

SOCIAL MEDIA MONITORING DURING ELECTIONS

CASES AND BEST PRACTICE TO INFORM ELECTORAL OBSERVATION MISSIONS

OPEN SOCIETYEUROPEAN POLICY
INSTITUTE

DEMOCRACY REPORTING INTERNATIONAL

AUTHORS

Rafael Schmuziger Goldzweig Bruno Lupion Michael Meyer-Resende

FOREWORD BY

Iskra Kirova and Susan Morgan

EDITOR

Ros Taylor

OPEN SOCIETY FOUNDATIONS

© 2019 Open Society Foundations







This publication is available as a PDF on the Open Society Foundations website under a Creative Commons license that allows copying and distributing the publication, only in its entirety, as long as it is attributed to the Open Society Foundations and used for noncommercial educational or public policy purposes. Photographs may not be used separately from the publication.

Cover photo: © Geert Vanden Wijngaert/Bloomberg/Getty

opensocietyfoundations.org

CONTENTS

3	FOREWORD
5	EXECUTIVE SUMMARY
7	INTRODUCTION
9	CONTEXT
9	Threats to electoral integrity in social media
9	The framework of international election observation
10	The Declaration of Principles of International Election Observation
12	WHAT ARE INTERNATIONAL OBSERVER MISSIONS DOING ON SOCIAL MEDIA DISCOURSE?
14	WHAT ARE EUROPEAN GOVERNMENTS DOING?
17	WHAT ARE CIVIL SOCIETY ORGANIZATIONS DOING?
17	European civil society
19	A glimpse beyond Europe
21	Non-government initiatives: Europe & beyond
23	Topics/objects of analysis
24	Platforms
26	Monitoring tools

1

27	GUIDELINES FOR EOMS
27	Monitoring of social media vs traditional media
29	Cooperation between actors and information exchange partnerships
29	Dealing with data
29	Working in different contexts
31	SWOT analysis for EOMs in social media monitoring
32	RECOMMENDATIONS
35	ANNEX 1: SURVEY OF INTERNATIONAL ELECTION OBSERVATION ORGANIZATIONS
36	ANNEX 2: BRIEF DESCRIPTION OF THE INITIATIVES ANALYSED (based on interviews)
36	a. Non-governmental initiatives
40	b. Governmental/inter-governmental initiatives

FOREWORD

Concern over online interference in elections is now widespread – from the fallout of the Cambridge Analytica scandal to the pernicious effects messaging apps have had in elections in Kenya or Brazil. Yet regulatory and monitoring efforts have lagged behind in addressing the challenges of how public opinion can be manipulated online, and its impact on elections.

The phenomenon of online electoral interference is global. It affects established democracies, countries in transition, and places where freedom of expression and access to information are tightly controlled.

At the Open Society Foundations we have supported research looking at a wide variety of electoral contexts – ranging from the last German federal elections to the Brazilian presidential election, the American midterms and the European Parliament elections. As this experience revealed domestic and international, state and non-state actors manipulate information online in order to shape voters' choices or simply confuse and disorient citizens, paralyze democratic debate and undermine confidence in electoral processes. These players often act in ways that are indistinguishable, with some direct and indirect cooperation taking place.

The result is detrimental to the quality of our public debate and our ability to deliberate issues and seek common solutions as societies.

Much attention has focused on foreign threats, following the revelations of Russian interference in the US 2016 presidential elections, or on the hyperactivity of the far right online which pushes anti-establishment views into the center of debates. Yet digital campaigning by mainstream political

parties can easily become manipulative too – whether it is the use of bots and paid trolls to engineer false debates and narratives, the misuse of personal data or the targeting of political advertising at voters. Some of this activity might be illegal, but much of it is unregulated – to the detriment of our electoral rights.

As the authors of this report point out, freedom from manipulative interference of any kind is a core element of the right to vote and participate in political life, and enshrined in the International Covenant on Civil and Political Rights.

Until recently independent election observation missions and their assessments represented the most authoritative voice on the conduct of elections. Not any more. Traditional election observers have found themselves entirely unprepared to address these new challenges, particularly since there has been little rule setting in this new field.

The regulatory gap between online and offline political communication and elections is staggering. Even as monitors track broadcast media and advertising, elections are manipulated online.

Initial responses by recent international electoral observation missions in Kenya, Georgia and Nigeria – as described in this report – have aimed to highlight false information or hate speech disseminated during election periods. This approach follows a similar focus by regulators and platforms on uncovering and removing false or harmful content online. Germany's NetzDG and the UK's white paper on Online Harms are examples, as are content oversight boards such as the one established by Facebook. These types of measures can harm free expression and offer only partial solutions.

Content moderation has limited impact, as it is easy to circumvent red-flag language caught by algorithms and much of it still relies on users' own reporting of problematic material. Most importantly, it raises free speech concerns and serious questions about the legitimacy of online platforms – or governments for that matter – to act as arbiters for online speech. Deep knowledge of specific contexts – to address challenges like the misuse of Facebook to spread radicalization in Myanmar, for instance – is also critical, or important cultural tropes will be missed. Places where there is a history of election-related and other violence are particularly sensitive in this respect.

From the perspective of election observers, trying to cope with the volume of information and the speed at which stories or memes can go viral has made the task of monitoring content on social media around elections seem impossible.

In this new landscape, balanced and comprehensive oversight of elections and the online sphere will require innovation. In addition to focusing on the content, we need to start thinking about the online architecture that enables these distortions of the democratic debate and the influence of malign actors. Much of this architecture stems from the business model of web platforms, which relies on

selling users' personal data for targeted advertising in order to generate revenue. The current debates on data protection and microtargeting, and the rules put in place by Facebook and Google to ban foreignfunded advertising at election times, are a start.

But fundamental questions of what should be legal and illegal in digital political communication have yet to be answered in order to extend the rule of electoral law from the offline to the online. Answering these questions would help determine the right scope for online election observation, too.

This scoping report explains why social media is one of the elements of a democratic, rule-of-law based state that observer groups should monitor. It aggregates experience from diverse civil society and non-governmental initiatives that are innovating in this field, and sets out questions to guide the development of new mandates for election observers.

The internet and new digital tools are profoundly reshaping political communication and campaigning. But an independent and authoritative assessment of the impact of these effects is wanting. Election observation organizations need to adapt their mandate and methodology in order to remain relevant and protect the integrity of democratic processes.

Iskra Kirova and Susan Morgan

Open Society Foundations

EXECUTIVE SUMMARY

The international election observation community has lagged in its response to new threats to electoral integrity in social media. Challenges from disinformation campaigns, incitement to violence and manipulative public relations campaigns online hardly figure when international election observers report their findings. During the many recent controversies on disinformation in elections, international Election Observation Missions (EOMs) contributed little, because the traditional election observation methodology did not provide any means to analyse this emerging area of concern. A survey of eight major election observation organizations shows that they understand the problem and are ready to address it, although only a few have taken concrete steps to do so (see Annex 1 for details).

The European Union and the National Democratic Institute (NDI) have been more proactive, as have smaller election specialists from MEMO98 (Slovakia) and Democracy Reporting International (author of this report). The much-needed connections between election observers and other communities such as data analysts and journalists, academic researchers and disinformation experts are beginning to be made.

Feedback from the principal international election observation organizations and the outcome of interviews with experts from 18 governments and non-governmental actors that engage in monitoring disinformation on social media (details in Annex 2), highlights the contrasts as well as the space for synergies:

- Disinformation initiatives have a **headstart**: they have already been experimenting with methods of monitoring social media and in reporting on outputs. They have technical knowledge of tools for monitoring, even though there is no established overall framework to address social media/online disinformation in elections. While some initiatives try to approach the issue with intensive technological developments using software and AI solutions, others focus on content-specific aspects of disinformation, narrowing down the analysis to lines of enquiry that are specific to their political contexts.
- Reactive vs long-term observation: initiatives to tackle disinformation tend to be reactive. Often, they try to follow developments in real time and to intervene by debunking stories and alerting platforms, authorities or the wider public. Traditional election observation does not directly react to electoral developments, to avoid becoming part of the campaign. For this reason, it usually only provides an overall assessment of the electoral process after election day.
- Ecosystem vs single players: Several initiatives to fight disinformation work in coordination with other groups, such as factcheckers or journalists. The major EOMs are stand-alone actors. They exchange information with other groups but aim to give an overall verdict based exclusively on their own findings. EOMs tend to be more visible, but in recent elections reports by disinformation groups may have eclipsed the coverage of traditional election observers' findings.

- Experimentation: Disinformation groups experiment with social media monitoring focusing on different tools, platforms, actors and forms of expression. International election observers follow their set methodologies. International election observation is a politically sensitive activity, mostly based on an invitation by the host government, so international observers have little scope for experimentation.
- Guidelines & methodology: International election observers follow a detailed methodology, the essence of which is written into the *Declaration of Principles for International Election Observation* from 2005. In the disinformation field there is no agreed framework, and discussions on overall questions of methods, tools, approaches and ethics of social media monitoring are still in the early stages. Reports on disinformation usually include neither assessment nor measurement of the impact or relevance of certain disinformation campaigns.

Given that disinformation monitoring by non-EOMs is more developed, there are good practices to be found in the work of these groups on many of

the challenges - such as the size of the data, the shortcomings of existing software for social media monitoring and the comparison between contexts.

These provide a lot of material for election observers to consider and to develop further. To make the analysis of social media in elections more effective, we recommend:

- That disinformation monitors and election observers create more links and co-operate more systematically;
- Civil society initiatives provide a set of best practices that do not put the reputation of EOMs at risk when monitoring the impact of social media during elections. These initiatives should be adopted.

More recommendations can be found at the end of the report. The organizations and initiatives covered in this report do not provide a comprehensive list of each relevant actor or method used. However, the case studies provide ideas and approaches that can guide the monitoring efforts of EOMs.

