Digital Democracy Risk Assessment:

Background Paper

DEMOCRACY
REPORTING
INTERNATIONAL

Digital Democracy Risk Assessment:

Background Paper

2020

Funded by:

civitates
a philanthropic initiative for democracy and solidarity in europe

With contributions by:

MEMO98

This publication is a result of a project carried out by Democracy Reporting International with contributions from MEMO 98 and the financial support of NEF-Civitates. The contents of this publication do not reflect the position of NEF-Civitates. This publication was developed by the DRI Social Media & Democracy Team, with contributions from Jon Vrushi.

July 2020

Author: **Helena Schwertheim**

Contents

Section 1: Introduction

Democracy is becoming increasingly digital. The rise of the internet and social media has enabled those who wish to exploit the fissures of modern democracy to undermine elections and democratic discourse. The speed, scope and scalability of how information travels on social media differentiate from how traditional media works, allowing these new technologies to be exploited for undemocratic purposes.[1] Political parties and candidates, governments, campaign consultants, foreign actors have weaponized social media to spread disinformation, incite hate and violence, and meddle in elections.[2]

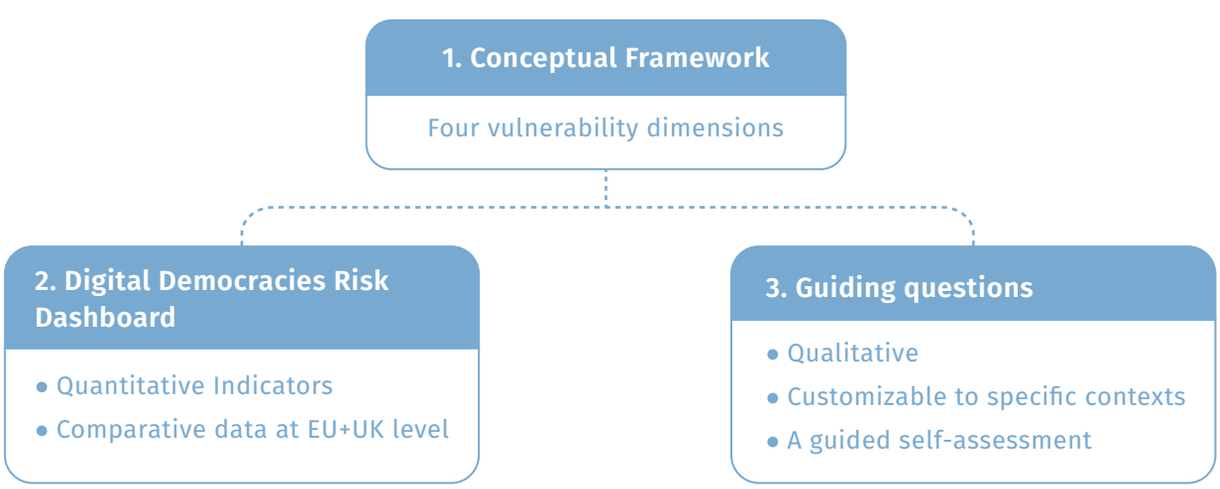
As more citizens, political debates and democratic processes move online, we require a better understanding of the new challenges and opportunities this poses to democracy. Fact-checking, social media monitoring and investigative journalism are developing our understanding of the threats to elections and democratic debate. At the same time, we need to expand our knowledge of the vulnerabilities and weaknesses that this new digital age poses to our democratic systems. However, the threats will keep evolving in parallel to technological changes. Understanding vulnerabilities in the democratic system allows safeguarding and resilience building in the long term. Knowledge is the first step to building resilience.

The Digital Democracy Risk Assessment is a tool for civil society organisations and other researchers to assess a country's vulnerabilities to online manipulation around elections. The Assessment's approach is to focus on the vulnerabilities. It does not assist users to establish the existence of adversarial manipulation campaigns, networks, or their impact. Instead, it helps users to map vulnerabilities of a country's election ahead of the event.
This Background Paper provides the theoretical basis and evidence basis on which the Framework the Digital Democracies Risk Assessment is built.

The Digital Democracy Risk Assessment is based on:
1. The **Conceptual Framework** outlining vulnerability dimensions
2. The **online Digital Democracy Risk Dashboard** which provides relevant data on 27 EU member states (and the UK)
3. Guiding Questions for a qualitative assessment to contextualise and customise assessments, found in the User Guide.

All these resources can be found on the Risk Observatory website:
https://digitalmonitor.democracy-reporting.org/risk-observatory

Digital Democracies Risk Assessment



1 Guide for civil society on monitoring social media during elections, 2019, https://democracy-reporting.org/wp-content/uploads/2019/10/social-media-DEF.pdf
2 Kofi Annan Foundation, 2020, pg 25 Protecting electoral integrity in the digital age, https://www.kofiannanfoundation.org/app/uploads/2020/01/f035dd8e-kaf_kacedda_report_2019_web.pdf

Section 2: How online manipulation affects electoral integrity

Online manipulation campaigns are generally designed to create network-specific effects, targeted at particular electorates (geographically: specific electoral districts/sociologically or psychologically: specific groups of people) rather than the entire population. Short-term political online manipulation cannot swing massive parts of the population, but it can aim at smaller changes, for example in specific swing constituencies (convince voters to stay home or to vote for a specific party or candidate). Beyond such specific objectives it can aim at diminishing trust in democracy and elections and long-term political polarisation[3]. In sum, online manipulation campaigns are often designed to erode electoral integrity. For this reason, the Digital Democracy Risk Assessment focuses on establishing the vulnerabilities a country's electoral integrity may face.

