Digital Democracy Risk Assessment:

A user guide

DEMOCRACY
REPORTING
INTERNATIONAL

Digital Democracy Risk Assessment:

A user guide

Funded by:

civitates
a philanthropic initiative for democracy and solidarity in europe

With contributions by:

98

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

What is the Digital Democracy Risk Assessment?

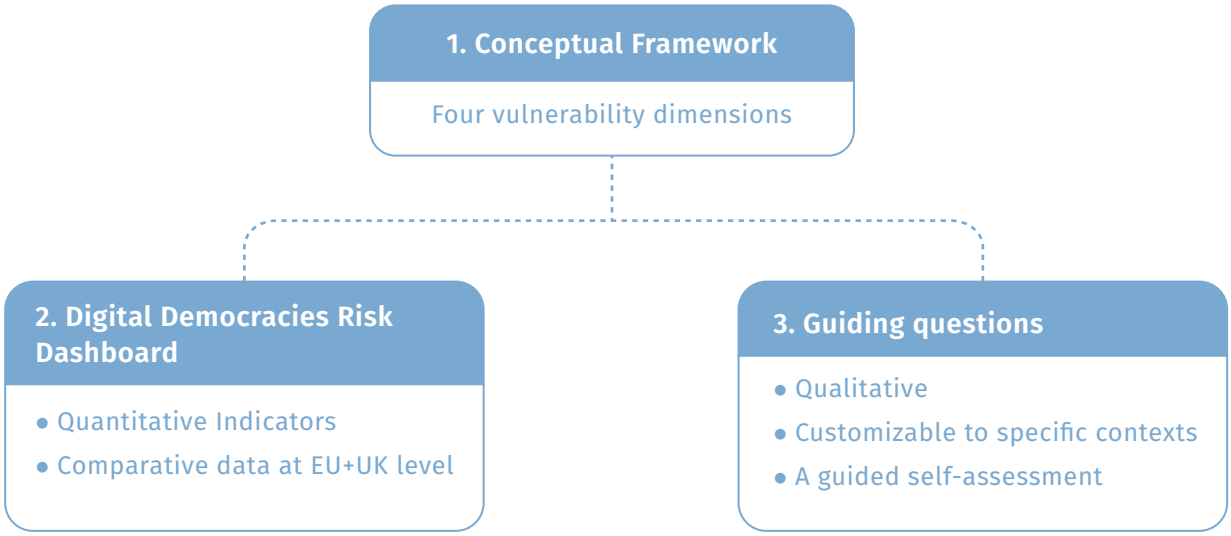
Democracy is becoming increasingly digital. The rise of the internet and social media has expanded political participation, but it has also opened possibilities to manipulate online discourse and elections. The speed, scope and scalability of how information travels on social media is completely different from traditional media, making online discourse a highly attractive target for manipulation[1]. Political parties and candidates, governments, campaign consultants, foreign actors have abused social media to spread disinformation, incite hate and violence, and meddle in elections.

The Digital Democracy Risk Assessment is a tool for civil society organisations and other researchers to assess the vulnerability of a country's electoral integrity[2] to online manipulation[3]. It allows researchers and organisations to **assemble a report on an election's vulnerability to online disinformation** based on a standard methodology and comparable data sets. For now, it includes data on European Union member states and the UK.

This User Guide explains the components needed for assembling a Risk Assessment. All related documents needed for this can be found on the online **Risk Assessment.** This document guides the user through the following components which make up the Digital Democracy Risk Assessment:

- The **Conceptual Framework** outlining vulnerability dimensions
- The online **Digital Democracy Risk Dashboard** which provides relevant data on 27 EU member states (and the UK)
- **Guiding Questions** for a qualitative assessment to contextualise and customise assessments. They are included in this document.

Digital Democracies Risk Assessment



[1] DRI Social Media Monitoring Methodology: https://democracy-reporting.org/wp-content/uploads/2019/10/social-media-DEF.pdf