INTRODUCTION

Social media platforms have become a major influence on elections: they are increasingly being used to shape political opinion and beliefs generally, and in electoral periods they influence voter choices. Reports from many countries have shown that disinformation attempts to manipulate elections, be it via discrediting campaigns, external influence or trying to suppress voter turnout. Some may represent violations of electoral or other rules, while others may not be illegal in national legislation, but are nevertheless inconsistent with the idea of fair campaigning as outlined in international law. Besides disinformation, social media also facilitates the placement of paid political and issue-based ads, targeted to the preferences of different groups of voters.

Referring to legislation when it comes to social media monitoring poses an additional challenge to initiatives that wish to use it as guidance when defining the scope of their analysis. So far, regulation on what is acceptable or not when it comes to social media use for political purposes is very fragmented, and in the very few countries where laws have been put in place, it is still too early to assess whether they

are having positive results. Some of the companies behind these platforms have enforced self-regulatory measures which usually increase the requirements for users running political ads or advertise on matters of national interest. They have created several Ad Libraries to increase transparency about who runs such ads and which groups are being targeted. Legislative efforts may help guide monitoring efforts in the future, but regulatory initiatives both at the national¹ and international² levels need to be developed further before they can provide clear guidelines for electoral observers.

Election Observation Missions – whether international missions or domestic observer groups – used to provide an authoritative voice on the integrity of a given election. However, with social media now an important aspect of electoral dynamics and legislation failing to respond to its challenges, these missions have lost relevance, since their assessment does not usually include an analysis of the role of social media. Instead, it has been left to investigative journalists, monitoring initiatives, data protection groups, intelligence services and factcheckers to reveal disinformation on social media.

The NetzDG is an example of legislation applied by Germany to address hate speech on social media platforms. Other initiatives aiming at regulating aspects of social media have been attempted in France, UK, Italy, Czech Republic and others (in Goldzweig et. al (2018) "Beyond Regulation: Approaching the challenges of the new media environment", Dahrendorf Forum. Available at: https://www.dahrendorf-forum.eu/wp-content/uploads/2018/12/Beyond-Regulation_Final.pdf

² Such as the *EU Action Plan against Disinformation*. Available at: https://eeas.europa.eu/headquarters/headquarters-homepage/54866/action-plan-against-disinformation_en

Election observers have only belatedly woken up to the challenges. Some have started introducing expertise to their missions and a few have published initial scoping papers and results. This paper will look at these emerging practices, identify good examples and compare them to disinformation analysis done by non-election observer groups (groups that do not observe elections as their core business). We have studied three main groups of actors for this comparison:

 The main organizations that deploy international election observation missions based on the 'Declaration of Principles', the leading methodological document;

- State actors in the EU that track disinformation;
- Non-state actors that look at disinformation in the EU, with a few examples from beyond the EU.

The study is based on oral and written interviews or surveys with eight election observation organizations and with interlocutors from 18 governments or non-governmental organizations that monitor social media for political purposes. We also reviewed published documents from six initiatives. This study was researched and written by Rafael Schmuziger Goldzweig (DRI Social Media Research Coordinator), Bruno Lupion (researcher) and Michael Meyer-Resende (DRI Executive Director).

CONTEXT

THREATS TO ELECTORAL INTEGRITY IN SOCIAL MEDIA

The Oxford Internet Institute notes:

"The number of countries where formally organised social media manipulation occurs has greatly increased, from 28 to 48 countries globally. The majority of growth comes from political parties who spread disinformation and junk news around election periods. There are more political parties learning from the strategies deployed during Brexit and the US 2016 Presidential election: more campaigns are using bots, junk news, and disinformation to polarise and manipulate voters."

While it is clear that social media is used to manipulate discourse and opinions around elections. The way this is done varies according to a set of variables still to be defined. Are they being carried out by domestic actors or foreign powers? Is it a coordinated action or attempts from several groups? Do they rely on automated bots, human trolls, paid advertising or sharing by sympathetic networks? Which narrative strategies do they use? What type of disinformation should be tracked when it comes to electoral influence? The guiding principles of electoral observation missions can shed light on some of these questions.

THE FRAMEWORK OF INTERNATIONAL ELECTION OBSERVATION

The reference framework for election observation is grounded in human rights. The principle organizations that deploy observers either apply obligations and commitments that their member states freely adhered to - for example in the case of the Organization for Security and Co-operation in Europe (OSCE), the African Union (AU) and the Organization of American States (OAS) – or to international human rights obligations, in the case of countries that deploy observers to countries other than their own. This is the case for the EU, the NDI and the Carter Center.

The right to vote in elections and to stand as a candidate (Article 25 International Covenant for Civil and Political Rights) provides the cornerstone in this framework, with other political rights being equally essential - such as the freedoms of expression, opinion and assembly and the right to an effective remedy (independent courts) to address possible rights violations. The framework of election observation encompasses the elements of a democratic, rule-of-law based state which observer groups monitor for an extended period – belying the journalistic caricature of a blind focus on election day.

Discourse on social media fits into this framework from several perspectives. Most importantly, freedom of expression implies that "everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice." (Article 19 ICCPR).

Social media are an important tool to expand these freedoms, but when manipulated they can undermine them. Much of the debate on freedom of expression is concerned with restrictions, and less with a manipulative use of social media and other online content. However, the right to vote and to participate in political life is also concerned with the systemic aspects of opinion *formation* (and not only *expression*). The UN's Human Rights Committee (the monitoring body of the International Covenant on Civil and Political Rights), noted in its *General Comment* 25 (the right to vote and political participation):

"Persons entitled to vote must be free to vote for any candidate for election and for or against any proposal submitted to referendum or plebiscite, and free to support or to oppose government, without undue influence or coercion of any kind which may distort or inhibit the free expression of the elector's will. Voters should be able to form opinions independently, free of violence or threat of violence, compulsion, inducement or manipulative interference of any kind."

THE DECLARATION OF PRINCIPLES OF INTERNATIONAL ELECTION OBSERVATION

Initiated by the NDI in 2005, several leading international election observation missions – under the aegis of the UN – endorsed the *Declaration of Principles of international election observation*, which have been backed by more than 60 groups. They form the basis for the annual meeting of leading international observer organizations. The principles set out the recognised international approach for election observation, and serve as a quality seal that contrasts the practices of fake observer groups that have sprung up in authoritarian states. They elaborate the foundation of democratic elections in human rights.

They define international election observation as:

"(...) the systematic, comprehensive and accurate gathering of information concerning the laws, processes and institutions related to the conduct of elections and other factors concerning the overall electoral environment; the impartial and professional analysis of such information; and the drawing of conclusions about the character of electoral processes based on the highest standards for accuracy of information and impartiality of analysis. (...) observer missions must make concerted efforts to place the election day into its context and not to over-emphasise the importance of election day observations."⁵

⁴ UN Human Rights Committee, General Comment 25, 1996, point 19

⁵ Point 4 of the Declaration

The *Declaration* also states that its endorsers "recognise that international election observation missions must be of sufficient size to determine independently and impartially the character of election processes in a country and must be of sufficient duration to determine the character of all of the critical elements of the election process in the pre-election, election-day and post-election periods."

Applied to social media, these principles raise several challenges, especially in view of the huge amount of material being posted on social media during an electoral period:

- What would a systematic gathering of discourse on social media look like? What would be the criteria and the plan for doing so?
- Comprehensive: is it realistic that observers could comprehensively assess the social media sphere? As the US 2016 elections showed, unexpected problems may be discovered much later, such as the disinformation campaigns by the Russian 'Internet Research Agency'. Will observers be able to detect significant problems while an election is unfolding?

- Accuracy: the analysis of social media is a new field with many discussions about the accuracy of different methodologies. There are wide-ranging debates, for example, on what a social bot is, what disinformation means and how to measure the sentiments of written texts.
- Impartiality: disinformation and hate speech can emanate from many political sources. Observers would need to follow all of those that may have a significant impact.
- Drawing of conclusions: the research on the impact of social media on political opinion and voter choice and behaviour is not rich, and it is difficult to determine the impact of disinformation. 900,000 Americans saw the headline that falsely claimed that Pope Francis had endorsed Donald Trump as the best candidate for President. But how much weight does one false story carry when people consume news every day?
- Sufficient size: if it was possible to gather a comprehensive, accurate and systematic view of flaws in social media discourse, how big would that mission be?

This paper surveys the practice and intentions of international election observer groups on social media monitoring and explores what other groups are doing in this field, in particular in the EU, in order to provide inspiration for tradition election observers.

WHAT ARE INTERNATIONAL OBSERVER MISSIONS DOING ON SOCIAL MEDIA DISCOURSE?

International EOMs have only belatedly started to pay attention to social media discourse. The question of social media figured in discussions of the annual meeting on the *Declaration of Principles*, the main meeting of international election observers, in 2017 and 2018. However, while this forum has addressed many questions of methodology in detail, it has only discussed the bigger picture when it comes to social media. Of the international groups, the NDI and the EU seem so far to have been the most agile.

The NDI included in its 2017 Kenya report a paragraph summarizing the country's social media landscape and highlighting examples of disinformation campaigns. They also addressed the problem of disinformation in the mission sent to Liberia on that same year, despite not addressing specifically the role of social media due to extremely limited internet penetration. The organization posted a long-term 'disinformation analyst' to its Georgia election observation mission in 2017. In its support of domestic election observer groups, NDI has started providing technical assistance, including

data collection and analysis tools. It has an internal guidance note on 'disinformation and electoral integrity'.

The EU included a chapter on the analysis of 'online related content' in its *Election Observer Handbook*⁹. It follows the chapter on the monitoring of traditional media, and mostly explores the role of online media and looks at freedom of expression issues (restrictions of content) and hate speech issues. It does not cover the question of public discourse on social media and the disinformation threat. So far EU EOMs have only provided limited information on online content and social media.

