Alliance of Democracies

ELECTION RISK MONITOR

German Federal Election 2021

Authors
Olaf Böhnke
Carlo Zensus

Disclaimer

This report is written by Olaf Böhnke and Carlo Zensus. It was published by The Alliance of Democracies Foundation in November 2021 as a contribution to the continuous work of the Foundation, including the activities of the Transatlantic Commission on Election Integrity (TCEI) and its objective to highlight the global threat of foreign election interference and protect the integrity of democratic elections. The report and its recommendations solely reflect the opinions of the authors.

About the authors

Olaf Böhnke is the Berlin Director of the Alliance of Democracies Foundation (AoD) and Senior Advisor to AoD's Transatlantic Commission on Election Integrity (TCEI). He is focused on the global threat of election interference and how digital technology is challenging our democratic societies and has worked for many years in leading positions in the German Bundestag. He is the former director of the ECFR office in Berlin as well as the founding Executive Manager of the European China Policy Unit at the Mercator Institute for China Studies (MERICS). He was an associate fellow at the German Council on Foreign Relations (DGAP) and a visiting professor for political sciences at the Free University of Berlin.

Carlo Zensus is an Election Integrity Project Associate at the Alliance of Democracies Foundation. He holds a LLM in Law and Politics of International Security from the Vrije Universiteit Amsterdam and a MSc in Crisis Management from Leiden University. He joined the TCEI Germany Project passionate about ensuring that the 2021 German federal elections remained fair and free from malign interference. He gained his professional experience from working with the German Marshall Fund of the United States, the Hague Centre for Strategic Studies, the Dutch Ministry of Defence, and most recently the Delegation of the European Union to the United Nations in Vienna.

Acknowledgements

The authors would like to thank the numerous non-governmental organizations, foundations and think tanks who contributed to the successful launch of our engagement during the 2021 elections in Germany, especially Microsoft Germany, Alfred Herrhausen Gesellschaft, Twitter Germany, NewsGuard and Democracy Reporting International.

Finally, we would like to express our appreciation to all candidates across the political aisle, who supported our engagement during the 2021 elections and signed the election pledge.

Impressum

Election Risk Monitor: Germany 2021
Authors: Olaf Boehnke, Carlo Zensus
Design: Danielle Piatkiewicz

Table of Contents

Introduction

After 16 years in power, the end of Angela Merkel's chancellorship gave a special significance to the 20th Bundestag election, which took place on 26. September 2021. As this was the first time that no incumbent head of government stood for re-election, it was anticipated in advance that this election could have a major impact not only on the country's future domestic policy, but also on its international standing as the largest member state of the EU and the fourth-largest economy in the world.

Although Berlin had seen one of the gravest foreign cyberattacks in Europe on its federal parliament in 2015, issues such as foreign influence operations or disinformation campaigns have not received much attention in the broader political debate for a long time. But with the COVID-19 pandemic, mis- and disinformation activities became a wide-spread problem of growing concern for German authorities and civilian watchdog organizations alike.

Against this backdrop, the German election in 2021 took place in a year of heightened political tensions that focused predominantly on two topics: First, the ongoing COVID-19 pandemic, which was accompanied by a continued emotional debate about the resulting restrictions of personal liberties.

> “ The increasingly radical “Querdenker” movement can be identified as a driving force behind wide-spread disinformation. ”

At the same time, Germany had seen a no less emotional debate on how to combat the ongoing climate crisis, which was further intensified by devastating floods in western parts of Germany in July 2021 that killed 184 people. This debate was also characterized by a high degree of mis- and disinformation.

Due to the pandemic, much of the electoral campaign shifted to the digital space, which is why all political parties and their candidates significantly expanded their presence and interactions with voters on social media and the internet compared to previous elections. Finally, the entire election campaign period was characterized by an open and dynamic, political race, with polls predicting very different coalition constellations over the months leading up to Election Day.

All these ingredients represented an ideally suited opportunity for foreign and domestic actors to influence public opinion and sow mistrust and division within the electorate during the 2021 federal election. However, such malign meddling attempts not only attack state institutions and politicians, but also threaten the universal right of all citizens to participate freely and independently in their democratic elections. Although attempts by malign actors to interfere in democratic elections have long been known and well documented by many experts, it is important to bring these facts and findings also to the attention of a wider population in an understandable way. Our engagement during the 2021 federal election in general and this Election Risk Monitor in particular is a contribution to these efforts.