Key concepts

Electoral integrity

"An election with integrity as any election that is based on the democratic principles of universal suffrage and political equality as reflected in international standards and agreements, and is professional, impartial, and transparent in its preparation and administration throughout the electoral cycle". [5]

Electoral integrity also depends on citizens' confidence in electoral and political processes.

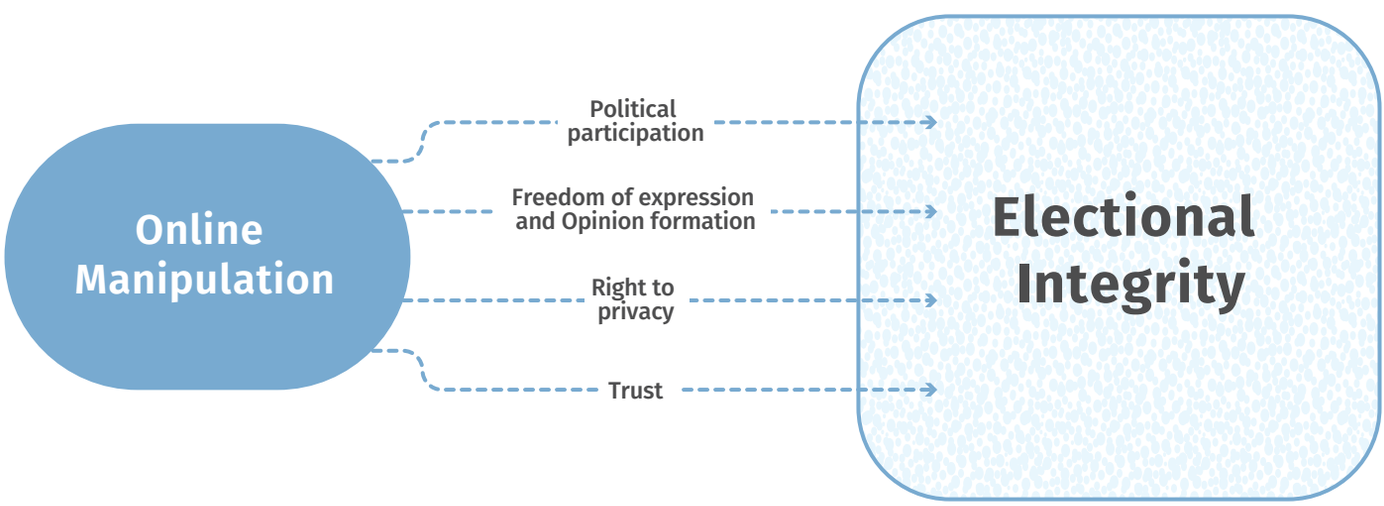
Public discourse and debate around elections is an essential part of any electoral process.[6]

Online manipulation [4]

"The use of social media for the purpose of manipulation or interfering in elections – misleading information about how to participate, voter suppression and intimidation, and false or misleading affiliation".

As technology develops, so will new techniques and strategies by adversaries.

We see four entry points through which electoral integrity can be affected by online manipulation. Specifically, through political participation, freedom of expression and opinion formation, privacy, and political trust.



3. Howard, 2020, Lie Machines, Yale University Press
4. Cyberattacks and other forms of digital interference is also a way to interfere in elections. The Digital Democracy Risk Assessment focuses on vulnerabilities concerned with social media and does not cover vulnerabilities related to cyberattacks and digital infrastructure variables.
5. International IDEA and the Kofi Annan Foundation, 2012, pg 6, Deepening Democracy, https://www.idea.int/publications/catalogue/deepening-democracy-strategy-improving-integrity-elections-worldwide
6. Meyer-Resende, 2018, A New Frontier: Social Media / Networks, Disinformation and Public International Law in the Context of Election Observation, pg. 6, https://democracy-reporting.org/wp-content/uploads/2018/10/A-new-frontier_social-media_election-observation_Briefing-Paper-by-Michael-Meyer-Resende.pdf

International law enshrines the right to political participation, privacy, and protects free communication as cornerstones of any democracy. The right to political participation (Article 25 of the International Covenant on Civil and Political Rights (ICCPR) [7]) requires, inter alia, freedom of expression, but also focuses on how opinions are formed (and not only how they are expressed). [8]

In the words of the UN Human Rights Committee which monitors the implementation of the ICCPR: "The free communication of information and ideas about public and political issues between citizens, candidates and elected representatives is essential. This implies a free press and other media able to comment on public issues without censorship or restraint and to inform public opinion. The public also has a corresponding right to receive media output"[9] The right to privacy is enshrined in Article 17 of the ICCPR.[10] As the Digital Democracy Monitor explores, false or misleading information, hate speech, political advertisements and false amplification methods are misinformation strategies that can influence political discourse during, before, and after election periods, through these entry points of political participation, freedom of expression and opinion formation, privacy, and political trust.