Recent EU EOMs sometimes included a short chapter with an overview of the social media landscape (main networks, numbers of users)¹⁰ and some impressions on their use, but most of them contained little information on social media discourse, and no structured monitoring nor quantification of social media activity during the campaign.¹¹

- NDI. Available on pp42-43 at: https://www.ndi.org/sites/default/files/NDI%20Final%20Interational%20Election%20
 Observation%20Mission%20Report%20-%20Liberia%202017%20Presidential%20and%20Legislative%20Elections%20%282%29.

 pdf
- 8 NDI. Available on p12 at: https://www.ndi.org/sites/default/files/NDI-GE%20EOM%202017-%20IR-ENG.pdf
- 9 EU Election Observer Handbook, Third Edition, 2016
- 10 Final Report EU EOM to Pakistan, 2018
- 11 Final Reports of EU EOMs to Lebanon 2018, Zimbabwe 2018, Tunisia 2018, Liberia 2017

The EU is currently undertaking many activities to improve the capability of EU EOMs, including

- the inclusion of a digital analyst in an EU EOM for the first time (Nigeria);
- a workshop on EOM monitoring of online campaigns, held by the EODS project;
- Democracy Reporting International will bring together a working group under the EU-funded Supporting Democracy project to develop a methodology for social media monitoring in elections for the use of any interested group (international or national).

These initiatives are in addition to a wide-ranging effort to deal with EU internal disinformation challenges.

Annex 1 provides an overview of the status quo of the principal international election observation groups.

WHAT ARE EUROPEAN GOVERNMENTS DOING?

Overall, governments seem to take a more cautious approach to social media monitoring than civil society organizations do. This is probably because it may be perceived as surveillance of individual citizens or that a government is trying to get an informational advantage - even if only publicly available data (public posts on social media) are monitored without a focus on individuals.

Governments and intergovernmental bodies appear to mainly deal with disinformation as it relates to factual inconsistencies around the electoral process and, when it comes to the origins of disinformation, external actors (state and non-state alike). The following table summarizes some initiatives.

TABLE 1
Government initiatives on social media monitoring

GOVERNMENT EUROPE/INTERGOVERNMENTAL Country / Has ever monitored or is **Focus on domestic** Software/ **Body** Scope Range organization monitoring elections? actors or foreign tools used Which ones? influence NATO StratCom NATO / Round the clock Both Twitter Tools built Monitors Center of Based monitoring not specifically automation, and in-house Excellence in Latvia in election periods bots and VKontakte trolls Swedish Swedish 2018 Twitter Sweden Both Monitors Tools built Defence elections influence and in-house discussion Research operations, Agency threats to boards elections East StratCom EU Yes, but not exclusively. Focused Monitors TV, BrandWatch webpages, Task Force on Russian disinformation Got budget and new employees to monitor runinfluence on Facebook up to the 2019 European the Eastern and Parliament elections Neighbourhood Twitter No. Initiatives to counter German Both, with a greater Positive Germany Ministry of disinformation by focus on foreign narratives Foreign Affairs disseminating German regarding influence facts/narratives in foreign Germany countries as a public to counter diplomacy tool disinformation Policy France Foreign Monitors Yes, but not Planning comprehensive. Published influence disinformation Staff (CAPS), a concept paper & case campaigns, Minister for study on the 'Macron leaks' harmful Europe and narratives, Foreign Affairs12* media ecosystem, bots and trolls Inter-ministerial Denmark No. Issued an action plan Focus on Monitors task force: to build resilience ahead of Russian influence Ministry of the 2019 General Danish influence campaigns Elections (disinformation) Justice, Defence and Foreign Affairs13* Yes, 2017 Presidential Centre against Czech Focus on Monitors Terrorism and Republic Elections. The Centre Russian disinformation, Hybrid Threats monitors threats related to influence foreign (Ministry of the internal security of the propaganda the Interior)14* Czech Republic, including and terrorism disinformation campaigns threats

^{*} Based on desk research and not interviews.

¹² Available at: https://www.diplomatie.gouv.fr/en/french-foreign-policy/manipulation-of-information/article/joint-report-by-the-caps-irsem-information-manipulation-a-challenge-for-our

¹³ Available at: http://um.dk/en/news/newsdisplaypage/?newsid=1df5adbb-d1df-402b-b9ac-57fd4485ffa4

¹⁴ Available at: https://www.mvcr.cz/cthh/clanek/centre-against-terrorism-and-hybrid-threats.aspx

Government initiatives are generally more focused on geopolitical aspects of electoral monitoring - namely attempting to avoid external actors (state and non-state alike) from influencing national elections. This is the case when we look at the French, German, Czech and Danish examples, which also focus on questions related to security and terrorism threats.

When it comes to initiatives monitoring national elections, the Swedish government seeks to avoid factual inconsistencies around the management of the electoral process. It monitored online commentary and discussion boards on Swedish websites to look for posts that conveyed a threat to the Swedish elections, such as planned attacks on polling stations.

Obviously, governments may do much more through intelligence agencies, which cannot be assessed by this study (a report by Privacy International¹⁵ explores the limits of data collection from intelligence agencies, but does not cover how intelligence services monitor social media in elections).

Two intergovernmental initiatives – the East StratCom Task Force and the NATO StratCom Center of Excellence – have different scopes: the former is an EU initiative to spot, debunk and compile disinformation narratives led by Russia, while the latter is a research centre that channels expert opinion to NATO.

WHAT ARE CIVIL SOCIETY ORGANIZATIONS DOING?

The following sections map 17 initiatives from non-governmental actors in the field of social media monitoring during elections. They were selected based on desk research on the 28 EU member states and relevant initiatives in the US and other non-European countries. Potential interviewees were contacted via email from 17 December 2018 onwards, and interviews were conducted between 19 December 2018 and 24 January 2019. A more comprehensive description of each organization/initiative can be found in Annex 2 of this study.

EUROPEAN CIVIL SOCIETY

Many initiatives are experimenting with social media monitoring of political trends in Europe. We interviewed nine initiatives at the European level to understand details on the monitoring exercise they have done, as well as the phenomena they are monitoring on each platform and the tools used for the analysis. The following table summarizes the initiatives.

TABLE 2

Non-governmental initiatives on social media monitoring (Europe)

NON-GOVERNMENTAL INITIATIVES

(civil society, academia, think tanks, consultancies)

EUROPE								
Organization/ Initiative	Country	Has monitored or will monitor social media in which elections?	Domestic actors or foreign influence	Phenomena	Range	Software, tool or service used		
EU Disinfo Lab	Belgium	Italian 2018 Federal Elections	Both	Disinformation and hyperactivity	Twitter	Visibrain, Gephi		
Prague Security Studies Institute	Czech Republic	Czech Parliament Election in 2017 and Senate and Presidential Elections in 2018. Will monitor the EU Parliament Election in 2019	Both	Disinformation, but also looking at broader context	Websites and Facebook public pages	Versus		
Debunk.eu	Lithuania	Not the main focus, but will monitor Lithuanian Presidential and Municipal Elections in 2019	Prioritise foreign influence	Disinformation	Websites and Facebook public pages. Plans to include TV broadcasters and video using speech to text technology	Tool built in-house		
Stiftung Neue Verantwortung (SNV)	Germany	2017 German Federal Elections	Both	Disinformation	Websites, Facebook public pages and posts and Twitter	TalkWalker		
European Values Think- Tank / Kremlin Watch	Czech Republic	Czech Presidential Elections in 2017 and Parliament Elections in 2018	Foreign (Russia)	Disinformation and hostile influencing activities	Websites and Facebook pages	-		
Oxford Internet Institute (OII) / Computational Propaganda Project	UK	Not the main focus, but monitored the 2017 UK General Election and several others	Both	Political bots and disinformation	Facebook and Twitter	Tools built in-house		
Bakamo.Social	UK	2017 French Election	Both	Disinformation and thematic or emotional patterns	Twitter	TalkWalker		
		E	ASTERN EUROPE					
Atlantic Council / Ukrainian Election Task Force	Ukraine	2019 Ukrainian Presidential Election	Foreign influence, mainly Russia	Disinformation, cyberattacks, kinetic operations	TV broadcasters and webpages	Semantic Visions		
International Society for Fair Elections and Democracy (ISFED)	Georgia	Georgian 2018 Presidential Elections	Both	Violation of electoral laws, disinformation and Russian narratives	Facebook	Fact-a-lyzer		

European initiatives by civil society during elections have multiplied since 2017. Without an overarching methodology to follow, the projects focused on different aspects and adapted to the restrictions of data that can be collected (especially in relation to Facebook), as well as the needs of the specific political contexts. In terms of phenomena, the focus was on monitoring disinformation (during and outside elections); in the case of Eastern Europe, with a particular focus on disinformation campaigns coming from Russia.

Some initiatives explored in detail the use of social media in specific elections (Bakamo.social, ISFED, SNV, Prague Security Studies Institute), while others tried to actively fight disinformation in partnership with factcheckers (Debunk.eu). Selected best practice from such initiatives will be featured in the final section of this report.

A GLIMPSE BEYOND EUROPE

To complement the survey of European initiatives, it is useful to consider some specific projects from outside Europe that focussed on monitoring social media in elections. Non-governmental initiatives around the world are helpful in identifying rising trends and challenges that can inform the work of EOM on social media monitoring. This section lists eight organizations in the US, Brazil and Nigeria that are working nationally or globally in topics related to disinformation, Russian interference and monitoring of paid ads.

