DEMOCRACY
REPORTING
INTERNATIONAL

Assessment of Online Risks for the 2021 German Federal Elections

Assessment of Online Risks for the 2021 German Federal Elections

DEMOCRACY
REPORTING
INTERNATIONAL

About Democracy Reporting International

Democracy Reporting International (DRI) strengthens democracy by shaping the institutions that make it sustainable. We support local ways of promoting democracy with impartial analysis and good practices, bringing international standards to life. The belief that people are active participants in public life, not subjects of their governments, guides what we do. We work with local actors to protect and expand our shared democratic space in a polarized world, regardless of political opinions or personal beliefs. Find out more at: http://www.democracy-reporting.org

Acknowledgements

This report was written by Erik Meyer, with contributions by Michael Meyer-Resende and Helena Schwertheim. The report findings are based on the expert roundtables hosted by DRI on 20 April and 27 April 2021. Forset designed the layout of this publication.

Date: June 2021

This paper is part of a project funded by Reset. Its contents do not necessarily represent the position of Reset.

Reset.

Contents

1. Executive Summary

The COVID-19 pandemic has significantly increased the degree of digital transformation in Germany. As a result, the 2021 federal election campaign will take place in a context where many voters have increasingly been using social media networks, messenger services and video platforms to communicate, obtain information and organize their lives.

There are specific risks associated with online political communication and, for a number of reasons, the 2021 federal elections are of particular interest to actors active in spreading disinformation. The end of the Angela Merkel era, as the current Chancellor leaves office, and a further weakening of the traditional major parties point to a reorientation of German politics. The political frictions caused by the COVID-19 pandemic and the measures taken to address it increase the risks of political extremism.

At the same time, a number of factors specific to the German context reduce the risks present in the context of other democracies. These factors include:

- Germany's federal electoral law: Compared to traditional first-past-the-post systems, the German system provides no opportunity for targeted manipulation of the overall result by influencing the results in a small number of constituencies;
- Many elements of the legal framework are stronger than is the case in other democracies, particularly the Network Enforcement Act (Netzwerkdurchsetzungsgesetz, NetzDG), which requires digital platforms to take action against content that is prohibited by law; and
- Media outlets that meet standards for professional journalism are reported as more important for the formation of public opinion in Germany than in other democracies, and public trust in these media outlets is comparatively high.

Other factors, however, represent threats to the fairness of the online campaign in the following areas:

Paid online political advertising:

- Expenditures on paid political online advertising are rising, but there is little transparency in this area. One reason is that legislation with regard to party and campaign financing is very weak, while another is that online providers make available only limited information on paid campaign materials (in their "advertising archives"). Further, there are many grey areas, such as in the legal obligations of social media "influencers";
- Sending particular political advertising materials to specific groups (microtargeting) undercuts the principle of political responsibility, as it is no longer possible to trace what has been promised to whom; and
- Paid advertising more generally is also problematic when used to support the dissemination of disinformation, e.g., in directing users to pseudo-journalistic media outlets whose purpose is the spread of propaganda or of fake media content.

Hate speech:

- The dissemination of hate speech (prohibited content that attacks or uses discriminatory language against individuals or groups) is significantly curtailed by the NetzDG, but it continues to find many ways online, often targeting women and minorities;
- Campaigns mobilizing people to take part in violent activities in order to attract attention (for example: to attempt to storm the parliament building). Until recently, social media platforms have paid little attention to this danger; and
- Due to a restrictive interpretation of the NetzDG, no specific obligations exist for major distribution channels. Through the platform Telegram, for instance, obviously antisemitic content continues to be distributed to large groups of users.

Disinformation:

- Controversial issues that lead to polarization, which regularly arise in democracies, are pushed to extremes, and thus distorted;
- Perceptions of what are the most politically important issues are manipulated. This may be done through automatic accounts that create artificial reach for a topic or a claim, or by the coordinated actions of real users aimed at giving the impression of spontaneous public outrage;
- Disinformation regarding the electoral process: The Alternative für Deutschland Party (Alternative for Germany, AfD) has adopted this strategy embraced by a large part of the United States Republican Party that suggests that postal voting is being used to commit systematic fraud;
- Clumsy communication by authorities or journalists is often used to create disinformation; and

Cyberattacks against authorities or online meetings (for example: in the case of the CDU (Christian Democratic Union of Germany) party conference in January 2021 serve to create disinformation.[1] These spread a sense of threat and confusion, with the aim of weakening trust in democratic processes.