Political trust (citizen trust in government) is a key element of electoral integrity, and it is essential for governability. Political distrust weakens beliefs in mutual security, and once they begin to erode, organized online disinformation, and hate speech will likely have more success in electoral environments. Undermining public trust in government is often an objective of disinformation campaigns, often through the polarization of society.

Of specific interest are these points:

• **False or misleading information** can harm electoral integrity in various ways[11]. At the deepest level, disinformation can impact political participation fundamentally by influencing worldviews, political beliefs, or ideologies. For example, long-term attacks on the credibility of journalists can result in cynicism and distrust in a professional community that provides essential information for a fact-based democratic discourse. Disinformation can also impact electoral choice or actions; misinformed voters may choose a candidate who does not actually meet their preferences. In this way, disinformation can remove accountability form elections[12]. Lastly, disinformation can influence electoral behaviour by providing misleading information on election day, e.g. sending voters to the wrong polling station, or posting fake images of security checks which may deter marginalised groups from voting.

• Although **hate speech** does not have a universal definition, it can be understood as messages with the purpose of attacking a person or a group on the basis of attributes such as race, religion, ethnic origin, sexual orientation, disability, or gender. Hate speech online can be used to disengage certain groups from going to vote or participate in elections (voter suppression). Most forms of hate speech are considered as illegal content in many jurisdictions.

• **Paid advertising** is the basis of most platforms business models. It has various forms (paid ads, boosting posts, etc.). It can be used to amplify, and microtarget messages that can endanger democratic discourse and electoral integrity[13],

---

7 "Every citizen shall have the right and the opportunity, without any of the distinctions mentioned in article 2 and without unreasonable restrictions: (a) To take part in the conduct of public affairs,directly or through freely chosen representatives; (6) To vote and to be elected at genuine periodic elections which shall be by universal and equal suffrage and shall be held by secret ballot, guaranteeing the free ex pression of the will of the electors; (c) To have access, on general terms of equality,to public service in his country."

8 See General Comment 25 of the ICCPR: "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"

9 General Comment 34 on Article 19, point 13

10 Article 17 of the ICCPR notes that "no one shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor to unlawful attacks on his or her honour and reputation". It further states that "everyone has the right to the protection of the law against such interference or attacks."

11 For further detail, see: Meyer-Resende and Goldzweig, 2019, Online threats to democratic debate: A framework for a discussion on challenges and responses, https://democracy-reporting.org/wp-content/uploads/2019/06/BP_Threats-to-digital-democracy.pdf

12 Kofi Annan Foundation, 2020, pg. 55, Protecting electoral integrity in the digital age, https://www.kofiannanfoundation.org/app/uploads/2020/01/f035dd8e-kaf_kacedda_report_2019_web.pdf

13 Blöbaum, Trust and Journalism in a Digital Environment, 2014, pg 21, https://reutersinstitute.politics.ox.ac.uk/our-research/trust-and-journalism-digital-environment

especially if there is no transparency and no rules on campaign financing. Paid ads have been used for example to send highly polarising messages to votes from inauthentic accounts. The lack of regulation of online political advertising allows distinct and selected messages to be sent to different audiences without transparency – often audiences based on demographics, interests, geography and other political variables, and creating internet echo chambers and allowing domestic and foreign actors to push polarising and misleading messages to voters. The hidden nature of online, highly targeted campaigning diminishes the opportunity for public scrutiny and increases the potential for echo chambers, entrenching polarised political views, and provides undue advantage to those who have access to this data.

• **Artificial manipulative behaviour/actors** (including coordinated inauthentic behaviour and bots) use automation to scale the spread of misleading or intimidating content. Every platform, for their unique characteristics, have different ways in which this manipulation can occur. Also, the objectives of this manipulation are not always political, they may have economic motivations but political consequences (for example invented sensationalist political stories to drive traffic to spam websites).

A genuine democratic election with integrity requires that candidates and political parties can communicate their messages freely, and that voters receive diverse information that they can discuss freely to make an informed electoral choice. We therefore assume that online interference has an impact on electoral integrity, through undermining public trust, freedom of expression and freedom to be able to form opinions (democratic discourse).

Section 3: Enabling factors that exacerbate the effects of online interference on electoral integrity

This section unpacks what is understood as key vulnerability factors of electoral integrity in the digital age. These can be divided into four dimensions: State, Politics, Media and Society.