Key Observations

Germany continues to be a prime target of election interference operations conducted by foreign adversaries in 2021. Even though no disinformation or cyber operation resulted in a significant altering of the election process or result, numerous attempts were made by foreign and domestic actors. Despite this, instead of a short-term impact, these attempts seek to undermine the long-term trust of citizens in the legitimacy of their democratic election and sow distrust in politicians and governmental institutions. Such interference attempts will not cease to be aimed at Germany in the future, making a comprehensive and whole-of-government approach to defend against such malign meddling indispensable.

Disinformation

In the run up to the German Federal Election in 2021, we saw a dramatic increase in false narratives and disinformation being spread across social media platforms, originating from both domestic and foreign actors. Domestic disinformation networks were also responsible for much of the false news spread during the election.

When it comes to foreign disinformation activities, Russian state-run media outlet "RT DE" (Russia Today Germany) and social media accounts linked to Russian operatives played a vital role throughout the election cycle. Common narratives related to Covid-19, vaccination, mail-in ballots, as well as specific false narratives about respective candidates, in particular Green party frontrunner Annalena Baerbock. These narratives tapped into widely held assumptions about a candidate or party, and fueled misconceptions about respective policy positions.

At times, mainstream media picked up such false reports in their own reporting, too, thus unintentionally increasing the reach and spread of political disinformation. In particular, the leading candidates of the Green Party and the CDU became targets of false and misleading narratives during the election campaign, which impaired their ability to convey their political positions in an unbiased manner.

Cybersecurity

The actual voting process in Germany is completely conducted in a non-electronic way, i.e., no vote is casted digitally. The voting is therefore not dependent on IT security and is not susceptible to electronic manipulation. Consequently, no penetration of voting systems or the transmission of election results to the Federal Returning Officer were reported. Nonetheless, over the course of 2021 and throughout the election cycle, several cyber intrusions were conducted, targeting in particular parties, individual members of various parliaments (Bundestag and state parliaments), and even the office of the Federal Returning Officer.

- In January 2021, hackers attempted to infiltrate the political convention of the Christian Democratic Union (CDU), at which the new party leader was to be elected.
- In September 2021, the Federal Statistical Office of Germany, which is home to the Federal Returning Officer, was targeted by a cyberattack.

- Throughout 2021, at least three hacking attempts were registered by German authorities which targeted parliamentarians from the federal as well as several state parliaments.

In light of these developments, on 24 September 2021, two days ahead of the election, the European Union took drastic action and publicly attributed these and other cyber influence operations to the Russian government and called them out for their malign interference in elections of EU member states.

Disinformation

When speaking about disinformation in this report, we mean “*the fabrication or deliberate distortion of news content aimed at deceiving an audience, polluting the information space to obscure fact-based reality, and manufacturing misleading narratives about key events or issues to manipulate public opinion.*”[1]

In general, it can be observed that online communication significantly alters the way people interact with each other: communication becomes faster, non-stop, and more direct. Moreover, traditional gatekeepers of information such as journalists - who vet information regarding its truthfulness, accuracy, and credibility - disappear, leaving no distinction between sender and receiver of a respective piece of information. In other words, everything can be shared, with everyone, by anyone - a paradigm shift for political communication in democracies which has not only led to a welcome de-hierarchization and pluralization of the political debate, but at the same time represents a major gateway for disinformation and manipulated media content into the digital information ecosystem.

Throughout the election cycle, the German government appeared to be well aware of the danger of targeted attempts to influence public opinion through political disinformation campaigns and made efforts to comprehensively protect the electoral vote.[2] To date, however, there is no central body in Germany responsible for detecting and debunking online disinformation, and therefore various state institutions have been involved in efforts to combat the spread of disinformation in the past. For the 2021 federal election, the *Bundeswahlleiter* (Federal Returning Officer) was in charge and coordinated all efforts, which included a dedicated website that continuously listed false reports about the election spread on social media in real time for the press and interested citizens.[3]

> “Striking to the 2021 Federal Election when compared to previous elections was the reliance of political parties on social media as the primary vehicle of political interaction with the electorate due to the omnipresent COVID-pandemic.”

[1] EUvsDisinfo, “Election Meddling and Pro-Kremlin Disinformation”, 2019, https://bit.ly/3meTdkd

[2] Die Bundesregierung, "Bundestagswahl 2021 - Mögliche illegitime Einflussversuche fremder Staaten - Fragen und Antworten", https://bit.ly/3HNgTrI

[3] Der Bundestagswahlleiter, "Erkennen und Bekämpfen von Desinformation", https://bit.ly/3nHGydw

Meanwhile, most social media platforms continued their practice of labeling or content moderation against the spread of disinformation during the election and also increased their cooperation with fact-checkers and watchdog groups to this end.