Foreign interference:

The EU reports that Germany is the main target of Russian disinformation campaigns in Europe,[2] and China is also increasingly being mentioned in this context. Care should be taken in attributing disinformation campaigns to foreign actors, so as not to represent these actors as more important or powerful than they are.

Foreign disinformation refers to the spreading of disinformation or hate speech already described above. Specific additional risks arise from the distribution of illegally acquired information (for instance, data from the hacking attack on the German parliament).[3]

At the end of this report, we recommend short-term measures to reduce these various risks for the federal elections.

1. Janosch Delcker, “Cyber Threat Looms Large over German Election”, DW, 25 May 2021, https://www.dw.com/en/cyber-threat-looms-large-over-german-election/a-56775960.
2. EuvsDisinfo, “Vilifying Germany; wooing Germany”, 9 March 2021, https://euvsdisinfo.eu/villifying-germany-wooing-germany/
3. Farah Bahgat, “Russia-Backed Hackers Target German Legislators: Report, 26 May 2021, https://www.dw.com/en/russia-backed-hackers-target-german-legislators-report/a-57018097.

2. Background

On 20 April 2021, Democracy Reporting International (DRI) hosted a roundtable in Berlin with relevant civil society representatives to discuss the risks during the online campaign for this year’s federal elections in Germany. For providing their expertise and comments, we would like to thank the representatives of:

- The Alliance of Democracies Foundation
- The federal parliamentary group of the Alliance 90/The Greens party
- The Center for Monitoring, Analysis and Strategy (CeMAS)
- The European New School of Digital Studies
- The German Marshall Fund
- The Leibniz Institute for Media Research, Hans Bredow Institute
- HateAid
- The Institute for Strategic Dialogue (ISD)
- The John F. Kennedy Institute for North America Studies of Freie Universität Berlin
- Stiftung Neue Verantwortung (SNV)
- Tactical Tech

On 27 April 2021, a summary of the conclusions from the round table was presented and discussed by a wider circle. Apart from participants from the scientific institutions and civil society organizations mentioned above, representatives from the following bodies also took part:

- AlgorithmWatch
- The Heinrich Böll Foundation
- Stiftung Mercator
- The Oxford Internet Institute
- The German Federal Foreign Office
- The EU East StratCom Task Force

In addition, representatives of the State Media Authorities of Baden-Württemberg and Berlin-Brandenburg, as well as of the social media platforms Facebook and Twitter, presented assessments and related initiatives they have undertaken. The following outlines the key aspects of these discussions, but does not necessarily reflect the opinions of all participants.

In 2020, DRI developed the Digital Democracy Risk Assessment, an instrument for evaluating the susceptibility of national elections to online manipulation. The Assessment provides a conceptual framework, a user guideline and a dashboard containing data for the 27 EU member states and the United Kingdom. The conceptual framework comprises four dimensions that make elections susceptible to online manipulation: the state, politics, media and society. The present report provides an overview of the risks for the German federal elections in relation to these four dimensions. The discussion at the round table, as well as the risks examined, frequently covered several dimensions at the same time.

3. Political context of the 2021 federal elections

On account of its geopolitical situation and its influence within the European Union, Germany is a political actor of global importance. Domestic developments in the country are, therefore, of interest to many foreign actors.

For several reasons, the 2021 federal elections are of particular significance:

- The end of the Merkel era and a possible reorientation of German politics;
- The likely further shift in the party system, at the expense of the former major parties;
- Increasing global competition between democratic states and authoritarian systems;
- The political frictions caused by the COVID-19 pandemic, including greater polarization and, in a number of states, a fundamental rejection of the government's COVID-19 response or a denial that the pandemic is dangerous;
- Increasing political extremism that is also, but not only, based on the rejection of measures taken to tackle the pandemic. Right-wing extremism is present in the German parliament in the form of the AfD. In this context, there has been a shift in discourse that delegitimizes democracy in general; and
- The further move online of political communication during the pandemic, meaning that political parties will communicate online to a greater extent during the election campaign than they did in 2017, regardless of the specific pandemic situation. This will present starting points for political debate that increasingly takes place on the internet.