Digital Democracy risk assesment conceptual framework

Vulnerability dimensions

State

- Rule of law
- Electoral administration
- Content regulation
- Electoral system
- Trust in government

Politics

- Civility and Political use of social media
- Tightness of political race
- Trust in political parties
- Political finance transparency
- Emotive politics
- Foreign interference

Media

- Media plurality, freedom and fractionalisation
- Consumption
- Connectivity
- Trust in media
- Trust in government
- Technology companies' response

Society

- Societal polarisation
- Education
- Public perception of misinformation as a problem
- Perceived resilience to misinformation
- Citizen media literacy

State

In this section:

- Rule of law
- Electoral administration
- Content regulation
- Electoral system
- Trust in government

1

Rule of law

The rule of law means that people live under a clear framework of applicable and enforced laws, but it goes beyond the fact that laws are in place and followed. The rule of law also means that all laws are introduced following a democratic process and respect human rights.[15] This includes electoral laws, and broader concepts such as access to justice to citizens, the quality of the investigative criminal system, and predictable enforcement of (any) laws. In environments with low levels of rule of law, state may act with greater impunity regardless of the actual regulation, and hence greater levels of risk to electoral integrity can be expected.

Electoral administration

Conducting an election is a huge logistical challenge which involves the complex management of people, technology and resources.[16] Electoral management bodies (EMBs) are the state organisations that are tasked with the administration of elections. They require both the capacity (funding, staff and knowledge) and independence (from the government and political parties) to perform its tasks effectively, and to be perceived by the public to be doing its job well. Doubt in professional, impartial behaviour by EMBs can question the legitimacy and accuracy of the entire election. Disinformation can harm electoral integrity by undermining trust in free and fair electoral procedures themselves, by creating rumours over the administration of the election and question the legitimacy and accuracy of an election.[17]

Content regulation

Regulation of platforms content and hate speech: The technology offered by social media platforms allows precise targeting of groups and individuals. Bad actors can exploit ideological and cultural divisions, raising questions over hate speech, discrimination, and the impact on democratic discourse and electoral integrity more broadly. A well-known example is the Russian attempts to influence the 2016 U.S. presidential elections by targeting African-American voters. [18]

Broader forms of government regulation on content are a sensitive topic, given its potential to violate freedom of expression. However, at both the EU level and in several country states, legislation exists that aims to curb illegal content online. In Germany, the 2017 Network Enforcement Law (NetzDG) introduces possible imposition of fines on social networks if manifestly illegal content is not taken down within 24 hours. France passed a similar regulation in 2020[19], and the EU is set to release a regulatory package (the Digital Services Act) in 2021 which may contain notice-and-action rules for illegal content[20]. Free speech advocates criticise that such laws- can give rise to "copycat" legislation in countries with weaker institutions could be misused and abused. For example, countries such as Russia, Venezuela, The Gambia and Egypt have similar-sounding legislation, though the details differ. For the risk assessment a real world understanding of legislation is essential.

15 See DRI's primer "Components of the rule of law in the European Union", 2019, https://democracy-reporting.org/wp-content/uploads/2019/09/Rule-of-Law_A-Primer.pdf
16 James et al., 2016, Council of Europe, https://www.venice.coe.int/files/13EMB/13EMB_Toby_James_Leontine_Loeber.pdf
17 James et al 2016, Council of Europe, https://www.venice.coe.int/files/13EMB/13EMB_Toby_James_Leontine_Loeber.pdf
18 Shane and Frenkel, "Russian 2016 Influence Operation Targeted African-Americans on Social Media."
19 https://www.reuters.com/article/us-france-tech-regulation/france-to-force-web-giants-to-delete-some-content-within-the-hour-idUSKBN22P2JU
20 https://www.europarl.europa.eu/legislative-train/theme-a-europe-fit-for-the-digital-age/file-digital-services-act

Electoral system

Disinformation has the potential for greater impact in "first-past-the-post" majoritarian elections, where disinformation actors can focus on narrow swing constituencies to influence the results and allocation of seats.[21] For example, in the UK a parliament may depend on only a few single-member districts, which disinformation actors can focus on and target users in these districts. Due to the college system, US presidential elections are usually decided in only a few swing states. If they are tight in any swing states, targeting small parts of the electorate can have an impact on the nation-wide result of who becomes the President. Such strategies do not work easily in proportional electoral systems with large electoral districts. Hence, countries with majoritarian electoral systems can be assumed to be more open to online manipulation.

Trust in government

Citizen trust in government is essential for social cohesion and is essential for governability. Undermining trust in government institutions (government and political parties) is often a core objective of disinformation campaigns and online interference, seen in strategies that aim to polarize society. Members of government are frequently the targets of online disinformation, and in low-trust environments political actors often seem to fuel polarized debates by attacking political enemies[22]. Conversely, studies by Newman et al[23] and Tsfati and Cappella[24] show that in high-trust countries online disinformation is generally published by anonymous sources or alternative websites – not by other political actors. Therefore, public trust in government is often in the cross-hairs of adversaries. Needless to say, lacking trust in government may be justified in authoritarian or corrupt regimes.

21 Reilly, 2001, Democracy in Divided Societies: Electoral Engineering for Conflict Management (Cambridge: Cambridge University Press); Drutman, 2017, "The Case for Proportional Voting," National Affairs 34: 50-63.