Domestic Disinformation

Disinformation spread by domestic actors represented a worrisome aspect of the election cycle in 2021. Clearly attributing disinformation on the Internet is often difficult. In addition to political activists of all political stripes who use their own, affiliated or fictitious social media accounts to spread misleading and false narratives, organized right-wing networks, often strongly associated with the AFD, conspiracy theorists, but increasingly also average citizens have discovered social media platforms as their virtual megaphone. Similar to foreign disinformation campaigns, the narratives used by domestic actors during the 2021 election were: the Covid-pandemic, vaccinations, mail-in voting, the floods in western Germany, and ad hoc topics relevant to the various political election campaigns, such as speed limits on German highways or accusations of plagiarism by some of the candidates. Of the disinformation narratives analysed by watchdog organization Avaaz 46% targeted the Greens, 32% CDU/CSU, and 18% SPD, amounting to 96% of all disinformation spread throughout the election cycle.[4]

> “Of all politicians affected by disinformation, the Green Party's top candidate Annalena Baerbock received the most attention from domestic actors, at 25%.[5] ”

One narrative spread about the Green candidate referred to her alleged association with George Soros.[6] To support this claim, a picture Baerbock took with Soros at the Munich Security Conference in 2019 was spread across social media accompanied by highly false context. An additional narrative argued that Baerbock sought to restrict keeping pets in order to save CO2.[7] This example clearly shows how contentious topics such as climate change, but also antisemitic narratives, are used as a vehicle to defame a respective candidate.

A typical tactic used to mislead the public about the Green Party's policy positions was to deliberately exaggerate claims about climate change to such an extent that they gave the impression that the party wanted to ban basically everything, such as meat consumption, cars, or flights for private travel. While the party did call for behavioral changes throughout the election, the above allegations created completely misleading and false narratives. Other narratives spread about Baerbock included her alleged call for the abolishment of the widow's pension, as well as claims that she lied about her resume. Sexist narratives came on top. After she announced her candidacy a photoshopped picture spread across social media which allegedly showed Baerbock modelling naked for a photo

[4] Avaaz, "Deutschlands Desinformations-Dilemma 2021",
[5] Ibid.

[6] Correctiv, "Schmutziger Wahlkampf - Wie Desinformation die Bundestagswahl vergiftet", https://bit.ly/3DHALdv

shoot.[8] While the attribution of specific posts to their original source is often difficult, it nonetheless is apparent that the Greens were in particular targeted by right-wing networks. Research done by DER SPIEGEL analyzed nearly one million Facebook posts associated with right-wing and conspiracy theorist networks, of which 1535 posts included potentially illegal hate speech aimed against the Greens. In comparison, of the posts analysed, only 265 targeted the CDU, and 174 the SPD.[9]

The efficiency of spreading such simplistic narratives about a particular candidate is all the greater if they confirm long-held assumptions citizens have about a candidate, even if they later find out they are not true. It is not always clear who spread the disinformation about Baerbock. However, research has proven that many authors of such posts are average citizens who reject the idea of a government led by a Green chancellor Baerbock for ideological or sexist reasons.

The CDU, led by Armin Laschet, was also significantly targeted by disinformation and misleading narratives. As State Minister of North Rhine-Westphalia he was primarily responsible for responding to the devastating flooding in West Germany. Quickly, false narratives about his role in the flooding circulated, ranging from him diverting donations made to the victims of the flood to a foundation, of which his wife is the patron, to then be used for his own campaign. Similarly, it was suggested in several social media posts that he actually didn't visit the regions affected most by the flooding. Both narratives were proven false. Similar to Baerbock, claims arose during the election campaign that Laschet plagiarised parts of his book "Die Aufsteiger-Republik", written in 2009. Following these revelations several small Telegram Groups appear to have organised a coordinated approach to spread hashtags which implied that Laschet is a liar. The goal of these efforts was to promote hashtags on Twitter in order to create trends. [10]

> “ But not only parties and candidates were in the crosshairs of disinformation activities. The credibility of the actual election itself was also called into question - similar to what was already observed in the USA in 2020. ”

Especially right-wing extremist networks such as "*1 Prozent*” (1 Percent) and the AFD were already casting doubt on the legitimacy of the postal vote in the spring of 2021 and questioned the trustworthiness of the actual voting process and the results even before election day. The state election in Saxony-Anhalt on June 6, 2021, served as a test case for the federal election, where allegations of election fraud spread massively on Twitter after Election Day. [11] Over 2.6 million Twitter users saw the hashtag *#Wahlbetrug* (election fraud) after the election. Throughout the federal election campaign, social media was abuzz

[8] Ibid.