3.1 Media context: The current relevance of online political communication

Due to the increased degree of digital transformation caused by the COVID-19 pandemic, online content has become increasingly important to the formation of public opinion in Germany. "Almost half of all Germans (45 per cent) now use search engines, social networks and instant messenger services on a daily basis to stay informed about current affairs," an analysis conducted by the State Media Authorities for the second half of 2020 found.[4] This development applies to informed media use in general, but explicitly political communication on Facebook, Instagram and Twitter is also relevant. One-fifth of the German population over the age of 14 encounter political messages through these channels on a regular basis.[5] An online study by the public broadcasters ARD and ZDF for 2020 shows that those messaging services that can be considered part of individual communication are used more frequently as well. A little more than two-thirds of the population (68 per cent) use messenger services such as WhatsApp daily.[6]

4. Die Medienanstalten, "Informierende Mediennutzung so hoch wie nie – Internetnutzung legt weiter zu", 29 April 2021, https://www.die-medienanstalten.de/service/pressemitteilungen/meldung/informierende-mediennutzung-so-hoch-wie-nie-internetnutzung-legt-weiter-zu
5. Ibid
6. Natalie Beisch and Carmen Schäfer, "Internetnutzung mit großer Dynamik: Medien, Kommunikation, Social Media", Media Perspektiven 9/2020, https://www.ard-zdf-onlinestudie.de/files/2020/0920_Beisch_Schaefer.pdf

A survey conducted by Eurobarometer 2019 found that 47 per cent of German citizens trust the media.[7] This figure may appear low, but compared to other EU countries it shows a relatively moderate level of trust (the median level being 44 per cent. The highest level of trust was recorded in Finland, at 73 per cent, while Greece shows the lowest level, with 20 per cent).[8]

3.2 Framework conditions with structural effects

STATE: THE ELECTORAL SYSTEM

The German electoral system of mixed proportional representation is less susceptible to being influenced by disinformation campaigns than pure majority voting, as it prevents the mobilizing of a small number of votes in marginal constituencies alone to significantly influence the proportional composition of the parliament as a whole. In addition, the multi-party system allows for many different possible ruling coalitions and, therefore, prevents the case of an "either-or election". As such, those factors that create options for manipulation are reduced. Against this background, a more general kind of influence that aims to undermine trust in the democratic process is to be expected.

MEDIA: THE REGULATION OF INFORMATION INTERMEDIARIES

In many ways, the legal framework regulating politically relevant online communication in Germany is more restrictive than in other democracies. The key element in this is the NetzDG, which obliges social network providers to adhere to minimum standards in the fight against the spread of illegal content. Its effects, however, have been controversial, as critics accuse it of "overblocking" that threatens free speech because the platforms implement their community standards in a more restrictive way to avoid NetzDG cases. Some of the positive effects that have been observed are a greater awareness of problematic content and an increased use of resources for self-regulation. At present, the relevant practice of content moderation and "deplatforming" has not been evaluated independently, as the necessary data are not fully available.

Another regulatory mechanism is provided by the provisions of the State Media Treaty (Medienstaatsvertrag), which gives the State Media Authorities a supervisory role over intermediaries.[9] The State Media Authorities do not, however, carry out systematic monitoring but, instead, only respond to instances that are brought to their attention, e.g., when complaints are made or when problematic content achieves a wide range of coverage.

With regard to the elections, the implementation of the requirement to identify online political advertising when it comes to the cooperation of advertisers with influencers will also play a vital role. Moreover, political advertising must be continuously identified as such, even when content marked as advertising is shared by users. Another challenge now faced by the State Media Authorities is monitoring

7. See the data on trust in media in the dashboard of the Digital Democracy Risk Assessment on "media" (https://digitalmonitor.democracy-reporting.org/risk-assessment), based on the survey data of the Eurobarometer collected by the EU Commission (https://data.europa.eu/euodp/en/data/dataset/S2253_91_5_STD91_ENG).
8. Ibid.
9. Germany has 14 State Media Authorities (Medienanstalten) – one per Federal state. Traditionally, these have been responsible for the licensing and supervision of radio and television broadcasters, but now this is expanding to include intermediaries (social media platforms). For detail, see: https://www.die-medienanstalten.de/en/about-the-media-authorities.

compliance with journalists' duty of care by online media that have not been monitored in the past.[10] In 2021, some "alternative media" were notified of violations of their duties for the first time, although it is unlikely that the resulting procedures will lead to any short-term sanctions.