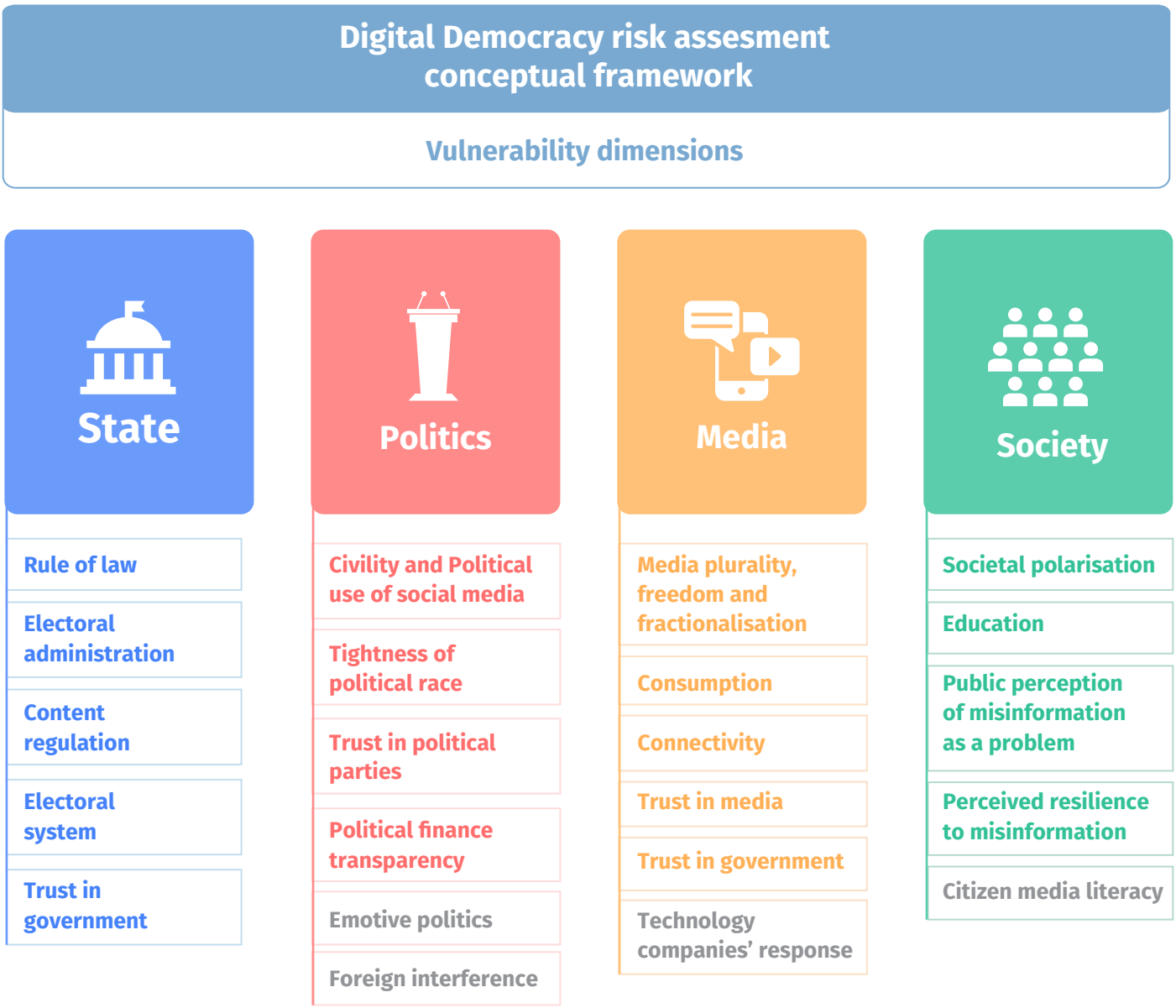
[2] "An election with integrity as any election that is based on the democratic principles of universal suffrage and political equality as reflected in international standards and agreements, and is professional, impartial, and transparent in its preparation and administration throughout the electoral cycle", see: https://www.idea.int/publications/catalogue/deepening-democracy-strategy-improving-integrity-elections-worldwide , and see the Background Paper on the Risk Assessment website for detail.

[3] We define online manipulation as "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". See the Background Paper on the Risk Assessment website for detail.

The Digital Democracy Risk Assessment's Conceptual Framework

This Assessment focuses on 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. Therefore, it answers the question whether a country and its election may be an attractive target for actors of disinformation.

We see online manipulation as threatening electoral integrity by impacting political participation, freedom of expression and opinion formation, privacy and trust. The Conceptual Framework identifies four dimensions where countries and their elections become vulnerable to online manipulation: State, Politics, Media and Society. Each dimension is broken down in attributes, which have been chosen based on their proven relationship to online manipulation[4].



Color text: data available in the Dashboard and Guiding Questions.
Grey text: Guiding Questions only.

[4] For more information on the theoretical basis and reason for selecting these dimensions and attributes, as well as the relationship between political participation, freedom of expression and opinion formation, privacy and trust, see the Background Paper on the Risk Assessment website for detail.

The Digital Democracy Risk Dashboard:

The Dashboard provides data on all dimensions and most attributes for 27 EU member states and the UK. It presents the data organised in the logic of the Conceptual Framework, and its "heatmap" visualisation easily indicates attributes or dimensions that may be more at risk to disinformation campaigns. As a comparative tool, the Dashboard can also be used to compare and contrast data across countries to the attribute level.

