access to the research community unlike other platforms. The release of data packages with accounts and content associated with potential state-sponsored information operations has also proved valuable.

There have been calls for the disclosure of more details in the data packages related to disinformation operations.
The fight against disinformation at the EU level is backed by numerous legal principles and rights. The table summarises some of them:

### TABLE 7
Legal Framework

<table>
<thead>
<tr>
<th>Principles and rights that demand the EU and Member States to fight disinformation</th>
<th>Content</th>
<th>Normative text or body</th>
</tr>
</thead>
<tbody>
<tr>
<td>A genuinely democratic transparent election</td>
<td>Numerous bodies (UN, Council of Europe, OSCE)</td>
<td></td>
</tr>
<tr>
<td>Freedom of expression encompasses the right to receive and impart information and ideas “without interference by public authorities”</td>
<td>As above</td>
<td></td>
</tr>
<tr>
<td>Right to political participation is concerned not only with the expression of opinions, but also with their formation</td>
<td>As above</td>
<td></td>
</tr>
<tr>
<td>Right to vote in elections implies that voters should be able to form their opinions free from inducement or manipulative interference</td>
<td>UN’s Human Rights Committee, interpreting Article 25 ICCPR</td>
<td></td>
</tr>
<tr>
<td>Use of personal data</td>
<td>EU law forbids abuse of personal data in elections, such as for malicious micro-targeting in political campaigns</td>
<td>General Data Protection Regulation</td>
</tr>
<tr>
<td></td>
<td>European political parties cannot take advantage of infringements of rules on protection of personal data to try to influence the outcome of EP elections</td>
<td>EP Regulation N. 1141/2014</td>
</tr>
<tr>
<td>Political ads</td>
<td>Regulation of political ads are defined and imposed by Member States. At the EU level, there is just a recommendation for transparency, but no precise requirements. EC is discussing a new Digital Services Act that might contain political ads rules</td>
<td>Under discussion</td>
</tr>
<tr>
<td>Video-sharing platforms</td>
<td>Companies are required to protect people from incitement to violence or hatred. Also, Member States and video-sharing platforms providers are required to promote development of media literacy</td>
<td>Audiovisual Media Services Directive</td>
</tr>
<tr>
<td>Cyber threats</td>
<td>EU can impose sanctions or other restrictive measures, such as asset freeze and travel bans, to counter cyber-attacks that constitute an external threat to the Union or its Member States</td>
<td>Council Regulation (EU) 2019/796</td>
</tr>
<tr>
<td>Self-regulation</td>
<td>Signatories of the EU Code of Practice on Disinformation committed to hinder monetisation of financially driven disinformation, to increase transparency related to political ads and to safeguard integrity of their systems</td>
<td>EU Code of Practice on Disinformation</td>
</tr>
</tbody>
</table>
6. RECOMMENDATIONS

The following list brings together the recommendations throughout the report:

6.1 EUROPEAN COMMISSION

Build Stronger Analytical Capacity and Coordination Among EU Bodies

The EEAS StratCom team should be empowered to carry out deeper analyses to monitor disinformation campaigns. This capacity should be used also to inform the East StratCom Task Force, the Western Balkans Task Force and the Task Force South, to modulate their debunking and responses in their respective geographical areas. The EEAS StratCom team, in coordination with the three task forces, should continue to feed the Rapid Alert System with their monitoring and findings.

The EU could have a senior officer or permanent structure to coordinate efforts to tackle disinformation.

Foster Coordination and Preparedness Among Member States

The fight against disinformation needs coordination among Member States. The Rapid Alert System should be strengthened.

The EU institutions should support Member States to develop and improve their national monitoring systems of hybrid threats and disinformation, which in turn would strengthen the inputs received by the Rapid Alert System.

Support Civil Society Organisations

Dealing with domestic disinformation or foreign disinformation spread by individuals or organisations based in the EU is difficult for the EU.

The EU should leave this task to civil society organisations, which face less institutional constraints to investigate disinformation and have already demonstrated the capacity to do so. These organisations, however, face financial constraints and their analyses usually are restricted to a few countries. The EU should support initiatives and make sure that monitoring continues between elections and covers all EU member states.

Address Co- or Normal Regulation

The EU should consider co- or normal regulation for some issues related to disinformation, such as political and issue ads, procedural standards for content regulation (e.g. appeal bodies), transparency on algorithm choices and ranking systems and the capacity the platforms put in place in each Member State.

An opportunity in this regard is the new Digital Services Act, currently under discussion by the EC and expected to be revealed by the end of 2020.

Improve Media Literacy Among Citizens

The EC should support the inclusion of media literacy in school curricula and support similar projects for the elderly across Europe. Likewise, it should support the inclusion of an assessment of students’ media literacy competences in the next round of the OECD PISA test.

6.2 INTERNET PLATFORMS

Political and Issue Ads

Companies should improve their APIs to allow researchers and journalists to smoothly query data from their ad libraries. Twitter and Google should also include issue ads in their transparency policies.

Improve Integrity

Although the companies have made efforts and built dedicated teams to increase integrity in their systems, this capacity should be greatly improved by combining AI and qualitative analysis. Civil society organisations with much less resources than the companies were able to spot malicious activity not identified by social media companies around the EP elections.

YouTube should include rules to explicitly downgrade disinformation or forbid inauthentic coordinated behaviour in its policies, as Google News policy does. Also, algorithms improvements, such as the Top News and Breaking News shelves, should be implemented across Europe.

More Coordination and Cooperation

Tech companies should deepen their coordination and cooperation efforts with governmental agencies, public bodies and civil society organisations. The experience has shown that multi-stakeholder approach is needed to tackle disinformation.

Revamping the Code of Practice

Internet platforms and the advertising industry should use the one-year assessment to discuss a revamp of the text and to satisfy requirements and current practices of self-regulation. They could use that opportunity also to pursue coordination on political and issue ads transparency policies, while the issue is not regulated at the EU level.

Fact-checking

Facebook should expand its partnerships with fact-checkers to analyse more content and reach all 28 EU countries. The initiative should also be permanently extended to Instagram to check disinformation spread via photos and memes. Twitter would benefit from a similar approach.

Empowering the Research Community

Facebook should invest more resources to solve technical
problems that are delaying the implementation of the partnership with researchers. Also, the company should unblock access via its API to public pages and posts.

6.3 CIVIL SOCIETY

More Coordination and Cooperation

Civil society organisations should press tech companies to increase coordination and transform findings into action. Also, it would be beneficial if CSOs manage to coordinate on which countries and which aspects of disinformation to monitor.

Adopting Common Reporting Standards

CSOs should discuss and adopt common reporting standards on methodologies and results.

Integrating Fact-checkers

Fact-checkers should partner with other organisations from civil society devoted to analysing social media dynamics. Insights brought by social media analysis would help fact-checkers act faster and before disinformation gets widespread traction. Also, European networks of fact-checkers should have an interface with official monitoring mechanisms and internet platforms.
ANNEX: TIMELINE OF ACTIVITIES AND INITIATIVES

- High Level Expert Group report is published
- EC issues Communication "Securing free and fair European elections"
- Code of Practice comes into force
- Rapid Alert System is launched
- Facebook begins to enforce political ads policy
- EU Action Plan
- First meeting of the European cooperation network for EP elections
- Twitter and Google begin to enforce political ads policy
- European Media Literacy Week
- European Parliament elections
- One-year assessment of Code of Practice