POLITICS: PARTY AND CAMPAIGN FINANCING

While the system for state funding of political parties in Germany has many positive aspects compared to those in other countries, international and civil society organizations have identified regulatory shortcomings and the need for reform, in particular with regard to transparency in party donations and campaign financing. For instance, the value of donations, along with the name and address of the donor only have to be listed in a party's financial reports when the sum is greater than 10,000 euros. These reports, however, are presented only once a year, and only donations in the amount of 50,000 euros or more received by a party must be immediately reported to the Presidium of the Bundestag, followed by the publication of the donation. The OSCE Office for Democratic Institutions and Human Rights (OSCE/ODIHR) and the Council of Europe Group of States against Corruption (GRECO) have both called for the introduction of a duty to report any campaign funding received individually in a timely manner.

POLITICS: TRUST IN POLITICAL PARTIES

Political parties continue to be important democratic institutions, including as key actors during election campaigns. The lower the level of trust in parties is, the more receptive voters may be to disinformation about them and about politics overall. A survey conducted by Eurobarometer 2019 found that 29 per cent of German citizens have trust in the political parties in their country (without providing any data to which parties this refers).[11] This figure may appear low, but actually represents a high level of trust compared to other EU countries (the highest level of trust recorded was in Denmark, with 48 per cent, while Great Britain showed the lowest, at 8 per cent).[12] These data were compiled prior to the COVID-19 pandemic.

SOCIETY: TRUST IN GOVERNMENT

A certain level of trust by citizens in the elected government is important for social cohesion and the effectiveness of governance. Often, a key goal of disinformation campaigns and online interventions aimed at the polarization of society is to undermine confidence in the government and political parties. A survey conducted by Eurobarometer 2019 found that 45 per cent of German citizens trust their government, a moderate but not high level of trust compared to other EU countries (the levels in this survey ranged from 13 per cent in Croatia to 63 per cent in the Netherlands).[13] This survey was conducted before the COVID-19 pandemic, and the associated state reactions have likely rendered the data less meaningful.

10. Landesanstalt für Medien NRW, "In den Blick genommen: Journalistische Sorgfaltspflichten im Netz", 12 February 2021, https://www.medienanstalt-nrw.de/presse/pressemitteilungen-2021/2021/februar/in-den-blick-genommen-journalistische-sorgfaltspflichten-im-netz.html.
11. See the data on trust in media in the dashboard of the Digital Democracy Risk Assessment on "Politics: Trust in Political Parties" (https://digitalmonitor.democracy-reporting.org/risk-assessment/), based on the survey data of the Eurobarometer collected by the EU Commission (https://data.europa.eu/euodp/en/data/dataset/S2253_91_5_STD91_ENG).
12. Ibid.
13. See the data on trust in media in the dashboard of the Digital Democracy Risk Assessment on "State: Trust in National Government" (https://digitalmonitor.democracy-reporting.org/risk-assessment/), based on the survey data of the Eurobarometer collected by the EU Commission.

3.3 The risks regarding central areas of activity of political online communication

Political online advertising

Paid political advertising in online formats is, as a rule, not transparent. It is difficult, if not often impossible, to discover who is responsible for what with regard to specific online content; who buys advertising and to what extent; and to which target groups it is addressed and what data are used to target these groups. Even though a number of social media platforms, such as Twitter and TikTok, by their own assessment no longer offer political advertising related to elections, there remains a significant grey area in which candidates and parties spend increasingly large sums. This can be illustrated, for example, by the growing number of political advertisements on Facebook and Instagram, as well as by the increase in relevant advertising expenditures.[14] In this context, the call for greater transparency is one prerequisite for analysing the effects of this type of advertising, as it has not to date been possible to explore these through external monitoring and scientific research.

Apart from the lack of transparency, the following risks exist:

- Violations of the General Data Protection Regulation (GDPR), for instance, when voters are classified according to their political orientation. The organization Tactical Tech has produced several reports that investigate the global business of using politically significant personal data;[15]
- Extremist forces that attempt to demobilize or mobilize certain segments of the electorate with the help of paid advertising;
- Paid advertising that leads users to pseudo-journalistic content that obviously does not meet professional journalistic standards and, instead, spreads disinformation and propaganda;
- Violations of campaign financing because expenditures are not declared and cannot be publicly verified;
- An impoverished political debate and level of political responsibility due to the microtargeting of messages. Arguments and promises can remain invisible to many or be distributed in a highly fragmented way and, therefore, will not be discussed in public. This undermines political parties' public responsibility for their positions and promises;
- The legal framework for regulating online political advertising is weak. Parties and candidates are not required to publish their online advertising expenditures in a timely manner or to make information on this available. Stiftung Neue Verantwortung has stated that: "There are clear guidelines that specify what type of demographic data can be used by whom for sending bulk mail by post. With regard to behaviour-based microtargeting on the internet it is the platforms alone that usually determine how they approach the targeting of political advertising.";[16]