[9] SPIEGELONLINE, "Im Visier der Hetzer", 23.7.20 21, https://bit.ly/3cJUHQY

[10] Correctiv, "Schmutziger Wahlkampf“

[11] Institute for Strategic Dialogue, "Desinformations-kampagnen gegen die Wahl: Befunde aus Sachsen-Anhalt", 21.6.2021, https://www.isdglobal.org/wp-content/uploads/2021/06/Bericht-Landtagswahlen-Sachsen-Anhalt-Final.pdf

with reports alleging that absentee ballots had been falsified, particularly by politicians close to the AFD. The *Bundeswahlleiter* responded to the spread of these false reports by providing concrete evidence on its website that absentee ballots were not only properly used in past elections, but also that there is no evidence to support the claim that absentee ballots are fraudulent.

Finally, the role of traditional media in inadvertently spreading disinformation about political candidates that originated on social media was repeatedly raised as a problem during the election campaign. In a study commissioned by Avaaz, it emerged that in a ranking of media channels on which people had encountered fake news about Green frontrunner Annalena Baerbock during the election campaign saw classical television (22%) in first place, followed by mainstream media (print/online - 18%).[12] Only then came social media platforms such as Facebook (17%), WhatsApp (10%) and Telegram (5%).

> “Obviously, many newsrooms still do not seem to have developed a clear approach to their reporting on how to cover fake stories, even if they appear newsworthy, without amplifying them further.”

Foreign Disinformation

The core of foreign playbooks of election interference is primarily to deepen and exacerbate antagonisms and existing fault lines in a society by exploiting contentious and polarizing issues through the massive dissemination of disinformation or manipulated information. In 2017, the refugee crisis and Chancellor Merkel's migration policy were massively exploited for these purposes to spread false and misleading information and conspiracy theories. At the time, both domestic populists and foreign state actors deliberately used this issue because it was at the center of the political debate and represented an important and highly emotional campaign issue for many voters.

By 2021, the refugee crisis no longer had suitable momentum, although it resurfaced from time to time as a test balloon. The political momentum had all but disappeared, and instead, foreign disinformation operations focused primarily on two other issues: First, the respective candidates of the major parties were targeted, especially Baerbock of the Greens and Laschet of the CDU.
Second, Covid-19 was instrumentalized as an example of government overreach and abuse of power by bureaucrats. Having said that, the precise attribution in real time of who is behind targeted disinformation operations remains a major challenge for many observers and researchers. However, even in 2021, the bulk of disinformation and conspiracy narratives disseminated by foreign-state actors or foreign-state media appear to be attributable to the usual suspect: Russia. Chinese, Iranian or even Turkish disinformation did not play a significant role in any of the analyses and media reports evaluated. For this reason, the focus below will be on Russian

[12] Avaaz, "Deutschlands Desinformations-Dilemma 2021"

disinformation narratives during the 2021 federal election.

> “Compared to other European states, Germany remains the country in the EU most targeted by Russian disinformation and propaganda campaigns.”

For years, Germany has been a prime target of Russian disinformation activities when it comes to foreign operations. The European External Action Service identified over 700 cases of Russian disinformation since 2015.[13] In a non-public report of the German Federal Ministry of the Interior from June 2021, the Ministry warned of a significant increase of hybrid efforts aimed at undermining societal unity, trust in public institutions, and the holding of the election itself, with a particular focus being placed on Russia as the perpetrator of these efforts.[14]

In the 2021 German elections, it appeared that Russian disinformation campaigns were not structured as a component of one large-scale election interference operation, but were conducted in a more subtle and ambiguous manner over the course of several months. Following the classical Russian playbook, disinformation activities sought to continuously sow distrust of citizens and specific demographic groups towards the German government and the country's democratic structures by nurturing anti-establishment, right-extremist, populist and divisive narratives. The topics which were highlighted in Russian disinformation campaigns had a clear focus on contentious issues, which however did not necessarily have a direct link to the election itself. These topics in particular included the Covid-19 pandemic, vaccines and state-ordered restrictive measures and were focussed specifically on the "Querdenker" movement and their distinct state-critical, and partially, state-opposing attitudes.[15]

Russia’s main media outlet in Germany is RT DE (formerly Russia Today) and its network of subordinate social media accounts is vital in the distribution of such narratives, exemplified inter alia through a budget allocation of 550 million EUR for RT and Sputnik (Russia’s second state-sponsored media outlet, which was recently rebranded to SNA News) over the next four years.[16] Research on the activities of RT DE over the past months have shown that the channel's reach and engagement rates in 2021 on Facebook were much higher than those of other mainstream media outlets like BILD, Tagesschau or DER SPIEGEL, even though RT DE actually has significantly fewer followers as its media competitors.[17] One reason for this is the channel's strong focus since August 2020 on the anti-government “Querdenker” movement. In particular, RT DE's coverage of anti-COVID demonstrations received millions of views in some cases.[18]