The Dashboard uses the most recent data from open sources. You can find it on the **Risk Assessment** website. There you can also find the **Methodological Note** with information on the data sources, indicator construction and coding.

Guiding Questions:

The Guiding Questions are organised along the four vulnerability dimensions (State, Politics, Media and Society). As the qualitative component of the Digital Democracy Risk Assessment, the Guiding Questions are used to add context to the quantitative Dashboard data. The Guiding Questions are designed to complement the Dashboard and allows users to map and assess the magnitude of these vulnerabilities.

The Guiding Questions provide a summary of the relationship between the various factors and how they may impact electoral integrity. This assists users in understanding how to read the Dashboard and considerations for building a Risk Assessment. For detail on the assumptions and relationships between these factors and the effect on electoral integrity, see the Background Paper on the **Risk Assessment** website.

1. State

Attribute	**Assessment questions:** ***Questions to consider when assessing the vulnerability of upcoming elections***	**Dashboard indicators:** ***What is measured?***	**Assumption/relationship to electoral integrity:** ***How does this attribute make elections more vulnerable to online interference?***
Rule of law	• To what extent is the rule of law respected in the country? • To what extent are government regulations effectively enforced? • To what extent is there equal, fair access to justice for citizens? • How effective is the criminal investigative system? Are online crimes (such as prohibited hate speech) prosecuted and enforced? • For detail, see the DRI publication: **The Components of the Rule of Law: A Primer**	Rule of law: Legal Certainty and Judicial Review	Low rule of law increases the vulnerability. Risk of impunity for malicious actions

Electoral administration	• Does the Electoral Management Body (the national institution legally responsible for managing some or most of the essential elements of an election) have the staff, funding, and independence to carry out its role in managing the election? • Was the current executive and/or legislature elected through free and fair elections? • How fair and clear are the electoral laws?	Electoral Management Body Capacity and Fair electoral process	The less capable electoral administration is, the more vulnerable electoral integrity is. Loopholes in legislation open the scope for online abuse. History of unfair elections may point at government unwilling to enforce electoral fairness.
Regulation of illegal content	• Does law exist that regulates (online) content in, e.g. hate speech or false information on electoral process? • Does the government use resources or institutions to monitor online content?	Government capacity to regulate online contentand Government online content regulation approach	Less regulation of online content increases vulnerability. Inability to monitor and enforce regulation increases vulnerability.
Electoral system	• What kind of electoral system does the country have for the given elections?	Lower chamber electoral system	Majoritarian electoral systems may be more vulnerable, especially when lead candidates/parties are close (high return on investment for manipulative interference)
Trust in government	• To what extent do people trust the government? • To what extent do people trust other state institutions?	Trust in government	Less trust in government increases vulnerability

2. Politics

Attribute	Assessment questions: *Questions to consider when assessing the vulnerability of upcoming elections*	Digital Democracy Risk Dashboard indicators: *What is measured?*	Assumption/relationship to electoral integrity: *How does this attribute make elections more vulnerable to online interference?*
Civility	• How often do major political parties use hate speech as part of their rhetoric? (Hate speech is any speech that is intended to insult, offend, or intimidate members of specific groups, defined by race, religion, sexual orientation, national origin, disability, political opinion, or similar trait) • How normalised is use of hate speech by political parties and members of the political elite?	Political parties hate speech	The more frequent and accepted hate speech is by political parties, the greater the vulnerability (online hate speech silences voices and contributes to extreme polarisation)
Tightness of political race	• Are pre-election opinion polls tight/close? Tight polls create more incentives for disinformation agents to swing results	Difference in votes between the two top political parties in the last elections (retrospective)	The tighter election outcomes are to call (especially in majoritarian systems), the greater the vulnerability
Political use of social media	• To what extent do major political parties and candidates use social media during electoral campaigns to communicate with constituents?	Party/candidate use of social media in campaigns	Dependent on "Civility". Greater use of social media in election campaigns increases vulnerability in low civility environments. Greater engagement of the political elite in online politics increases the number of actors and targets for disinformation campaigns.