14. Fieber, "Wie Deutschlands Parteien auf Facebook Politik machen - und warum die AfD so erfolgreich ist", 15 April 2021, https://web.de/magazine/politik/deutschlands-parteien-facebook-politik-afd-erfolgreich-35712388
15. For more information, see: https://ourdataourselves.tacticaltech.org/projects/data-and-politics/
16. Julian Jaursch, "Regeln für faire digitale Wahlkämpfe", Stiftung Neue Verantwortung, 8 June 2020, https://www.stiftung-nv.de/sites/default/files/regeln_fur_faire_digitale_wahlkampfe.pdf

- While the GDPR prohibits the "processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs" (Article 9), there remain considerable ambiguities, such as in cases where these characteristics are derived indirectly from other personal characteristics. In addition, there is no protection provided in the GDPR against advertising based on the assessment of psychological characteristics (Article 22, on profiling); and

- The weak legal framework is reflected in the fact that no institutional foundation exists; no public authority systematically monitors political online advertising, and this task is left to non-state actors.

Online hate speech and illegal content

"Hate speech" is a general term that covers statements prohibited under the German Criminal Code, in particular sedition (Article 130), threat, slander or defamation, while in a number of studies a broader concept of "hateful speech" is used. In either case, the term does not cover the making of polemical or highly critical statements, which is common practice in political debates.

The issue of hate speech in online public spheres has an explicitly political dimension. Hate speech aims to polarize discussions to an extreme degree, in order to discourage or silence particular groups of users. Online hate speech directly affects people's mental well-being and can incite others to commit acts of violence, as became clear in the murder of Walter Lübcke, the District President of Kassel.[17] Studies conducted by the Amadeu Antonio Foundation show that hate speech often overlaps with right-wing terrorist content.[18] The Institute for Strategic Dialogue (ISD) has published numerous reports that demonstrate how extremist movements, in particular right-wing extremists and jihadist movements, implement sophisticated communication strategies that use violent rhetoric as a major element in the radicalization and mobilization of their followers.[19] The ISD has also demonstrated that a large share of the spread of hate speech can be attributed to a very small number of users.[20]

The risks ahead of the federal elections include:

- Systematic hate campaigns to intimidate and/or silence people with different opinions. These campaigns often target women, minorities or people that have a prominent role in political life (politicians, journalists, etc.). Stressful debates like these discourage others from taking part in political processes, and even from voting or standing as candidates for political office;

- Interference with the electoral process, through hate speech targeted at those involved in organizing elections (election workers and officials);

- Campaigns mobilizing people to take part in violent activities in order to attract attention. The attempt to storm the parliament building illustrates this;[21] and

17. For detail on this case, see: https://www.bbc.com/news/world-europe-53662899
18. Manemann, "Rechtsterroristische Online-Subkulturen: Analysen und Handlungsempfehlungen", Amadeu Antonio Stiftung, 2020, https://www.amadeu-antonio-stiftung.de/wp-content/uploads/2021/02/Broschu%CC%88re-Rechtsterroristische-Online-Subkulturen_pdf.pdf
19. Baldauf, Ebner and Guhl (Eds.), "Hate Speech and Radicalisation Online: The OCCI Research Report", Institute for Strategic Dialogue, 2019, https://www.isdglobal.org/wp-content/uploads/2019/06/ISD-Hate-Speech-and-Radicalisation-Online-English-Draft-2.pdf
20. Kreißel, Ebner, Urban and Guhl, "Hass auf Knopfdruck: Rechtsextreme Trollfabriken und das Ökosystem koordinierter Hasskampagnen im Netz", Institute for Strategic Dialogue, 2018, https://www.isdglobal.org/wp-content/uploads/2018/07/ISD_Ich_Bin_Hier_2.pdf
21. Blennhold, „Far Right Germans Try to Storm Reichstag as Virus Protests Escalate", New York Times, 31 August 2020, https://www.nytimes.com/2020/08/31/world/europe/reichstag-germany-neonazi-coronavirus.html

- The increase in hate speech, and especially through channels and on platforms that are not covered by the NetzDG. The messenger service Telegram includes many accounts, followed by tens of thousands of users, that share obviously antisemitic, racist or violent content. Despite this, the service is subject to almost no regulation in Germany. It is not even possible to identify where it is operated from and how the operators can be contacted.