[13] EUvsDisinfo, "Vilifying Germany; Wooing Germany", 9.3.2021, https://bit.ly/3DLSRLt

[14] Tagesspiegel, "Gezielte Diffamierung von Annalena Baerbock", 16.6.2021, https://bit.ly/30TzvG1

[15] SPIEGEL ONLINE International, "Germany Fears Influence of Russian Propaganda Channel", 03.03.2021, see: https://bit.ly/3CLytJ4

[16] EUvsDisinfo, "Vilifying Germany; Wooing Germany",

[17] EuvsDisinfo, "Figure of the Week: 100,000", 20.9.2021, https://bit.ly/3xe7fK0

[18] Avaaz, "Deutschlands Desinformations-Dilemma 2021"

Next to the political objective of dividing the German public, Russia is thereby also exploiting Facebook's algorithm to achieve an ever-increasing reach of its disinformation and propaganda. Pushing contentious topics on its social media channels is not a coincidence, as algorithmic changes made to Facebook's newsfeed resulted in divisive and controversial topics being spread more across the platform and among users, as was recently reported by the *Wall Street Journal*.[19]

When looking at the Bundestag election of 2021, of all the candidates for chancellor, Annalena Baerbock, frontrunner of the Green Party, was most strongly targeted by Russian disinformation. Due to her critical stance on the Russian gas pipeline Nord Stream 2 or Moscow's military operations in eastern Ukraine or Syria, and as a representative of a new style in German politics – female, young, and rather critical toward the Kremlin compared to centrist CDU and SPD politicians - Baerbock and the Greens were the perfect target for Russian information influence operations. Controversial political Green positions like the introduction of a speed limit, a reform of the immigration law or the demand for a fundamental energy transition were exploited by RT DE for its polarizing reporting, as well as other false claims, such as Baerbock is controlled and supported by U.S. investor and philanthropist George Soros, or the dissemination of her manipulated, fake nude picture.

Cybersecurity

Cyber disruption and cyber-attacks belong to the offensive tactics used in foreign election interference operations. The protection of elections and democratic institutions against such malicious interference by digital means is therefore of utmost importance for all democratic states. Elections over the past years have shown the vulnerability against such cyberattacks, the most famous case being the hack of the server of the Democratic Party in the run-up to the US 2016 elections.

In the context of a democratic election in the digital age, it becomes apparent that not only the critical infrastructure, such as the vote tallying and certification of results, are a potential target of cyberattacks, but also political candidates themselves, for example as targets for ransomware attacks, malware-spam, or phishing operations. Common denominator in these cases is that the perpetrators attempt to steal sensitive information and subsequently leak the stolen information to the public in an attempt to sway public opinion.

Cyber defence is therefore a vital component of the resilience against hybrid threats and subversive operations. In Germany, the *"Bundesamt für Sicherheit in der Informationstechnologie" (Federal Office for Information Security (BSI)*) is responsible for ensuring the security of critical digital infrastructure and assessing cyber threat levels to the nation. In the context of the federal election,

[19] Wall Street Journal, "The Facebook Files", 1.10.2021, https://on.wsj.com/3oVP3RB

the BSI worked closely with the Bundeswahlleiter and institutions on the state level to provide adequate cyber protection throughout the election cycle. For the federal election, it is important to reiterate that actual voting is done with pen and paper, no votes are cast digitally.[20] The vote is therefore not dependent on IT security and is not susceptible to manipulation.

When assessing the cybersecurity threats to the 2021 Federal Election, we can state from the outset that no penetration of the voting systems and the transmission of election results to the Federal Returning Officer occurred. When asked whether cyberattacks had any effect on the election, Horst Seehofer, Minister of the Interior, pointedly said "none".[21]

> “Over the course of 2021 and throughout the election cycle several cyber intrusions were conducted, targeting in particular parties, politicians, and the office of the Federal Returning Officer.”

In January 2021, it became known that hackers tried to infiltrate the political convention of the CDU, at which the new party leader was to be elected.[22] Through several Distributed Denial of Service (DDos) attacks, the perpetrators were able to successfully shut down the homepage of the CDU and the live stream of the convention. However, in preparation of such intrusions the CDU had set up the digital infrastructure through which the delegates were able to cast their votes on a separate system, thereby denying the perpetrators access. According to the CDU the hack was traced back to Russia.[23]

In June 2021, it was reported that several cyberattacks were detected which targeted German non-governmental organisations and political think tanks.[24] According to the Federal Ministry of the Interior, these attacks were also attributed to the Russian State. Through brute-force-attacks, in which an attacker submits many passwords with the hope of eventually guessing the correct password, the perpetrators attempted to gain access to sensitive information of the respective organisations. The Interior Ministry spoke of a "serious threat" in the context of the German Federal Election.