22 Humprecht, 2019, "Where 'Fake News' Flourishes: A Comparison Across Four Western Democracies," Information, Communication, and Society 22, no. 13: 1973–88.

23 Newman, Fletcher, Kalogeropoulos, Levy, and Nielsen, 2017, Reuters Institute Digital News Report 2017, https://reutersinstitute.politics.ox.ac.uk/sites/default/files/Digital%20News%20Report%202017%20web_0.pdf

24 Tsfati and Cappella, 2003, "Do people watch what they do not trust? Exploring the association between news media skepticism and exposure". Communication Research, 30(5), 504–529.

Politics

In this section:

- Civility and Political use of social media
- Tightness of political race
- Trust in political parties
- Political finance transparency
- Emotive politics
- Foreign interference

2

Civility and Political use of social media

The use of social media by political parties and candidates in electoral campaigns must be understood in the context of the civility of politics (use of hate speech and misinformation by politicians; political party members and candidates). They are key actors in political debate, increasingly so in the run up to elections. Direct communication on social media with voters is a powerful opportunity for connecting with the public and can genuinely be a positive tool for political participation and voter engagement. Conversely, if combined with a negative and polarised campaign environment (low "civility"), politicians use of social media can become problematic. By using social media, editors and journalists of quality media are cut out from the flow of political news and information. While social media bring greater access to discourse to all, which is welcome, it can also mean fewer checks on the quality of opinion and the truthfulness of reported facts that circulate online.[25]

Politicians' use of hate speech or misinformation online is even more threatening to the peace and stability of elections, as hate speech or use of inflammatory language can lead to increased polarization, violence, or intimidation. Also, the politicians are frequently the targets of online disinformation, and in low-trust environments political actors often seem to fuel polarized debates by attacking political enemies.[26] For example, during the 2019 Indian general elections the governing Bharatiya Janata Party (BJP) and the oppositional Congress Party were accused of spreading false and misleading information on each other's military policies in relation to the Kashmir territory.[27] Therefore greater use of hate speech and dissemination of misinformation by the politicians can increase the risk to electoral integrity.

Tightness of political race

If opinion polls predict tight results, there is a higher incentive for disinformation agents to try to swing the results in one or the other direction. Online manipulation campaigns are generally designed to create network-specific effects, targeted at particular electoral districts and segments of the population, rather than all the population. In tight races, a small swing in a sensitive constituency or segment of the population can determine the overall outcome (see above on electoral system). Targeting these audiences rather than the overall population is more cost-effective and makes tight political races more attractive for those looking to influence electoral outcomes.

Trust in political parties

Political parties are another important democratic institution and are key actors in the electoral campaign. Parties, especially the more centre or "establishment" parties are often the targets of disinformation strategies aimed to

25 Howard, 2020, Lie Machines, Yale University Press

26 Humprecht, 2019, "Where 'Fake News' Flourishes: A Comparison Across Four Western Democracies," Information, Communication, and Society 22, no. 13: 1973–88.

27 Ahmad, 2019 "Government Responses to Disinformation on Social Media Platforms: India", https://www.loc.gov/law/help/social-media-disinformation/india.php

undermine institutional legitimacy and destabilisation of elections.[28] The less trust there is in parties the more open electorates may be to disinformation about parties and politics. Of course, lacking trust in parties can be legitimate, where parties are used for authoritarian politics or corrupt. Parties can also be agents of disinformation (for example, the 2016 Brexit campaign and the 2016 Trump campaign used disinformation to disrupt.[29])

Political finance

Technology offered by social media allows the targeting of groups or individuals based on demographics, interests, geography and even more sensitive variables, such as race, religion or sexual orientation A lack of regulation of political finance (campaign finance or party finance) can result in non-transparent activity from domestic and even foreign actors, allowing them to use disinformation and skewing the level-playing field towards well-endowed interests.[30] It also allows political campaigning to take place by undeclared political actors, who often go undetected and raises the question of hidden, at times negative campaigning. For example, a study in Tunisia during the 2019 presidential and legislative elections showed that of the public Facebook pages identified as highly political engaged, 40% were not transparent of their affiliation, ownership or purpose.[31] Deceptive campaign practices that "emphasize rumour, conspiracy, disinformation, and manipulated media"[32] are facilitated if political finance legislation is incomplete or not adapted to the digital age, or not enforced. Some European countries have already implemented such adaptions, making monitoring and enforcement, often in partnership with technology companies themselves, the next hurdle.

Emotive politics

Emotive politics is linked to civility of politics. Some election issues may create societal tension or strong disagreement among the public. Emotional content is often the most effective content, travelling the fastest and furthest through networks via likes, comments and shares.[33] Emotional content is a legitimate form of campaigning but it becomes problematic when it only plays on people's feelings of superiority, fear, or anger. Studies[34] show that issues and topics raised in political campaigns, that tend to generate tension, emotion, and strong disagreements have a higher probability of manipulation via disinformation and hate speech. Election campaigns with a high presence of emotional topics can therefore be expected to be more vulnerable to online manipulation.