TABLE 3

Non-governmental initiatives on social media monitoring (outside of Europe)

NON-GOVERNMENTAL INITIATIVES

(civil society, academia, think tanks, companies)

OUTSIDE OF EUROPE / GLOBAL							
Organization/ Initiative	Country	Has monitored or will monitor social media in which elections?	Focus on domestic actors or foreign influence	Phenomena	Range	Monitoring software, tool or service used	
Alliance for Securing Democracy / Hamilton 68 Dashboard	US	Monitored electoral content during the run-up to the US 2018 midterm elections	Foreign influence (Russia)	Disinformation	Twitter	Own platform based on Twitter API. Version 2.0 developed by Graphika	
Atlantic Council / Digital Forensic Research Lab	US	French and German elections in 2017, Mexican and Brazilian elections in 2018, European Parliament, Indian and South African elections in 2019	Both, highlights when foreign influence	False accounts, false narratives, bots and disinformation	Several, including Facebook, Twitter and YouTube	Buzzsumo, CrowdTangle, Sysomos and Twitonomy, among others	
International Republican Institute / Beacon Project	US / EU	Monitoring also captures run-up to elections	Both, with a greater focus on foreign influence	Disinformation and hostile foreign influence	Websites, Facebook, Twitter	Versus	
Getulio Vargas Foundation / Digital Democracy Room	Brazil	2018 Brazilian General Elections	Domestic, with some references to foreign	Polarisation, disinformation, bots	Facebook, Twitter, YouTube	-	
Center for Democracy and Development West Africa (CDD) & University of Birmingham	Nigeria/ UK	2019 Nigerian presidential elections	Not specified	Disinformation	WhatsApp	Surveys and focus groups	
Who Targets Me*	UK / Global	Monitored political ads since it was launched in 2017	Not specified	Not specified	Facebook	Browser extension for Chrome or Firefox	
Political Ad Collector / ProPublica*	US	Monitored political ads since it was launched in 2017	Not specified	Not specified	Facebook	Browser extension for Chrome or Firefox	
Ad Analysis / Mozilla*	US / Global	Monitored political ads since it was launched in 2018	Not specified	Not specified	Facebook	Browser extension for Firefox	

^{*} Based on desk research and not interviews

Overall, such projects share the same trends as the European initiatives: some are more focused on one specific topic (the Hamilton 68 Dashboard focuses on Russian influence) while others take the broader national context into consideration (Digital Democracy Room looks into political polarisation and public discourse online in Brazil).

It is worth highlighting three initiatives that tried to address the need for transparency regarding paid ads on Facebook, a concern that gained traction after the Russian Internet Research Agency placed paid ads during the 2016 US election which were seen by 10 million people, according to Facebook¹⁶. Three initiatives (Who Targets Me, Political Ad Collector and Ad Analysis) tried to bypass the lack of data disclosure surrounding paid ads by asking users to install browser extensions that scraped details about Facebook ads shown to them. The first two, launched in 2017, offered details about targeted political ads on Facebook, while the third, launched in October 2018, has not had much time to be tested.

In light of its promise to make ad libraries available in other countries, Facebook temporarily blocked access to such tools in January 2019, citing privacy concerns. In response to this move, ProPublica said that the information provided by Facebook was incomplete and that the organization has routinely publicised ads run by organizations that were not recorded in the archive¹⁷. According to Who Targets Me, the core functions of their extension are still working and able to collect data from ads, but Facebook has blocked access to some components of the extension.

NON-GOVERNMENT INITIATIVES: EUROPE & BEYOND

Table 4 summarizes the actions of non-governmental initiatives in Europe and around the world, comparing monitored phenomena and platforms.

¹⁶ Facebook Newsroom. Available at: https://newsroom.fb.com/news/2017/10/hard-questions-russian-ads-delivered-to-congress/

¹⁷ The Verge (2019). Available at: https://www.theverge.com/2019/1/28/18201361/facebook-political-ad-transparency-tools-blocked-user-data-privacy

TABLE 4Non-governmental initiatives matrix

NON-GOVERNMENTAL INITIATIVES MATRIX: WHO HAS MONITORED OR IS MONITORING WHAT, ON WHICH PLATFORM?						
	Facebook	WhatsApp	Twitter	YouTube	Websites / discussion boards	Traditional media (TV, radio)
Disinformation/ information manipulation	Debunk. eu, Prague Security Studies Institute, SNV, Kremlin Watch, Oxford Internet Institute, Digital Forensic Research Lab, Beacon Project, Digital Democracy Room, ISFED	CDD & University of Birmingham, Digital Forensic Research Lab	Hamilton 68 Dashboard, EU Disinfolab, SNV, Oxford Internet Institute, Digital Forensic Research Lab, Beacon Project, Digital Democracy Room, Bakamo. Social	Digital Democracy Room, Digital Forensic Research Lab	Debunk. eu, Prague Security Studies Institute, Kremlin Watch, Ukrainian Election Task Force, SNV, Beacon Project, Digital Forensic Research Lab	Ukrainian Election Task Force
Bots/trolls	Digital Forensic Research Lab	-	Oxford Internet Institute, Digital Forensic Research Lab, Digital Democracy Room, Hamilton 68 Dashboard, EU Disinfolab, Bakamo.Social	-	-	-
Russian influence	Debunk.eu, Kremlin Watch, Beacon Project, ISFED	-	Hamilton 68 Dashboard, EU Disinfolab, Beacon Project, Bakamo.Social	-	Debunk. eu, Kremlin Watch, Ukrainian Election Task Force, Beacon Project	Ukrainian Election Task Force
Political ads	Who Targets Me, Mozilla Ad Analysis, ProPublica					

Topics/objects of analysis

Most of the initiatives covered focus on disinformation, with investigations of Russian influence associated with many of them. Bots, trolls and the role of internal groups were studied mainly by initiatives looking at different political debates online, not necessarily during elections (namely the Oxford Internet Institute and the Digital Forensic Research Lab). Some projects focused on the role of internal groups and their use of social media. Stiftung Neue Verantwortung research concluded that the Alternative für Deutschland party and far-right groups used disinformation as an important political mobilisation strategy during the 2017 German parliamentary election campaign. The Digital Democracy Room also found that right-wing groups were prone to use disinformation to mobilise voters during the Brazilian elections.

Debunk.eu in Lithuania stands out for its use of AI to automatically spot news articles with a high probability of being disinformation, and the support of a network of volunteers and newsrooms to confirm and debunk them. Beacon Project developed a web crawler that scrapes and sorts predefined sources within a given country. It offers a free tool to partner organizations, one of which is the Prague Security Studies Institute, which will use this platform to monitor the 2019 European Parliament elections in the Czech Republic. Another initiative in the Czech Republic is Kremlin Watch, which looks for disinformation supporting Russian interests in around 40 websites in the Czech language and their Facebook pages, not necessarily related to elections. The Ukrainian Election Task Force focused on the March 2019 presidential elections and aims to highlight disinformation to an international audience, rather than to the Ukrainian public.

Lastly, the link between disinformation and paid political or issue ads remains a central aspect when it comes to social media monitoring. As mentioned, the browser extensions Who Targets Me, Ad Analysis and ProPublica¹⁸, which tried to collect information on ads, had difficulties to access Facebook data. Facebook has started providing information about political ads through its Ad Library. The Ad Library is officially available for all countries and territories - from Antarctica to Western Sahara. What is unclear, however, is the amount of data included in each of the Ad Libraries. Browsing for information within them, we notice that libraries in the U.S., UK and Brazil are much more complete than the ones available for Nigeria and Tunisia, for example. There are similar discrepancies in the Ad Libraries available for EU countries. So far, detailed information is available about active and inactive ads in the U.S., with a consolidated list of organizations that paid for political ads and data easily searchable by keywords or organization names. For other countries (Nigeria, for example), none of this data is available. One can only look into active ads and search for the pages who are running them - it is not possible to check for inactive ads or search for ads using keywords¹⁹.

Google also launched an EU-wide searchable ad library for political ads, but it allows only searches for candidates and advertisers – not by topic²⁰. Twitter committed to make all political ads related to the European Parliament elections available in its Ads Transparency Centre, providing a list of all registered organizations allowed to place political campaign advertising²¹. As with Facebook, these measures do not apply in several other countries.

Apart from their efforts to make political ads more transparent, the companies increased the requirements for those posting political ads on

¹⁸ ProPublica (2019). Available at: https://www.propublica.org/article/facebook-blocks-ad-transparency-tools

More detailed information about the differences between ad libraries in the US and the EU is available here: https://democracy-reporting.org/facebooks-ad-library-for-european-parliament-elections-seven-steps-to-make-it-more-useful/

²⁰ Google Ad Library: https://transparencyreport.google.com/political-ads/region/EU?hl=en

²¹ Available at: https://ads.twitter.com/transparency/i/political_advertisers

their platforms. These include the obligation to prove registration in the relevant country, which makes foreign funding of political campaigns more difficult. For example, Facebook requires residency in Australia, Brazil, India, Indonesia, Israel, Thailand, Ukraine, UK, EU countries and the U.S. to run ads in these countries²². Google requires all election ads to show a disclosure identifying who paid for them and, like Facebook, says that sponsors of posts must be registered in the country where the political ad is being run. However, this currently applies only to the EU, India and the U.S.²³. The certification process was also implemented by Twitter in the U.S., Australia, India and the EU²⁴. While these requirements do not apply to all countries where these companies do business, they are being gradually implemented, and can influence the scope of observation by EOMs. The more data companies make available, the more there is to observe and analyse. Assessing the stated policy of the firms and whether it is being implemented is an obvious area for observation.

Platforms

In Europe, non-governmental initiatives have focused on two platforms: **Facebook** and **Twitter**. Websites, discussion boards and traditional media are also seen as relevant, mainly in countries that fear Russian interference, given the relative prominence of state-backed Russian media outlets such as Russia Today and Sputnik.