Shortly before the election in September 2021, the Federal Statistical Office of Germany, in which the office of the Federal Returning Officer is located, was targeted through a cyberattack.[25] According to the Ministry of Interior, the servers of the Federal Returning Officer were not directly affected, allowing the election to take place as planned. In August 2021, an additional cyberattack targeted the website of the Federal Returning Officer, rendering it unreachable for a few minutes.

Throughout 2021 at least three hacking attempts were registered by German authorities which targeted parliamentarians, both in the German Bundestag as well as the state parliaments

[20] Bundeswahlleiter, "Informationen zur Sicherheit der Wahl", https://bit.ly/32h8uMX

[21] Stuttgarter Nachrichten, "Wer am stärksten unter Cyberangriffen leidet", 21.10.2021, https://bit.ly/3cFQfTp

[22] SPIEGEL, "CDU meldet Hackerangriffe auf Parteitag", 16.01.2021, https://bit.ly/30PgYe7

[23] RND, "Hackerangriff auf CDU-Parteitag womöglich aus Russland", 21.01.2021, https://bit.ly/3DLU4lZ

[24] Tagesschau, "Vermehrte Cyberattacken aus Russland", 15.06.2021, https://bit.ly/3CLzFvS

[25] MDR, 'Ministerium: Wahlserver nicht von Cyberangriff betroffen", 24.9.2021, https://bit.ly/3HNjLF0

(Landtage).[26] In particular parliamentarians of the CDU/CSU and the SPD were targeted through phishing emails, thereby attempting to gain access to personal information, in order to subsequently release the information to the public as part of wider hack and leak operations. Some attacks were successful and infiltrated the systems of respective parliamentarians. [27] According to German security authorities, the hacker collective known as "*Ghostwriters*" were behind the attacks, which is commonly associated with the Russian GRU. [28] Consequently, the German government urged Russia immediately to suspend any cyber operations targeting German parliamentarians ahead of the federal election.

A spokesperson of the German Ministry of Foreign Affairs publicly stated that "the German government has reliable evidence on the basis of which the 'ghostwriter' activities can be attributed to cyber actors of the Russian State and specifically to the Russian military intelligence service GRU."[29] On September 9th, the Public Prosecutor General furthermore initiated an official investigation into the cyberattacks against German parliamentarians. [30] This move is particularly telling as in 2020 the Public Prosecutor General issued an arrest warrant against a suspected cyber spy from Russia for the hack of the German Bundestag in 2015.[31]

In light of these developments, on the 24th of September, two days before the election, the European Union took drastic action and publicly called out the Russian government for its malign interference in the elections of EU member states.

In its press release the High Representative on behalf of the European Union stated that "some EU member states have observed malicious cyber activities, collectively designated as Ghostwriter, and associated these with the Russian State. Such activities are unacceptable as they seek to threaten our integrity and security, democratic values and principles and the core functioning of our democracies." It furthermore argued that "these activities are contrary to the norms of responsible State behaviour in cyberspace as endorsed by all UN member states, and attempt to undermine our democratic institutions and processes, including by enabling disinformation and information manipulation."

This announcement, which publicly named and shamed Russia for its actions, can be seen as a wider shift in strategy on how to react to malicious cyberattacks by foreign actors who attempt to undermine the integrity of democratic elections. This summer the German government established a new process in order to faster detect and attribute cyberattacks.[32] Part of this new strategy is to coordinate a collective effort of different German authorities responsible for protecting against cyberattacks, including the *Bundesamt für Verfassungsschutz* (Federal Office for the Protection of the Constitution), the *Bundesnachrichtendienst* (Federal Intelligence Service), and the *Militärischer Abschirmdienst* (Military Counterintelligence Service). The *Auswärtiges Amt* (Federal Foreign Office) is the coordinating institution and possesses the

[26] Tagesschau, "Bundesregierung kritisiert Russland scharf", 06.09.2021, https://bit.ly/3xhpH4e

[27] Tagesschau, "Verfahren wegen Hackerattacken", 9.9.2021, https://bit.ly/3CK3MUI

[28] SPIEGEL, "Generalbundesanwalt ermittelt gegen Putins Hacker", 9.9.2021, https://bit.ly/3xfyfZE

[29] Tagesschau, "Verfahren wegen Hackerattacken"