Foreign interference

Electoral integrity is based on a notion of sovereignty - citizens hold their political leadership to account. In a networked world no election is immune to foreign opinions and international non-partisan support to democratic elections is legitimate, but foreign actors should not be able to determine or influence the outcome of a national election. Social media technology poses a new challenge to the sovereignty of elections as it is increasingly difficult to distinguish between domestic campaign activities and information operations by foreign governments or interest groups. [35]

One problematic example is how most platforms allow for foreign and anonymous purchasing of political advertisement. Despite efforts by platforms to introduce verification systems to prevent entities from purchasing political advertisement, these measures are not been effective as the issue persists.[36] The Oxford Internet Institute's 2019

28 Bennett and Livingston 2018, The disinformation order: Disruptive communication and the decline of democratic institutions, https://journals.sagepub.com/doi/abs/10.1177/0267323118760317
29 Bennett and Livingston 2018, The disinformation order: Disruptive communication and the decline of democratic institutions, https://journals.sagepub.com/doi/abs/10.1177/0267323118760317
30 Kofi Annan Foundation, 2020, pg 71, Protecting electoral integrity in the digital age, https://www.kofiannanfoundation.org/app/uploads/2020/01/f035dd8e-kaf_kacedda_report_2019_web.pdf
31 DRI, 2019 pg 3, Monitoring of electoral campaigning on social media – Tunisia, https://democracy-reporting.org/wp-content/uploads/2020/02/DRI-SMM-Report-EN-Web.pdf
32 Kofi Annan Foundation, 2020, pg 71, Protecting electoral integrity in the digital age, https://www.kofiannanfoundation.org/app/uploads/2020/01/f035dd8e-kaf_kacedda_report_2019_web.pdf
33 Wardle and Derakhshan, 2017, pg 7, Information Disorder: Toward an interdisciplinary framework for research and policy making, https://rm.coe.int/information-disorder-toward-an-interdisciplinary-framework-for-researc/168076277c
34 DRI, 2019 pg 34, Monitoring of electoral campaigning on social media – Tunisia, https://democracy-reporting.org/wp-content/uploads/2020/02/DRI-SMM-Report-EN-Web.pdf
35 Kofi Annan Foundation, 2020, pg 81, Protecting electoral integrity in the digital age, https://www.kofiannanfoundation.org/app/uploads/2020/01/f035dd8e-kaf_kacedda_report_2019_web.pdf
36 McGregor, Barrett, and Kreiss, 2019, "Barely Legal: Digital Politics and Foreign Propaganda," https://digitalpoliticalethics.weebly.com/uploads/5/0/9/9/50994643/mcgregorbarrettkreissapsa19_submit.pdf

report showed that at least seven countries have “cyber troops” engaging in foreign influence operations on Facebook and Twitter.[37] This measure is by no means exhaustive of a highly secretive and evolving phenomenon.

Foreign online influence is a real and increasing threat to electoral integrity. The more geopolitically relevant a country is, the more likely it is that foreign actors may target the country’s election. For example, Finland, a country with a long border to Russia, a member of the EU but militarily neutral saw a notable increase in fake news stories and propaganda from Russia, linked to military shows of force along its shared border.[38] In comparison, Portugal, a country relatively removed from many geostrategic struggles, was not as vulnerable to disinformation campaigns during the 2019 elections.[39]

37 Bradshaw and Howard, 2019, pg 2, The Global Disinformation Order: 2019 Global Inventory of Organised Social Media Manipulation, https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2019/09/CyberTroop-Report19.pdf

38 Standish, 2017, “Why is Finland able to fend off Putin’s information war?”, Foreign Policy, https://foreignpolicy.com/2017/03/01/why-is-finland-able-to-fend-off-putins-information-war/

39 Democracy Reporting International and ISCTE-IUL Media Lab, 2019, “Disinformation risks in Portugal’s election: More Brazilthan Europe?”, https://democracy-reporting.org/wp-content/uploads/2019/10/2019-10-01-Portugal_Disinformation_Risk-Assessment.pdf

Media

In this section:

- **Media plurality, freedom and fractionalisation**
- **Consumption**
- **Connectivity**
- **Trust in media**
- **Technology companies' response**

3

Media plurality, freedom and fractionalisation

The concepts of plurality, freedom and fractionalisation of media are all closely linked. Media pluralism refers to transparency and diversification of media ownership, commercial and owners' influence over editorial content. This assumes that a diversified ownership structure is likely to better represent the views and positions existing in society. Diversity can become problematic when it turns into fractionalisation - media providing highly polarised reporting or "agendas", to the detriment of factual reporting. Media freedom refers to (self) censorship and vulnerability to political interference.