Beyond Europe, the fact that WhatsApp and YouTube are hardly monitored or analysed leaves gaps, given the influence both platforms have in shaping political opinion and voter choice. WhatsApp was reported to

have been influential in the recent elections in Brazil. The private messaging app is widespread in the country, and actions taken by Facebook and Twitter to fight disinformation networks in their platforms may have prompted campaigners to become more active on WhatsApp, an encrypted platform.

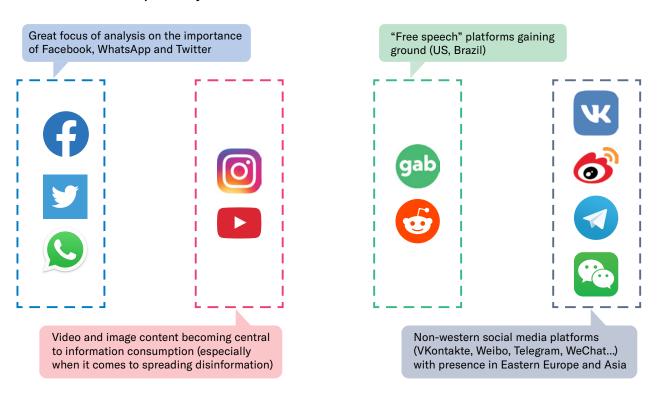
The use of WhatsApp is being monitored in the current election campaign in Nigeria. Researchers who analysed its impact in Sierra Leone indicated that its use is closely related to offline social structures. The mean size of groups in West Africa and Latin America is bigger than the ones in Europe, meaning that the viral aspect of such platform varies from country to country and is related to cultural habits, socioeconomic conditions and the level of connectivity available to users (particularly when it comes to mobile vs fixed broadband access).

Facebook has received attention outside Europe because of its political importance as the most popular social media platform. Twitter attracts similar attention for the ease of collecting and analysing data and because it is a service typically used for political debates. WhatsApp is a rising platform for the manipulation of public opinion in elections in Brazil and Nigeria. A few of the researched initiatives mentioned the role of YouTube, but none of them monitored platforms such as Instagram, Reddit and Gab, or Telegram, VKontakte, WeChat or Weibo. Research has been done on some of these platforms²⁵²⁶, but they were not mentioned in the interviews conducted by this study.

The social media landscape is dynamic, and observers should stay tuned to trends and monitor those that are relevant.

- 22 Available at: https://www.facebook.com/business/help/208949576550051#
- 23 Available at: https://support.google.com/adspolicy/answer/6014595?hl=en
- 24 Available at: https://business.twitter.com/en/help/ads-policies/restricted-content-policies/political-content.html
- Bandeira, Luiza (2018) "#ElectionWatch: Migration to Gab in Brazil", DRFLab. Available at: https://medium.com/dfrlab/electionwatch-migration-to-gab-in-brazil-67a1212c4c76
- 26 Nithyanand, Rishab (2018) "Russian propaganda spread on our site before 2016 election", Data and Society. Available at: https://matasociety.net/output/reddit-russian-propaganda-spread-on-our-site-before-2016-election/

FIGURE 1
Social media landscape and dynamics



Other social networks such as Gab and Reddit are benefitting from the shifting preferences of social media users, and gaining attention from users who question the community guidelines enforced by platforms such as Facebook, Twitter and others. Brazilians and U.S. Americans are among the top users of Gab, with spikes in registrations during the Charlottesville unrest and the recent presidential elections in Brazil²⁷. While neither is likely to overtake other social media platforms in popularity, they are spaces where extremist groups can organise themselves online without controls, offering them a quick way to coordinate disinformation campaigns and inflammatory speech on other social media platforms.

When it comes to content, visual forms of communication are increasingly central to

information consumption on social media. On Twitter, video content generates ten times more engagement than text-only tweets²⁸. Disinformation often uses manipulated or misleading video content. This trend makes platforms such as Instagram and YouTube important tools for disinformation, but few of the initiatives researched for this study have been looking at these platforms.

Lastly, non-Western social media such as Weibo, WeChat, VKontakte and Telegram, among others, present a challenge when it comes to social media monitoring in contexts where they coexist with Facebook, Twitter and WhatsApp. This is the case in some Eastern European countries, where VKontakte and Telegram have a relatively important presence, alongside Facebook, Twitter and WhatsApp.

²⁷ APublica (2018). Available at: https://apublica.org/2018/12/rede-social-de-ultradireita-chega-ao-brasil-com-acenos-a-bolsonaro/

²⁸ Twitter Business. Available at: https://business.twitter.com/de/blog/5-data-driven-tips-for-scroll-stopping-video.html

Monitoring tools

The organizations listed above use a variety of tools to monitor social media and digital content. They can be complex or easy to operate, free or paid, and off-the-shelf or bespoke solutions, sometimes built in-house. Most tools used are originally designed for business purposes and have been adapted to examine political content. They include:

CrowdTangle, a social media analytics solution bought by Facebook in 2016. It can monitor Facebook, Twitter, Instagram and Reddit. However, it is not publicly accessible and only offered by Facebook to selected partners.

TalkWalker, a paid, off-the-shelf tool for social media listening, analytics and reporting, used mainly for business purposes, but also useful for monitoring political and electoral content. However, its access to Facebook data was restricted after a change in the Facebook API. Others off-the-shelf solutions are **Sysomos, BrandWatch** and **Visibrain**.

Twitonomy is a platform for listening and analysing posts on Twitter, which is also useful when looking at the historical behaviour of Twitter accounts.

Versus is a platform developed by Beacon Project (International Republican Institute) and offered for free for partner organizations. It can scrape content from pre-defined sources, such as websites or Facebook public pages, and organise it automatically, allowing analysts to filter, sort and tag the content.

Fact-a-lyzer is an NDI/Open Election Data Initiative platform that facilitates data collection and analysis of insights for social media monitoring purposes. It was piloted for the Georgia 2018 elections in cooperation with the Georgian NGO ISFED. It facilitates data collection, coding and visualisation of publicly available data, and it was specifically designed to monitor Facebook in a political context (differently from platforms originally designed for marketing purposes).

There is no one-size fits all tool to facilitate and optimise data collection and analysis for political purposes. The adaptation of business intelligence tools demands not only the knowledge to use them, but creativity to combine them with other tools to gather relevant insights in an electoral context.

A challenge to overcome is to ensure that organizations and EOMs have access to data from Facebook, with tools for monitoring this context adapted to elections.

GUIDELINES FOR EOMs

The review of the practices of those organizations, government agencies or international initiatives provides insights that can inform the work of EOMs in monitoring social media.

MONITORING OF SOCIAL MEDIA VS TRADITIONAL MEDIA

The experience of social media monitoring is different from the monitoring of traditional media undertaken by many EOMs. Traditional media usually encompasses a limited set of actors (TV and radio stations, newspapers). Social media is far more complex, with a myriad of actors and content. By definition social media is shaped not only by "institutional actors" (governments, media, parties) but by many unofficial influencers (individuals, groups sympathetic to a party or a programme, etc.).

The selection of TV or radio stations to be monitored is based on relatively simple metrics:

"Those selected should include state/public and privately-owned media outlets, and ensure a varied balance considering, for example, political leanings and target audiences. Media aimed at minorities should be considered for monitoring, and the geographical balance

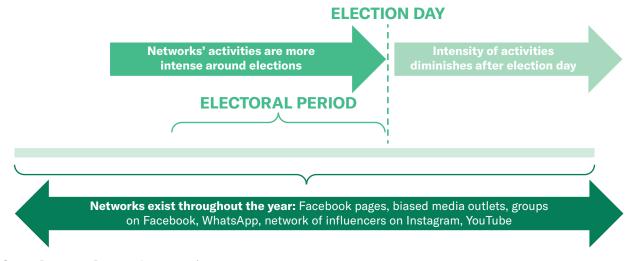
of the regional media should also be taken into account. For broadcast media, the media analyst normally monitors all programmes during primetime broadcasts and other election-related programming for the entire period of the defined campaign period. Television and radio programmes are recorded by the EU EOM and stored until the end of the mission."29

Selecting actors on social media is much more complex:

- The reach of traditional media is relatively clear (based on audience numbers). On social media, some private or anonymous accounts/sites/users that carry political content may have a wide reach, but it may not be easy to identify them.
- The number of actors: Traditional media include a known number of known TV or radio stations, while on social media the number of potential actors is huge.
- Size of material: Traditional media monitoring analyses some 100 hours of coverage. Social media monitoring must analyse millions of posts.
- Social media is dynamic: On social media an account may reach a large audience one day but be irrelevant on another. In contrast, traditional media's reach is relatively stable.

FIGURE 2

Timing: Disinformation networks act during election campaigns, but also permanently

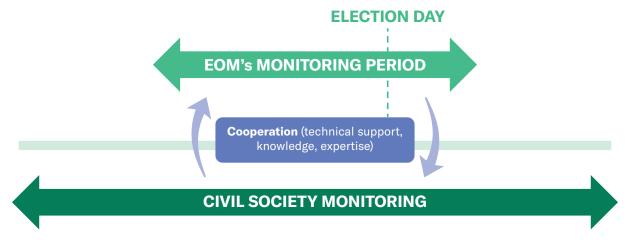


Source: Democracy Reporting International

EOMs usually focus on the pre-election/campaign period. However, when choosing what to monitor, EOMs would need to keep in mind groups or accounts that are known to spread disinformation on a continuous basis. In controversial elections, the post-election-day period may be critical, when results are tallied and published and when there may be intense public debates on the integrity of a particular election.

FIGURE 3

EOMs and other civil society monitoring periods



Source: Democracy Reporting International

Many civil society organizations monitor disinformation more permanently. EOMs need to connect to the information provided by these groups to understand the actor landscape and typical narratives that may have been promoted before election periods.