[30] Frankfurter Rundschau, "Cyberangriffe auf Bundestagswahl", 24.09.2021, https://bit.ly/3nJCPMl

[31] Tagesschau, "Bundesregierung will Zuordnung von Tätern", 07.10.2021, https://bit.ly/3oYiCSm

[32] Ibid.

authority to publicly attribute a respective cyberattack to a foreign government. While the detection and attribution of cyberattacks did already occur in the past, the responsible German authorities often worked alone and did not engage in sufficient cooperation and exchange of intelligence. While the attribution of cyberattacks to respective actors remains difficult, progress has been made over the last years, for example through enhanced methods to monitor server structures, analysing attack patterns and assessing the malware used. In conjunction with the public call by Germany and the EU for Russia to halt any interference in elections of EU member states, this strategy is a new diplomatic measure by democratic countries to respond and deter election interferences in the future.

Pledge for Election Integrity

As outlined throughout this report, elections during the digital age are particularly vulnerable to foreign and domestic interference. A lack of detailed legislation on what is allowed in digital election campaigning only further exacerbates this issue.

In Germany, there are few detailed reporting requirements for parties in relation to online advertising, and there is a lack of public campaign oversight and clear legal obligations for platforms, for example in regard to labelling requirements for advertisements and possible disinformation. Compared to an analog campaign, where clear transparency rules exist for television and radio advertising, digital elections in Germany are not regulated to an equivalent degree. But since digital campaigns are often based on the use of social media platforms, most of the regulations on what is permissible in the digital sphere therefore arise primarily from the platform providers' terms and conditions.

> “In the absence of legal regulations, voluntary commitments such as the TCEI “Pledge for Election Integrity” are therefore of particular importance in ensuring that parliamentarians and candidates for office adhere to common standards for digital campaigning.”

In the absence of clear regulation, voluntary commitments by parties send at least a positive signal to the public that those responsible are committed to a fair election campaign.

In the run-up to the Bundestag elections, there were increased efforts among the major German parties to agree on a common code for digital election campaigns. However, similar to the 2017 election, the parties were unable to agree on a common set of rules. For this reason, apart from the Alternative for Germany (AFD) and the Christian Social Union (CSU), all parties published

their own code of conduct in the beginning of their election campaigns.[33] [34] [35] [36] [37]

In support of a fair and transparent election, the Transatlantic Commission on Election Integrity (TCEI) therefore decided to launch its “Pledge for Election Integrity” during the German Federal Election in 2021. Since its first implementation during the European elections in 2019, the TCEI Election Pledge has evolved into a global standard for a healthy electoral process in the digital age. Aimed at parliamentary candidates who stand at the frontline of protecting democracies, the pledge is an effort to ensure the integrity of the election by setting out clear guidelines on how to run a fair and transparent digital election campaign.

Following an outreach campaign by our Berlin office, the TCEI Pledge was signed by a total of 144 politicians. Broken down per party, the pledge was signed by 49 politicians of the Green Party, 41 of the Social Democratic Party (SPD), 29 of the Free Democratic Party (FDP), 15 of the Left Party, 7 of the CDU/CSU, and 3 of the AFD.

The TCEI “Pledge for Election Integrity”

As political parties and candidates seeking office, we will not aid and abet those who seek to undermine democracy.

In particular, by signing this pledge we commit to:

- *Not fabricate, use or spread falsified, fabricated, doxed or stolen data or materials for disinformation or propaganda purposes;*
- *Avoid the dissemination of doctored media that impersonate other candidates, including deep-fake videos;*
- *Make transparent the use of any coordinated network activity to disseminate messages; avoid using such networks to attack opponents and other electoral stakeholders, or coordinate third-parties, proxies or fake accounts to undertake these actions;*
- *Take active steps to maintain good cyber hygiene, such as regular cybersecurity checks and password protection, and train campaign staff in media literacy and risk awareness, in order to recognize and prevent attacks;*
- *Transparency in foreign and domestic sources of campaign financing, including online political advertising purchases, in an effort to maximize public trust in the electoral process.*

[33] Bündnis 90/Die Grünen, "Selbstverpflichtung für einen fairen Bundestagswahlkampf", https://bit.ly/3xhHVCS

[34] CDU, "Wie wir Wahlkampf machen", https://bit.ly/3xhqh1U

[35] SPD Parteivorstand, "Acht Punkte für Fairness im digitalen Wahlkampf"

[36] FDP, "Beschluss des Präsidiums: Leitlinien der Freien Demokraten für einen fairen Wahlkampf", https://bit.ly/32mVDZD

[37] Bundeszentrale für Politische Bildung, "Selbstverpflichtungen für einen fairen digitalen Wahlkampf"

Calls for a comprehensive self-commitment were furthermore issued by *D64*[38], a think tank affiliated with the SPD, and *Campaign Watch*[39], a coalition of more than 20 civil society organizations initiated by Reset. When evaluating the specific components of digital election campaigns, it becomes obvious that although most parties are trying to define their own rules for digital advertising, there is plenty of room for improvement. Promising in this regard is that all parties believe that national or even European reforms are needed for digital campaigning.