Firstly, media plurality, freedom, and fractionalisation are linked through their central role in ensuring freedom of expression and formation of opinion. An open flow of information, freedom of expression and an open and pluralistic media, must be guaranteed for voters to be able to make up their mind freely and without manipulation.[40]

Secondly, media plurality and freedom provide one basis for quality media. Professional journalists and editors provide a critical independent source of public knowledge and play an important role in evaluating elected leaders, candidates, and public policy options.[41]

Diverse, investigative quality media are one key to ensuring a "public sphere" favourable to democratic discourse in which political opinions can compete on a level-playing field. In a diverse, plural media landscape with quality media, it is more difficult to promote one-sided narratives and misinformation.

Consumption

Consumption of quality online and print newspapers is an important proxy for understanding the consumption of media grounded in journalistic standards of impartiality and investigative research. Greater use of credible sources of information and opinion tends to reduce the demand for alternative, lower-information information sources.[42] Such alternative sources are often associated with both extreme nationalist and foreign (often Russian) strategies to undermine institutional legitimacy and destabilize parties, governments and elections.[43] In addition, we assume that consumption of quality media means greater readership of diverse, pluralistic and independent political information. As outlined above, this is key to ensuring a public sphere favourable to democratic debate and quality information flows, avoiding prevalent misinformation and polarisation.

40 Jones, 2019, "Online disinformation and political discourse: Applying a human rights framework", Chatham House, https://www.chathamhouse.org/sites/default/files/2019-11-05-Online-Disinformation-Human-Rights.pdf

41 Howard, 2020, Lie Machines, Yale University Press

42 Bennett and Livingston 2018, The disinformation order: Disruptive communication and the decline of democratic institutions, https://journals.sagepub.com/doi/abs/10.1177/0267323118760317

43 Bennett and Livingston 2018, The disinformation order: Disruptive communication and the decline of democratic institutions, https://journals.sagepub.com/doi/abs/10.1177/0267323118760317

44 Eurostat, Digital economy an society statistics – households and individuals, https://ec.europa.eu/eurostat/statistics-explained/index.php/Digital_economy_and_society_statistics_-_households_and_individuals

45 DRI, 2019, pg 28, Guide for Civil Society on Monitoring Social Media during Elections, https://democracy-reporting.org/dri_publications/guide-for-civil-society-on-monitoring-social-media-during-elections/

Connectivity

The level of connectivity is a starting point to consider the influence of social media in public debate. The more connected a country is, generally the more exposed it is to these threats. With over 89% of households having access to the internet,[44] Europe is one of the most digitally connected regions in the world – and from that perspective exposed to online manipulation, even if it is not the only parameter. However, social media consumption is complex and connectivity, type of platform, and the presence of social media platforms in a given market influence how people use social media in their lives also indicate how exposed they may be to manipulated.[45] Various factors need to be considered in this factor which generally can be understood as a measurement of exposure, such as levels or frequency of social media use, types of social media platforms used, and consumption of other forms of political information such as quality media outlets.

Trust in media

Pluralistic quality media is significant in ensuring trust in political and electoral processes – and is therefore key for electoral integrity. Firstly, it is a contributor to social trust in other institutions, where justified, and secondly, from the perspective of the public, there must be trust in media.[46] Trust through media refers to trust in journalism's main purpose, the selection and presentation of information as well as plural opinion to the public. By reporting malfunctions of systems and violations of norms (e.g. voter fraud, a candidate's misconduct), journalism provides the public with impressions of how trustworthy a person, system, or process is. Trust in media refers to trust in the institution of journalism itself, traditionally the programming of news outlets via print, TV and radio, and increasingly the websites, posts and online articles. Recent research by Humprecht[47] suggests that countries with highly trusted news organisations, politically driven disinformation is less successful. This indicates that trust in media should be considered a factor of risk to online manipulation. Trust in media should be contextualised. In countries with less free media or where ruling parties have significant influence and control over media, trust in media plays a different role in public life than in functioning democracies.

Technology companies' response

Election initiatives and self-regulation: The larger the market size of a country, the more likely technology companies themselves are to pay attention to discourse on their platforms and the potential exploitation of them to influence elections. For example, Facebook set up "election war rooms" to fight misinformation ahead of the US mid-term elections and the Brazilian General elections in 2018,[48] the European Parliamentary elections in 2019[49] and others. Beyond establishing war rooms, the company raised transparency standards to prevent foreign interference and make political advertising on Facebook more transparent,[50] as part of the voluntary EU Code of Practice on Disinformation, established in 2018.[51] While providing a metric and dialogue with technology companies, critics point to its limited potential of impact.[52,53]

Scrutiny from technology companies themselves on the use of their platform before and during elections can help protect elections from manipulative interference (foreign or domestic).
The international structure of these platforms can make it difficult to assess their more centralised responses to online manipulation. At the country level, it may be useful to look for proxy indicators illustrating the attention a country's election may be gathering from an online platform. For example, the number of local language (non-English) staff are recruited to monitor content or policy, or how much financial resources a platform is investing in a country's election initiative, what are its rules on ad transparency, how much information is available in the national language(s).