COOPERATION BETWEEN ACTORS AND INFORMATION EXCHANGE PARTNERSHIPS

One aspect highlighted during the interviews was the importance of cooperation. The connection between different actors in initiatives such as Debunk.eu allows them to quickly identify potential threats and share the information with volunteers and fact checkers to prevent items of disinformation gaining relevance. Compared to other countries, Lithuania has a highly connected ecosystem to fight disinformation.

When it comes to information exchange, a sharing agreement between the Digital Forensic Research Lab and Facebook allows improved action to foster election integrity. If the Digital Forensic Research Lab finds suspicious activity on Facebook, it flags it to the company for possible intervention. This is also the case for studies conducted by the Oxford Internet Institute. Their identification of bot networks helped Facebook to take them down.

These practices will be difficult for EOMs to adopt. Generally, EOMs do not interfere in the process, but only observe it. They avoid becoming part of the story and generally share findings only after election day. Interventions which call on platforms to take action may conflict with their non-intervention policy. Also, major EOMs are stand-alone operations, especially international EOMs. The EU and the OSCE avoid working with any specific national group, which could undermine their impartiality. Nevertheless, EOMs network intensively with domestic groups to gather information, and should expand this networking to groups dealing with and monitoring political discourse on social media.

DEALING WITH DATA

Social media monitoring entails the analysis of big amounts of data. Debunk.eu approached this challenge by training AI tools to identify content that was potentially spreading disinformation. The tool identifies articles that have a high likelihood of being disinformation, which are then verified by volunteers, who forward the most suspicious to media outlets. Journalists verify the claims and, if the story is false, write and publish a debunking story.

Risks associated with the use of AI tools by EOMs include the potential to oversee disinformation and hate speech content. Both can be subtle in different contexts, and identification can be more difficult considering the diversity of local languages. Also, the cost of AI can be significant, the length of EOMs is too short to train AI, and EOMs could be accused of having built bias into the algorithms.

Another option of dealing with the large amount of data is sampling, an approach used by Bakamo, Digital Democracy Room and others. However, it entails some risks such as bias in the choice of the sample and external validity.

WORKING IN DIFFERENT CONTEXTS

International EOMs typically work in widely different political and social contexts, which are reflected in the way that social media platforms are used. Organizations working in different countries, such as Digital Forensic Research Lab, Oxford Internet Institute and Democracy Reporting International can provide comparative insights on how to shape the analysis according to the context and the challenges of different languages, scripts and social media consumption.

Table 5 summarizes the challenges identified by the initiatives interviewed. It identifies the best practices adopted and insights on opportunities and risks for EOMs.

TABLE 5Challenges, best practices and risks & opportunities for EOMs

CHALLENGES Around Social Media Monitoring	BEST PRACTICES	OPPORTUNITIES FOR EOMS	RISKS FOR EOMS
Using findings to have immediate impact	Information exchange partnership with Facebook: Atlantic Council/Oxford Internet Institute	Partnerships with platforms may increase relevance of EOMs regarding access to data and impact of mission's findings	Actions taken by the platform during elections based on EOM findings would make observers part of the story, when their mandate is to observe only
Dealing with big amounts of data	Debunk.eu trained an Al algorithm that identifies potential false stories from several sources	Al tools can help cover more platforms and content in any given context saving time of observers in monitoring exercises	Al applications can be too costly and designing and training Al for each national context (including different languages) during a short time span is a challenge
	Bakamo applied a method to sample the data, drafting conclusions without covering the whole social media ecosystem	Sampling data can bring useful insights for EOMs monitoring efforts, reducing costs and time	Methodological biases linked to wrong sampling may harm the findings of EOMs
Data collection from Facebook (API restrictions and difficult to access publicly available data)	Use of Fact-a-lyzer by ISFED	The initiative to build a platform that looks specifically into electoral contexts is an innovation, considering the use of business intelligence tools that are not built for this purpose	The platform was tailor made based on ISFED's methodology and is not an easily adaptable solution for different contexts
Dealing with social media influence in different contexts	Digital Forensic Research Lab, Beacon Project, Oxford Internet Institute, Democracy Reporting International have experience in monitoring social media impact in different countries	Initiatives could offer comparable methodologies to identify the best approach to take in each context, and how these networks connect to each other	No risks associated
Good integration between different actors when it comes to fighting disinformation	Debunk.eu relies on partnerships to have a quick response to disinformation	EOMs may benefit from fostering connections between local actors that would help identifying trends related to disinformation and risks related to electoral processes	International EOMs usually do not enter partnership to avoid their impartiality being challenged
Guiding the monitoring effort based on existing legislation	ISFED monitored whether official political actors were complying with online campaigning rules in Georgia	It is clearer for EOMs to guide the monitoring exercise based on existing legislation, focusing the scope of the effort around more concrete issues such as political ads and standards for social media use around elections	The monitoring exercise may oversee questions that are not regulated and will hardly be subject to a clear regulation, such as disinformation. It also risks not looking at actors that hide behind fake pages

Best practices can be partially transferrable to EOMs. Exchanging the findings of previous research with social media platforms and other actors in a given context (media actors, civil society and governments) may help observers foresee what problems may arise during elections. Social media companies have different capacities in different countries, and only provide complete information through tools such as ad libraries in some of them. Knowing what tools are available and which actors are looking at social media helps to decide the best monitoring approach.

ISFED monitored how social media use for campaigns was contravening existing laws on online campaigning. While they found cases where candidates were misusing social media, such as instances of public servants campaigning via social media during working hours, many of the issues seen on social media have yet to be regulated (hate speech, disinformation, among others). Improved

regulation would help monitoring efforts focus on more specific questions.

Finally, there is clear demand for a tool that can help to collect and analyse data for political purposes. Most of the initiatives adapt tools made for marketing purposes on social media analysis during elections. Debunk.eu, Bakamo and ISFED are testing or developing their own approaches to solve this problem but are still far from reaching an ideal approach that is easily adaptable to different contexts.

SWOT ANALYSIS FOR EOMs IN SOCIAL MEDIA MONITORING

These best practices present risks and opportunities for EOMs. Many of them were pointed out by interviewees, as presented in Table 6.

TABLE 6

SWOT analysis of EOMs monitoring social media (based on interviews)

EOMS AND SOCIAL MEDIA MONITORING

Strengths Weaknesses

- Credibility derived from non-partisan status
- Unbiased perspective
- Know-how from election monitoring in different countries and periods (international EOMs)
- A degree of diplomatic protection (international governmental EOMs)

- Lack of training on how to monitor social media and digital content
- Limited knowledge of local context and connections to local digital 'ecosystem'
- Short timeframes to understand context
- Limitations to experimentation (governmental EOMs)

Opportunities Threats

- Increasing awareness of disinformation during elections increases EOMs relevance
- EOMs may open spaces for discussing and networking on social media in election issues
- Initiatives to monitor disinformation can make EOMs the target of disinformation actors that will try to undermine their credibility, attack their IT infrastructure, etc.
- Monitoring may be misinterpreted as data gathering on individuals

RECOMMENDATIONS

GOVERNMENTS:

- Encourage and fund experimentation by non-governmental organizations to further the development of methodologies and tools.
- Compare best practices across the EU.
- Foster networks to share lessons learned and take stock of new insights after elections.
- While governments/intelligence services sometimes issue warnings about disinformation, the absence of details/underlying data makes it difficult for NGOs and the wider public to assess them. Governments should substantiate these claims.

CIVIL SOCIETY:

- Increase cooperation, exchange of information and good practices in social media monitoring.
- More structured discussions by actors on methodologies, legal framework and ethics of social media monitoring.
- Increase and strengthen links between civil society groups and internet platforms so that the former can raise concerns in time and that findings are considered by platforms.
- Embrace experimentation.

EOMs:

- At a minimum, embed social media analysts in each EOM in order to understand and assess it with context and in detail (even if the EOM does not monitor social media). Social media analysts will make EOMs 'literate', i.e. able to connect and to understand the work and findings of groups monitoring social media and accusations raised by stakeholders on social media disinformation.
- International EOMs can expand methodology into areas that are more regulated and technically achievable. These could include the monitoring of paid ads (if made available by platforms) and costs (relating them to campaign expenditure provision); the monitoring of official pages of parties or candidates to track violations of electoral or wider rules (such as hate speech); and monitoring social media for violations of campaign silence provisions (where applicable).
- Explore the development of a credible methodology for social media monitoring by EOMs.
- While it is unrealistic for EOMs to comprehensively monitor all social media discourse during elections (given the size, dynamism and complexity of the material), criteria to determine the observation may include regulation, i.e. observers focussing on areas that are more regulated than others (such as campaign financing rules, violation of platform policies, breaking electoral silence).

- To ensure impartiality, research should be designed in a nonpartisan manner. It should not focus immediately on one part of the political spectrum but try to ascertain how all the relevant sides act on social media.
- Conclusions should be drafted in light of the capacity and approach of the mission, clarifying the scope, methodology and decisions that guided the analysis. Transparency is central to ensure that the conclusions are credible and replicable.
- Include a technical working group on social media monitoring in future meetings of the 'Declaration of Principles Group'.
- Address recommendations to tech companies too.
- Establish a set of ethical, legal and reputational guidelines for the work of social media analysts in EOMs.