The NetzDG requires large platforms to delete obviously illegal content, e.g., cases of slander, within 24 hours. It is difficult to determine to what extent the companies actually comply with this legal requirement. The current interpretation of the law does not extend to messenger services.

Disinformation

In recent years, disinformation has become more subtle, by mixing truth and falsehood, by ignoring or hiding contexts, or by creating the impression of being part of larger public debates. The systematic dissemination of false or misleading statements with regard to political issues or procedures, in particular, threatens the process of shaping public opinion and policies in democratic societies, and affects not only particular political content or individual political actors. The discrediting of journalists and the media, in particular, leads to a loss of trust and calls into question communication about verifiable facts in general. In that sense, disinformation can compromise public opinion regarding the quality of democratic elections (the "integrity of the elections"). Disinformation is frequently carried out by domestic actors who replicate campaigns in other countries – the United States in particular.[22]

The specific risks before the federal elections include:

- Controversial issues in German society that are polarized, which is normal in democracies, are pushed to extremes. This pattern can be found in all major debates. A legitimate discussion on immigration can be distorted in an extreme way by claims that there is a global conspiracy. A debate about the best approach to the COVID-19 pandemic is reduced to absurdity by groundless statements claiming that the pandemic does not exist or that vaccinations are another global conspiracy;

- There are attempts to manipulate perceptions of what the most politically important issues are. This may be done through automatic accounts that create artificial reach for a topic or a claim, or by the coordinated actions of real users aimed at giving the impression of spontaneous public outrage;

- Disinformation can directly focus on electoral matters, in order to undermine the credibility of the elections. The AfD adopts this strategy, embraced by a large part of the United States Republican Party, by suggesting that postal voting is being used to commit systematic fraud;[23]

- As in the case of hate speech, a switch can be seen to other platforms or services (messenger services, newsletters) where there is less monitoring and regulation. Again, there is a risk that online disinformation has effects beyond the online sphere (in Germany, this is a well-known phenomenon following the "case of Lisa");[24]

22. Huesmann, "Europawahl: AfD und rechte Aktivisten wollen das Vertrauen in die Demokratie untergraben", Watson, 23 May 2019, https://www.watson.de/deutschland/politik/503310736-afd-und-ein-prozent-rechtsextreme-untergraben-vertrauen-in-die-demokratie
23. Pohl and Humbs, "Die Mär von der gestohlenen Wahl", Tagesschau Investigativ, 14 January 2021, https://www.tagesschau.de/investigativ/kontraste/usa-afd-wahlbetrug-101.html
24. E.g., DFRLab, "Lisa 2.0: How pro-Kremlin media in Germany have been using a new fake to justify an old one", 11 March 2017, https://medium.com/@DFRLab/lisa-2-0-133d44e8acc7

- Clumsy communication by the authorities or journalists. A study by SNV in connection with the last federal elections found that successful disinformation often took advantage of poor communication;[25]
- Disinformation campaigns that react quickly to unexpected sudden events (for example, the fire at Notre Dame Cathedral in Paris); and
- Cyberattacks on authorities or (online) meetings (for example, the CDU party conference in January 2021) also contain an aspect of disinformation. They spread a sense of threat and confusion, with the aim of weakening trust in democratic processes.

Foreign interference

Russia is regularly mentioned as the most important foreign actor with regard to disinformation in Germany and, according to the findings of the European External Action Service, Germany is the main target of Russian disinformation campaigns in Europe.[26] Accordingly, since the end of 2015, more than 700 cases have been registered of Russian media spreading misinformation about Germany, albeit frequently aimed at the Russian public, while Russian channels in Germany, e.g., RT, tend to avoid obvious fabrications. China is also increasingly mentioned in this context.

Basically, however, it can be expected that disinformation by actors within Germany will have a greater impact. Attributing disinformation campaigns to foreign actors should be done carefully, so as not to represent these actors as more important or powerful than they are.

In the run-up to the elections, the following risks exist:

- Generally, there is wider geopolitical interest in Germany's political orientation after the end of the Merkel era. This interest can also manifest itself in an attempt to weaken key political actors and/or institutions;
- It is possible that data discovered during past or future hacking attacks (or phishing attacks) on the German parliament or authorities may be published at strategic moments (e.g., shortly before the elections), with the intention of influencing the campaign, public opinion and, ultimately, the outcome;
- These findings may also be used for the publication of personal data or to influence candidates ("doxing"). This leads to, among other things, feelings of insecurity and vulnerability among affected candidates, who might modify their behaviour as a result. The public perception of those affected may also be damaged; and
- Disinformation for specific target groups with immigration backgrounds. In this context, a motion with regard to the protection of the 2021 federal elections by the FDP parliamentary group[27] mentions especially the interaction between foreign television channels, such as RT Deutsch and online disinformation, or the role of the Turkish foreign channel TRT.4.