---

46 Blöbaum, Trust and Journalism in a Digital Environment, 2014, pg 21, https://reutersinstitute.politics.ox.ac.uk/our-research/trust-and-journalism-digital-environment

47 Humprecht, 2019, "Where 'Fake News' Flourishes: A Comparison Across Four Western Democracies," Information, Communication, and Society 22, no. 13: 1973–88

48 Newton, 2018, "Inside Facebook's election war room", The Verge, https://www.theverge.com/2018/10/18/17991924/facebook-election-war-room-misinformation-fake-news-whatsapp

49 Liptak, 2019, "Facebook set up a war room to combat misinformation ahead of Europe's Parliamentary elections", The Verge, https://www.theverge.com/2019/5/5/18530337/facebook-european-parlimentary-election-war-room-misinformation

50 Geisel, 2019, "Protecting the European Parliament Elections", Facebook, https://about.fb.com/news/2019/01/european-parliament-elections/

51 The five categories of commitments the Code of Practice outlines include 1) scrutiny of advertisement placements, 2) political advertising and issue-based advertising, 3) integrity of services, 4) empowering consumers, 5) empowering the research community.
For more, see: https://ec.europa.eu/digital-single-market/en/news/annual-self-assessment-reports-signatories-code-practice-disinformation-2019

52 Darabian, 2019, "Reflections on the European self-regulatory code of conduct", London School of Economics EU Media Policy Blog, https://blogs.lse.ac.uk/medialse/2019/02/14/reflections-on-the-european-self-regulatory-code-of-conduct-will-it-be-enough-to-curb-online-disinformation-in-upcoming-campaigns/

53 EU Commission Media Convergence and Social Media, 2020, Study for the assessment of the code of practice against disinformation https://ec.europa.eu/digital-single-market/en/news/study-assessment-implementation-code-practice-disinformation

Society

In this section:

- Polarisation
- Education
- Citizen media literacy

4

Polarisation

In a society where polarization is already high, social media can be easily abused to further exacerbate and intensify political division and conflict.[54] Studies show that increasing societal polarisation is a driver of the dissemination and production of online disinformation.[55] It typically causes a rise in negative feeling that each side of the political spectrum holds toward the other, making it more likely to believe only stories reflecting their already established opinions[56] and using only partisan source of information. Partisanship can also shape the sharing of and commenting of political content – for example Twitter can serve as a multiplier in diffusing false information because rumour spreaders build strong partisan follower networks.[47] Therefore, it can be assumed that greater polarisation increases vulnerability of online manipulation.

Education

Education is an important inoculator against misinformation. Initial evidence[58] shows that strong emphasis on critical thinking skills in school curricula can provide some resilience to misinformation. For example, Finland, with a strong emphasis on critical thinking and information literacy was the most resistant nation in Europe to fake news, according to the 2019 Media Literacy Index.[59] For this reason, the more educated a society is, including "digital literacy", the less vulnerable it may be to online manipulation.

Citizen media literacy

In a recent study of Stanford University students' ability to evaluate information sources online, the researchers were surprised by the degree to which respondents were unable to distinguish an advert from editorial content or to question the partisan nature of facts presented to them.[60] US graduate students are not a representative sample, however these results are one of many that highlight the need for more news literacy programmes. Indeed, news literacy programmes tend to be one of the few preventative measures to disinformation on which almost everyone appears to agree.[61] Therefore, countries where such programmes are in place or part of curriculums may be less vulnerable to online disinformation.

54 Kofi Annan Foundation, 2020, pg 31, Protecting electoral integrity in the digital age, https://www.kofiannanfoundation.org/app/uploads/2020/01/f035dd8e-kaf_kacedda_report_2019_web.pdf

55 Allcott, and Gentzkow, 2017, "Social media and fake news in the 2016 election", Journal of Economic Perspectives, 31(2), 211–236. https://web.stanford.edu/~gentzkow/research/fakenews.pdf
Shin and Thorson, 2017, "Partisan selective sharing: The biased diffusion of fact-checking messages on social media" Journal of Communication, https://onlinelibrary.wiley.com/doi/abs/10.1111/jcom.12284

56 Humprecht, 2019, "Where 'Fake News' Flourishes: A Comparison Across Four Western Democracies," Information, Communication, and Society 22, no. 13: 1973–88.

57 Humprecht, 2019, "Where 'Fake News' Flourishes: A Comparison Across Four Western Democracies," Information, Communication, and Society 22, no. 13: 1973–88.

58 The Media Literacy Index 2019, 2019, https://osis.bg/?p=3356&lang=en

59 Henley, 2020, "How Finland starts its fight against fake news in primary schools" The Guardian, https://www.theguardian.com/world/2020/jan/28/fact-from-fiction-finlands-new-lessons-in-combating-fake-news

60 Stanford History Education Group, (Nov. 22, 2016) Evaluation Information: The Cornerstone of Civic Online Reasoning. https://sheg.stanford.edu/upload/V3LessonPlans/Executive%20Summary%2011.21.16.pdf

61 Wardle and Derakhshan, 2017, pg 68, Information Disorder: Toward an interdisciplinary framework for research and policy making, https://rm.coe.int/information-disorder-toward-an-interdisciplinary-framework-for-researc/168076277c

DEMOCRACY
REPORTING
INTERNATIONAL