ANNEX 1: SURVEY OF INTERNATIONAL ELECTION OBSERVATION ORGANIZATIONS

	EU	OSCE/ODIHR	NATIONAL DEMOCRATIC INSTITUTE
Do you consider digital content/ social media relevant for electoral integrity?	Yes	Yes. Social networks and online media an important avenue for the conduct of election campaigns. Potential to broaden participation, but needs to respect civil and political rights	Yes. Manipulation can amplify voter confusion, dampening participation, galvanise social cleavages, (dis) advantage certain parties and candidates, and degrade trust in institutions
Should internal observers get involved?	Yes	Yes, but with a significant level of care (sound methodology)	Yes
Have you published documents on this?	 EU observer handbook chapter on digital content EODS/DRI Study "New Frontier" 	Not on social media (but on cybersecurity)	 Internal guidance document updates under D4D coalition
Have you started focussing on this in EOMs?	 Digital analyst in Nigeria EOM Planned EODS conference and training 	EOMs conduct qualitative monitoring of social media content and online media content (qualitative/ quantitative)	Yes. Kenya, Georgia and now Ukraine
What are your plans on this?	Develop methodology and build positions into EOMs	Consolidate methodology on observation of election campaigns, which will include the aspect of online campaigning	-

COMMONWEALTH	CARTER CENTER	ELECTORAL INSTITUTE SUSTAINABLE SOUTH AFRICA (EISA)	OAS	UN (DOESN'T USUALLY OBSERVE ELECTIONS)
Yes. We note it in particular for communication of election management bodies and other stakeholders (like parties) with the electorate	Yes, (dis-) information environment very relevant	Yes	Yes, but it depends on many factors including access to internet	Yes, it has changed how campaigns are conducted, how election management communicates, etc.
Yes, but methodology, consistency and transparency of doing it remain unclear	Yes	Yes	Yes	Yes, but many challenges: short duration of missions, limited resources, etc.
2016 report 'New Media in Elections' aimed at EMBs specifically	Not yet.	No	No	No
Not systematically	Not in big missions but in small teams in Zimbabwe and DRC	We follow election management bodies conduct in social media	Yes, but not yet in a systematic manner. In a preliminary manner in Mexico and Brazil 2018	No, the UN does not usually deploy EOMs. We decide in case we are tasked with one
Nothing specific. Requires broader institutional consideration/discussion	Experimentation and development of policy on this	We plan to expand and develop a methodology	We will work with the OAS special rapporteur on freedom of expression	No

ANNEX 2: BRIEF DESCRIPTION OF THE INITIATIVES ANALYSED (based on interviews)

A. NON-GOVERNMENTAL INITIATIVES

EUROPE:

Organization: Stiftung Neue Verantwortung (SNV) Country: Germany

Stiftung Neue Verantwortung is a German independent think tank that researches disinformation, among other issues. In 2017, it developed a study to identify how ten disinformation stories were shared and amplified in the threemonth runup to the German federal election. The stories were spotted by factchecking organizations in Germany, and the researchers used the platform Talkwalker, a web crawler, to scour the entire German language web - including Twitter and Facebook public pages and posts - to map who spread the stories, the most important amplifiers and the number of disinformation and debunking pieces. They were able to access Talkwalker through a partnership with the company Unicepta. It relied on URL and keyword searches, and student interns helped to code and clean the dataset. The research concluded that disinformation was an important political mobilisation strategy for the AfD and rightwing populists during that campaign. The organization had funding and plans to replicate the same methodology in the run-up to state elections in Bavaria and Hessen in 2018, but gave up after Facebook restricted the ability of Talkwalker and other similar tools to access its data via API. Stiftung

Neue Verantwortung says that Facebook was the main dataset due to the number of active users in Germany, and could not be left out of any new studies.

Organization: Debunk.eu Country: Lithuania

Debunk.eu is an initiative in Lithuania that aims to identify new disinformation articles within two minutes of their publication, relying on AI and partnerships with volunteers and media outlets. The tool currently analyses 20,000 articles per day, from more than 1,000 domains, and automatically assesses the probability that a new article is disinformation, considering variables such as keywords, social interactions and publications in multiple domains. The 2% of articles with the greatest likelihood of being disinformation are analysed by volunteers (known as "Lithuanian Elves"), who then forward the most suspicious to media outlets. Journalists verify the claims and, if the story is deemed false, write and publish a debunk. The initiative has partnerships with media companies that reach 90% of the Lithuanian population. In 2019, it plans to expand the range of the tool to 200,000 articles per day and use speech-to-text technology to analyse TV programmes and video on demand. Debunk.eu has tuned its algorithm and partnerships towards the next presidential election in Lithuania, in May 2019, which will include a daily

report sent to journalists with problematic stories and an early warning system. The organization also intends to scale its technology to 35 languages and other countries in the future. It is funded by Delfi, a major media company in the Baltic region, and Google Digital News Initiative.

Organization: Prague Security Studies Institute Country: Czech Republic

The Prague Security Studies Institute has monitored and published reports on disinformation narratives spread during the last three Czech elections — the parliamentary election in 2017 and Senate and Presidential elections in 2018. It has applied the same methodology in 2019 on the runup to the European Parliament elections. Its monitoring usually begins four to five weeks before election day and focuses on six to seven Czech websites that are known to be hubs for spreading disinformation, including their Facebook pages. To do this, it relies on the platform Versus, a web crawler developed by the Beacon Project (International Republican Institute) and offered at no cost to their partner organizations. The platform allows it to monitor Czech sources and sort articles and public posts on Facebook and Twitter. Manual coders analyse the content according to variables such as type of message, sentiment towards the candidate and number of shares in social media. During the monitoring, it produces weekly summaries and send them to journalists, state authorities and political parties, and activates an early warning system that informs candidates and journalists when a piece of disinformation has the potential to spread. It treats disinformation spread by domestic actors or foreign powers in the same way.

Organization: Kremlin Watch / European Values Think-Tank Country: Czech Republic

Kremlin Watch, a programme of the European Values Think-Tank, monitors disinformation narratives spread in the Czech Republic that support Russian interests. To do so, they manually analyse articles published by around 40 websites and their Facebook pages in the Czech language that are known to spread

disinformation and have a relevant readership. Some of the disinformation stories are debunked and the results are published in their website, in a newsletter and on their social media accounts, and sent to the East StratCom Task Force. Kremlin Watch has developed initiatives to identify disinformation campaigns during the run-up to the Czech legislative elections in October 2017 and the presidential election in January 2018. It also tracks disinformation during non-electoral periods, when the organization develops a systematic approach to identify its origins, the dynamics of its spread and the main narratives. The European Values Think-Tank produces and publishes studies on the topic, including an annual report about how the EU28 countries try to address Russia-led disinformation. It is considering adding countries from the Eastern Partnership and Western Balkans to future editions of that report.

Organization: Computational Propaganda Project / Oxford Internet Institute Country: UK

The Computational Propaganda Project at the Oxford Internet Institute investigates the interaction of algorithms, automation and politics, including disinformation campaigns and social media bots. One of its methods is to use software built inhouse to scrape vast amounts of public posts on Twitter and Facebook, look into which URLs were shared and classify them with the help of human coders familiar with the political context of the monitored country, aiming to measure how much "junk news" is being spread. It also has a Junk News Aggregator that tracks misleading, deceptive or incorrect information gaining traction on Facebook. Beyond monitoring initiatives, the organisztion also publishes papers about policy and regulation related to the issue.

Organization: EU Disinfolab Country: Belgium

EU Disinfolab is a Brussels-based NGO whose goal is to facilitate collaboration among stakeholders involved in fighting disinformation. In 2018 it published two studies that applied social network analysis to Twitter posts to investigate the spread of disinformation and echo chambers during the Italian

2018 election, and the hyperactivity surrounding the Benalla case in France. The open source software Gephi was used to map and cluster posts and human experts for semantic and qualitative analysis. Monitoring of the Italian elections study began three months before election day and initially focused on Kremlin-related Twitter accounts, but the organization claims that it is not particularly focused on Russian-led disinformation. EU Disinfolab is a partner of WeVerify, an initiative launched in December 2018 that aims to develop an algorithm-supported verification platform for digital content, with funding from the EU's Horizon program until November 2021.

Organization: Ukrainian Election Task Force / Atlantic Council Country: Ukraine

The task force was created to monitor the run-up to the March 2019 Ukrainian presidential election in three fields: kinetic operations, cyberattacks and disinformation. It is supported by the Atlantic Council, Victor Pinchuk Foundation and Transatlantic Commission on Election Integrity. It focuses on identifying and highlighting disinformation narratives spread mostly by the Russian state media via social media. The Task Force does not aim to inform Ukrainians, nor to spot domestic disinformation, but to identify foreign meddling in Ukrainian elections and to highlight it to Western audiences. It has partnered with two Ukrainian organizations, StopFake and Detektor Media, to look for narratives. A Czech company, Semantic Visions, looked for mentions of Ukrainian presidential candidates on over 24,000 digital sources with the .ru domain.

Organization: International Society for Fair Elections and Democracy (ISFED) Country: Georgia

ISFED came up with a methodology to track Facebook during the 2018 Georgian elections and experimented, in partnership with the National Democratic Institute, with the use of the platform Fact-a-lyzer, which collects Facebook data to monitor selected pages in a user-friendly interface. ISFED monitored social media to look for three things:

- Violations of electoral law
- Discrediting campaigns against candidates, parties and the electoral process
- Disinformation, divisive and illiberal narratives.

The first and second categories focused on public officials and national actors, while the third was associated with Russian narratives spread both by foreign and domestic actors. The findings of electoral law breaches helped to prevent abuses by public officials and public organizations during the electoral period. The other categories documented the narratives being discussed during the elections (namely anti-western propaganda, anti-NATO messages and xenophobia/homophobia), an area that they are willing to look into in the future with the help of manual coding. Apart from traditional API concerns, other challenges related to the dynamic environment of social media analysis during elections emerged: as voting day approaches, new pages are created and the intensity of content shared increases, making it more difficult to track such trends around election day. Lack of data, time and structure prevented a more comprehensive analysis.