25. Sängerlaub, Meier and Rühl, "Fakten statt Fakes. Verursacher, Verbreitungswege und Wirkungen von Fake News im Bundestagswahlkampf 2017", Stiftung Neue Verantwortung, 26 March 2018, https://www.stiftung-nv.de/de/publikation/fakten-statt-fakes-verursacher-verbreitungswege-und-wirkungen-von-fake-news-im
26. EuvsDisinfo, "Vilifying Germany; wooing Germany", 9 March 2021, https://euvsdisinfo.eu/villifying-germany-wooing-germany/
27. Deutscher Bundestag, "Antrag der Abgeordneten und der Fraktion der FDP", Drucksache 19/28743, 20 April 2021, https://dip21.bundestag.de/dip21/btd/19/287/1928743.pdf

4. Recommendations for action to minimize risks during the 2021 federal elections

Political online advertising

- As a general principle, the GDPR must be fully implemented, as it also prohibits political advertisers from using especially problematic targeting practices with the aid of personal data.
- Online platforms that sell political advertisements must monitor compliance with their own standards, as well as with the relevant laws.
- The definition and identification of political advertising must take into account not only the providers' established formats, but also any paid-for content. This also applies to influencers.
- Online platforms that offer political advertising must maintain comprehensive, detailed archives of advertisements, with immediate public access. These archives must be easily searchable and also provide interfaces for systematic research, including extensive, detailed data on the targeting and display criteria (detailed recommendations have been submitted by SNV).[28]
- Media and civil society organizations could make available browser extensions to users for collecting political advertising and comparing this to data from archives (for the 2021 federal elections, for instance, the television programme ZDF-Magazin Royale is providing these in cooperation with the initiative "Who Targets Me").[29]
- The political parties could commit themselves to act responsibly and transparently when buying online advertising, with the help of a code of conduct. In the Netherlands, many parties and platforms signed a code of conduct for greater transparency in political online advertising in the run-up to the 17 March 2021parliamentary elections.[30]

Online hate speech and illegal content

- The providers of online platforms must implement their own standards carefully and comprehensively. Where appropriate, this also applies to obligations arising from the NetzDG, and also with regard to the improved user-friendliness of the reporting channels for complaints about illegal content that were adopted in May 2021.[31] In addition to deleting certain content, the focus should be on questions of ranking. Hate speech is a highly emotional issue that, as a rule, quickly gives rise to many reactions that, in turn, can lead to algorithms giving a higher rating to such content in the timelines of users or in recommendations.

28. Jaursch, "Regeln für faire digitale Wahlkämpfe", op. cit., note 15
29. See: https://whotargets.me/de/
30. International IDEA, "First National Code of Conduct on Online Political Advertising in the European Union Signed by Dutch Political Parties and Global Online Platforms", 9 February 2021, https://www.idea.int/news-media/news/first-national-code-conduct-online-political-advertising-european-union-signed-dutch
31. Die Bundesregierung, "Änderung des Netzwerkdurchsetzungsgesetzes: Gezielte Bekämpfung von Hasskriminalität", 6 May 2021, https://www.bundesregierung.de/breg-de/suche/bekaempfung-hasskriminalitaet-1738150.

- The Federal Ministry of Justice should interpret Article 1 of the NetzDG according to both the wording and the intent and purpose of the law, and apply the law also to services that, with regard to their form, present themselves as private messenger services but are actually, at least in part, social networks. This should be examined in connection with the service Telegram, where publicly accessible groups with up to 200,000 participants can form.[32]

- Awareness must be raised among policymakers and authorities of the destructive effects hate speech has on political participation.