Political finance transparency	• To what extent is private and public party financing and electoral campaign financing transparent, effectively monitored and in case of infringement of rules subject to proportionate and dissuasive sanction? • Does regulation exist that forces donations to political parties to be made public? Is this enforced by the state?	Transparent regulation for political party financing	Lower transparency and regulation of political finance government increases vulnerability (for example for funds spent online with no transparency, accountability or limits)
Trust in politics	• To what extent do people trust political parties?	Trust in political parties	Lower trust in political parties increases vulnerability. 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.
Emotive politics	• To what extent are election campaign issues emotive? Do they create societal tension or strong disagreement among the public?	No data	The more emotive campaigns are the greater the vulnerability, as debates become personal and facts/ data lose their relevance
Foreign interference	• How geopolitically relevant are the upcoming elections? • Is there reason for governments or non-government actors to want to manipulate a certain electoral outcome? (e.g. geopolitical, resource, conflict reasons) • Is there a history of foreign interference?	No data	Greater geostrategic interests increase vulnerability (higher incentive for foreign interference)

3. Media

Attribute	Assessment questions: *Questions to consider when assessing the vulnerability of upcoming elections*	Dashboard indicators: *What is measured?*	Assumption/relationship to electoral integrity: *How does this attribute make elections more vulnerable to online interference?*
Media plurality	• Are different perspectives, voices, opinions and issues provided in the major media? • Are effective anti-monopoly policies in place? • Do impartial, open public media allow a pluralism of opinions? • Are public broadcasters a relevant source of information and do they provide balanced coverage?	Media pluralism; the degree to which opinions are represented in the media	Lower media plurality makes it easier to push one-sided narratives and facts, increasing vulnerability
Media freedom	• Are the media directly or indirectly censored? • Is self-censorship common among journalists (the term includes professional journalists, bloggers, and citizen journalists), especially when reporting on sensitive issues, including politics, social controversies, corruption, or the activities of powerful individuals? • Are journalists subject to pressure or surveillance aimed at identifying their sources?	Free and independent media	Less media freedom and independence increase vulnerability. Lack of media freedom can limit or restrict quality information access for citizens, potentially leading citizens to use alternative, low quality media outlets
Consumption	• What proportion of the population consumes online and print quality newspapers?	Consumption of print and online newspapers	Lower consumption of traditional quality media increases vulnerability, because information and debate is not grounded in journalistic standards of impartiality, research, etc. Instead spam and rumours may dominate debates.

Connectivity	• What proportion of the population consumes online and print quality newspapers? • What proportion of the population uses online social media or online messaging apps? • How many people have personal devices? • What are the main social media platforms used by people?	Consumption of online social media or online messaging apps	Greater connectivity increases vulnerability, as more of the population is potentially exposed to seeing or engaging with disinformation campaigns
Fractionalization	• Do major domestic media outlets give a similar presentation of major (political) news? • Do major domestic online media outlets differ greatly in the presentation of major events?	Online media fractionalization	Greater fractionalization increases vulnerability. Highly fractionalized media provides a polarised world view and can contributes to seeing news as competing "agendas". It also contributes to trust.
Trust in media	• How much do people trust news from different media sources? TV, newspapers, radio, social media platforms, messaging apps? • Which is the most trusted form of getting news?	Trust in media	Lower trust in established/ quality media leads to more reliance on social media/ low-quality reporting. In countries with highly trusted news organisations, politically driven disinformation is less successful.
Technology company response	• Do any of the major social media platforms have election initiatives for protecting upcoming electoral integrity or provide information for voters? • Do any of the major social media platforms have self-regulation that addresses disinformation and illegal content? • Have major social media platforms invested in local-language staff (if not English)?	No data	Lower interest and response from tech companies increases the vulnerability

4. Society

Attribute	Assessment questions: *Questions to consider when assessing the vulnerability of upcoming elections*	Dashboard indicators: *What is measured?*	Assumption/relationship to electoral integrity: *How does this attribute make elections more vulnerable to online interference?*
Polarization	• How polarised is society? To what extent is the electorate "sorted" into two political camps with deep divisions, potentially going beyond political opinion, including other orientations (religious belief, lifestyle, etc.) • To what extent is there general agreement on the general direction society should develop?	Polarization of society	Greater polarisation increases vulnerability, increasing societal polarisation is a driver of the dissemination and production of online disinformation
Education	• What is the average level of education in society? • What proportion of adults have a high school degree? • What proportion of adults have a university degree?	Average national education levels	Lower education increases vulnerability. Higher education levels are associated with greater critical thinking and media literacy.
Acceptance of misinformation	• Does the general public perceive misinformation as an issue in elections? • To what extent do people see misinformation, disinformation, fake news, and other forms of online manipulation as a problem for upcoming elections?	Acceptance of misinformation as a societal issue	Greater acceptance of misinformation increases vulnerability
Perceived resilience to misinformation	• Does the general public feel they are able to identify fake news or misinformation?	Self-reported resilience against misinformation	Given the self-reported indicator, interpretations of results should be careful of the accuracy of this data
Citizen media literacy	• Do citizen media literacy programmes exist at the state level, such as in schools, universities, or public campaigns?	No data	Lower citizen media literacy increases vulnerability

DEMOCRACY
REPORTING
INTERNATIONAL