Organization: Bakamo.Social Country: UK

Bakamo is a consultancy that maps how information spreads in social media and identifies thematic or emotional patterns linked to a specific content. It uses the tool TalkWalker to scrap large amounts of public posts from social media, such as Twitter, and then uses human analysts to clean the dataset and classify and interpret the narratives. The consultancy reported on patterns of disinformation during the 2017 French elections, funded by Open Society Foundation. It concluded that one in five links was shared from sources that contested the legitimacy of traditional media, and that Russian influence emerged as a distinct category in that disruptive narrative. Bakamo has also published a study on migration narratives in EU28 member countries for a German party foundation, and a report on the impact of disinformation campaigns on political radicalisation.

OUTSIDE EUROPE:

Organization: Beacon Project / International Republican Institute Country: U.S.

Beacon Project was created by the International Republican Institute in 2015 to help to organise a pan-European response to hostile influences, in particular disinformation. Initially it focused on activities emanating from Russia, but expanded to include threats to democratic governance at large, whether from domestic or foreign sources, in countries formerly under the influence of the Soviet Union. To do so, Beacon Project helps organizations to monitor their local media more efficiently. It has developed a web crawler, called Versus, and offers the platform for free to partner organizations. Versus scrapes pre-defined sources within a given media space in a country - mainly media outlets - but also Facebook public pages and Twitter accounts. Analysts and human coders use it to filter, sort and tag the content, looking for hostile narratives. In 2018, the initiative coordinated a media monitoring project in the Visegrad Four countries, in partnership with the following organizations: Prague Security Studies Institute (Czech Republic), Political Capital Institute and Center for Euro-Atlantic Integration (Hungary), Globsec (Slovakia) and Center for Propaganda and Disinformation Research (Poland). Beacon Project is not necessarily focused on elections, but its projects may overlap with them. It has a team of five staff (three in Brussels, one in Riga and one in Belgrade) and a programme director split between Brussels and Bratislava. Versus is being adapted to scrape media in other languages, such as Latvian, Lithuanian, Russian, Serbian, Bosnian and Macedonian.

Organization: Hamilton 68 Dashboard / Alliance for Securing Democracy Country: U.S.

Hamilton 68 is an online dashboard developed by the Alliance for Securing Democracy, housed at The German Marshall Fund of the United States, to help to spot information manipulation led by Russia. Version 1.0 of the dashboard was released in August 2017 and closed in December 2018. It monitored 600 Twitter accounts allegedly openly or covertly linked to Russian influence, and distilled the top ten most popular hashtags, URLs, domains, keywords and trends, among roughly 200,000 tweets a day. The list of monitored Twitter accounts was not disclosed. Occasionally, it published expert analysis adding context to the raw data. Version 2.0 is expected to launch in 2019 and will only monitor Twitter accounts openly connected to Russia, such as diplomatic officers, government-funded media and its main editors and commentators. Among other reasons, the update was designed to improve understanding of the methodology and to avoid misinterpretations of results. Technology is developed by Graphika, a social media monitoring firm. The dashboard is not focused on elections, but captures elections-related trends. Alliance for Securing Democracy is considering expanding its scope to monitor China- and Iran-linked accounts.

Organization: Digital Forensic Research Lab / Atlantic Council

Country: Based in U.S., employees in several countries

The Digital Forensic Research Lab is an initiative from the Atlantic Council whose mission is to expose and explain falsehood online, such as false narratives and false accounts, and to identify its sources and amplifiers. It has a team of 15 people with diverse professional backgrounds and based in different countries. It also develops projects and partnerships focused on elections. It helped to identify accounts involved in spreading disinformation about Emmanuel Macron in 2017 in France. In Germany it partnered with Bild and found a network of Russian Twitter bots amplifying AfD messages. It also worked on the Mexican and Brazilian presidential elections in 2018. This year, Digital Forensic Research Lab will look at the European Parliament elections and those in India and South Africa. The organization relies on different technological tools, such as Sysomos, CrowdTangle, BuzzSumo and Twitonomy. In 2018, it established an information sharing partnership with Facebook which was mainly focused on election integrity. If the organization finds suspicious activity, it shares it with Facebook. In exchange, Facebook offers sanity checks of their findings and details to enhance Digital Forensic Research Lab analysis, but does not grant it access to confidential data.

Organization: Center for Democracy and Development West Africa & University of Birmingham

Countries: Nigeria & UK

This consortium formed by CDD and the University of Birmingham was granted funding from WhatsApp to carry out a project analysing the impact of the platform on the upcoming elections in Nigeria. The monitoring will be in two states to balance regional representation and will focus on how key stakeholders - political parties, electoral officials, civil society, local leaders - are using social media and WhatsApp. Because of encryption and the difficulty in collecting data, data will be collected via surveys and focus groups, particularly among young people, and to educate citizens about the characteristics of disinformation. One component will show users stories circulating during elections and ask them if they think they are true or not, and what they did about it. The project will produce articles and policy briefs to document the impacts of WhatsApp during elections and to establish partnerships to see how academia and civil society can help governments reduce the potential threat posed by these platforms in West Africa.

Organization: Getúlio Vargas Foundation (Digital Democracy Room)

Country: Brazil

Digital Democracy Room was initiated after the political debate on social media in Brazil had become increasingly polarised. Hate speech and disinformation accelerated division and radicalisation, which became a central aspect of the 2018 elections. DDR tracked data from different platforms - Twitter, Facebook, YouTube - to analyse bot activity and the influence of international actors. Their Twitter analysis was facilitated by the ease of API access. Facebook's data restrictions limited the research but allowed some analysis.

WhatsApp became a major influence on the electoral process in Brazil. The private messaging app is very popular in the country, and action taken by Facebook and Twitter to fight disinformation networks on their platforms encouraged them to shift to the encrypted

platform. Since the researchers did not have the necessary data to analyse WhatsApp, they picked up stories shared on the platform as they spilled over to other social networks (Facebook and Twitter), trying to understand the role of the private messaging app in disinformation campaigns.

Organization: Truepic Country: U.S.

Truepic is a U.S. company that offers image and video certification and aims to be the world's first digital photo notary. Their app offers two services: it takes photos and record videos that are self-authenticating and may be used for legal or evidential purposes, and it is able to identify if a picture taken by a third party was manipulated. Truepic has done a small experiment during the US midterm elections and is planning to offer its technology for wider use during the 2020 presidential election. The company is considering offering its technology at no or little cost in areas where it can have a social impact, such as election observation missions that need to document voting procedures and campaign events.

B. GOVERNMENTAL/ INTER-GOVERNMENTAL INITIATIVES

Organization: NATO StratCom Center of Excellence Country: Based in Latvia

The NATO StratCom Center of Excellence is a research centre that focuses on communication-related issues. It does not have operational capacity to act in NATO operations or exercises, but may contribute expert opinion to them. The centre publishes a quarterly study entitled "Robotrolling Report" about automation on Twitter and VKontakte. It scrapes vast amounts of public posts from these two platforms which refer to NATO, the Baltics or Poland, using a list of terms and a system built in-house. It then uses coders and machine learning to identify the percentage of automated posts. Two years ago, it found that 70% of the conversations in

Russian were automated, while today it is at around 20%. The centre says that the problem has not gone away but has shifted from simple automation to anonymous accounts controlled by humans. It has also published a report about the black market for social media manipulation, such as likes or followers, and in 2019 will publish a report on how governments should structure protection mechanisms against disinformation. It has also experimented with image classification on Instagram and Facebook and has an established dialogue with social media companies.

Organization: Ministry of Foreign Affairs (MFA) Country: Germany

The German MFA work on disinformation is broader and does not focus on elections, instead tackling narratives related to foreign relations. One example is the #rumours about Germany site, which aims to tackle disinformation about refugees and migrants. It is also experimenting with social media listening platforms such as Talkwalker to understand the perception of Germany abroad, and considers disinformation to be one aspect of a broader discussion of hybrid threats fostered by state and non-state actors. The aim is to spread positive narratives rather than directly countering or debunking misinformation. In terms of international cooperation, the MFA is supporting the implementation of the EU Action Plan against Disinformation and working with G7 countries on the issue. It is interested in looking more broadly at hybrid threats and social media monitoring over the next few years.

Organization: East StratCom Task Force Intergovernmental organization: EU

The East Stratcom Task Force was set up in 2015 by the European Council to address Russia's ongoing disinformation campaign. It does so by gathering disinformation narratives, exposing the trends and methods behind them, and publishing the findings on the EUvsDisinfo.eu website. A newsletter and

social media accounts aim to raise awareness about the issue. Disinformation messages are tagged and included in a database that currently contains around 4,700 pieces of disinformation published in 18 different languages. The Task Force had few resources in its first three years, but recently benefited from the EU's increasing commitment to tackle disinformation. In 2018-2019 it was assigned its first budget of €1.1m with support from the European Parliament. This was increased to €3m in 2019-2020. The Task Force now has an overall staff of 16 people, of whom six focus on disinformation while the others work on proactive communications, media support and Russian language outreach. The team will hire two new employees in the spring of 2019. Since January 2019 it has contracted out professional media monitoring services, disinformation and data analysis expertise. The Task Force will receive information and feed into an EU Rapid Alert System to inform countries quickly of new disinformation stories, as outlined in the EU Action Plan on Disinformation.

Organization: Swedish Defence Research Agency Country: Sweden

The Swedish Defence Research Agency (FOI) is a governmental agency which is part of the Ministry of Defence. In 2018, it was commissioned by the Swedish Civil Contingencies Agency (MSB) to produce two studies on monitoring social media and digital content. One analysed the behaviour of Twitter bots and mapped possible influence operations. The other monitored online commentary and discussion boards on Swedish websites to look for posts that conveyed threats to the Swedish elections, such as attacks on polling stations. Data scientists developed an in-house web crawler to scrape the data, created two dictionaries of words possibly related to threats, filtered material with those terms and submitted it to human coders to delete false positives. In the process they identified rumours and complaints about the election, but no credible threats.