Disinformation

Disinformation can be illegal (if, for instance, it is defamatory), but there is no general prohibition against lying. The short-term minimization of risks in this area should, therefore, focus especially on aspects of transparency and on fact-checking, even though these are often far less visible than the disinformation they are concerned with. A special focus should be on the automatic spread of news by platforms whose algorithms interpret users' initial interest (disinformation can be exciting) as a signal prompting them to display this news in a prominent position (ranking). Opportunities for action included the following:

- Systematic efforts by social media platforms to identify disinformation and ensure that distribution algorithms assign a lower ranking to such content. This also includes proactive cooperation with civil society organizations and other experts concerned with the related challenges. Ideally, a direct working relationship should be established, in order to communicate current developments rapidly;

- Standards for self-regulation should be applied in a consistent manner, in specific cases including the deletion of accounts. These steps must be taken in a transparent way, so that those affected have recourse to complaints and legal procedures (see NetzDG);

- Social media platforms could adjust their designs to identify disinformation and to stop or slow its distribution;

- The ad hoc rules implemented by the platforms, e.g., during the United States presidential election in 2020, for election-related content must be clearly defined and published in a way that users can comprehend;

- Authorities and the media must review their public communication, especially during the election year, in order to ensure that statements and articles cannot be misunderstood. For instance, media should clearly identify the age of their online articles (e.g., "this article is more than 6 months old"), in order to prevent older information being spread as current news or "scandals" (theguardian.com, for example, applies this in an exemplary manner); and

- Authorities, and especially those involved in organizing and administering the elections, must communicate comprehensively and proactively, especially on social media. In this respect, there is still a lot to be done.[33] While official information on the federal elections is displayed on social-media platforms, the visibility of trustworthy sources should generally be increased on these.

32. Laufer, "Fällt Telegram wirklich nicht unter das NetzDG?", Netzpolitik.org, 4 February 2021, https://netzpolitik.org/2021/hasskriminalitaet-faellt-telegram-wirklich-nicht-unter-das-netzdg/
33. The Federal Returning Officer maintains social media profiles but, so far, these seem to have only a limited reach (in mid-May 2021, there were just over 9,000 followers indicated for @Wahlleiter_Bund on Twitter, and just under 200 subscribers on Instagram).

Foreign interference:

The short-term minimization of risks in this area of activity will likely be difficult, but still possible:

- The creation of awareness among potentially affected officials, as well as institutions and organizations that are relevant for the elections, must continue and be intensified. This could be done, for example, by the Federal Office for Information Security. Political parties, in particular, should also extend their measures with regard to the participation of campaign volunteers.

- Parties could make a commitment to refrain from any systematic use of personal data resulting from doxing or leaks during the election campaign.

- Trust in media continues to be high among the German public. Reporting on disinformation campaigns should aim to ensure wide-ranging public awareness of such practices.

5. Long-term recommendations for action and challenges

Solutions to many of the problems addressed require medium- and long-term strategies, either with the aim of developing and implementing regulations and evaluating their impact, or in order to increase resilience in society, e.g., through political education and increasing digital media literacy. The starting-points for these measures are:

- During the next parliamentary term, the legal framework for party and campaign financing should be systematically adapted to the realities of today. A commission for the future of digital elections could encourage the development of regulations and raise awareness of already existing laws.

- With regard to long-term solutions, the European Commission has presented different kinds of regulatory frameworks for curbing or preventing disinformation on the internet. Many of the organisations participating in the roundtable discussions have presented statements on this matter.

- A number of formats and platforms have not to date received adequate attention from political decision-makers. Live video can reach a large audience at the time of broadcasting, so many of the proposed measures would no longer be effective in such instances. In this respect, we have seen the more advanced media activity and infrastructure, including in real-time communication, on the part of an active conspiratorial online community that continues to grow, most recently in the phenomenon of so-called lateral thinkers ("Querdenker"[34]) protests. In this context, the possibility of monetizing deliberately misleading content, for instance on YouTube, should be addressed and, following the relevant classification of content, be precluded. Advertisers should request that their advertisements not be shown immediately before videos spreading disinformation. With regard to its growing usage numbers, there should also be a greater focus on TikTok.

Precisely because digital communication, including social media, and the accompanying risks for the democratic process based on its ability to shape public opinion and policies, are highly dynamic developments, the associated problematic aspects must be monitored and addressed on an ongoing basis. Democracy Reporting International's approach is to facilitate exchange among regulatory authorities and scientific institutions, civil society initiatives and commercial platforms, in order to identify risks at an early stage and to address these in a cooperative way. The round tables and the present evaluation form the basis for this ongoing process during the 2021 federal elections and beyond.

34. Fürstenau, „Meet Germany's 'Querdenker' COVID Protest Movement", DW, 03 April 2021, https://www.dw.com/en/meet-germanys-querdenker-covid-protest-movement/a-57049985