For the German election in 2021, all major parties pledged not to spread disinformation intentionally and knowingly. The issue of non-transparent micro-targeting remained unanswered by the parties, as none of the major German parties explicitly committed to refrain from micro-targeting. Some self-commitments did mention the method of micro-targeting in online political advertising. But in most cases, the self-imposed restrictions on this were so vaguely worded that they were unlikely to have led to greater transparency in practice. Regarding the first commitment of the “Pledge for Election Integrity", namely "not to fabricate, use or disseminate falsified, fabricated, pixelated or stolen data or materials for disinformation or propaganda purposes," all parties committed not to engage in such practices and furthermore verified the accuracy of all posts published on their social media channels. The second commitment, "to avoid the dissemination of manipulated media impersonating other candidates," is also noted in the self-commitments of all parties. Only the SPD explicitly stated to prevent the use of deepfake videos.

All parties also pledged not to use fake profiles to spread messages, which is reflected in the third commitment of the TCEI Election Pledge. In general, automated bots are used by all major political parties to interact with potential voters; however, the parties committed not to use bots to disseminate manipulative messages. Another commitment in the pledge is to "take active steps to maintain good cyber hygiene, such as regular cybersecurity and password protection reviews, and train campaign staff in media literacy and risk awareness to detect and prevent attacks." All parties recognized the importance of this aspect, with the Greens, CDU/CSU, FDP and the Left Party organizing regular training for campaign staff ahead of the election, while the SPD did provide candidates and campaign staff with a written guide on digital campaigning security. None of the parties provided an independently audited overview disclosing the sources of their online campaign funding. This aspect of digital campaigning is reflected in the fifth commitment of the Election Integrity Pledge, which calls for "transparency regarding foreign and domestic sources of campaign financing, including the purchase of online political advertising."

While the voluntary commitments of the individual parties as well as the pledges developed by civil society are a good starting point to ensure a fair digital election campaign free of malicious interference, comprehensive legislation on this issue is indispensable. To ensure a fair and transparent digital election campaign legal regulations should be developed by the new government that cover the digital election campaign in its entirety, including possible sanctions for unfair behaviour.

[38] D64 Zentrum für Digitalen Fortschritt, "Code of Conduct für digitales Campaigning", April 2021

[39] Campaign Watch, "Leitfaden für Digitale Demokratien", see: https://campaign-watch.de

Conclusions

Germany remains a prime target for election interference by malicious actors seeking to permanently undermine the integrity of German democracy. Throughout the election year in 2021, we observed a significant level of political disinformation activities ("Grundrauschen") as well as an increased number of cyberattacks on parliamentarians and government institutions.

> After a thorough evaluation of all relevant reports and studies, it can be concluded that none of these influence activities - neither in the area of disinformation nor in the area of cyberattacks - had an outcome-changing effect on the Bundestag election.

On the one hand, the federal government has made significant efforts to strengthen the security and integrity of the federal elections. In particular, the Federal Reporting Officer set up a highly efficient system of intra-government cooperation and involved all key institutions at an early stage. Furthermore, he as well as the minister of the interior ensured a high degree of transparency, inter alia through joint press events with the heads of the Federal Office for Information Security, the Federal Police and German intelligence services.

In addition, numerous information events, manuals, and workshops for candidates by the parties themselves, the BSI, tech companies, civil society organizations and think tanks - reinforced by extensive and high-quality media coverage - also contributed significantly to the protection of the integrity of the Bundestag election. In conclusion, Germany remains politically moderate after the 2021 elections, also because its society is less polarized in comparison to other democracies. This is potentially the reason that many disinformation and conspiracy narratives do not seem to have achieved a mass impact - not even during the hot phase of the election campaign. Furthermore, Germany's media environment can be considered as healthy, balanced by trusted public sector Radio and TV broadcasters. Nevertheless, some traditional media outlets - as well as some of the political parties - urgently need to think about better ways of dealing with distorted or false information after the election.

> It is important, especially for the next four years of the new federal government and the new Bundestag, to keep a close eye on that part of Germany's society that already held strong anti-government and anti-democratic statements before the election, predominantly articulated on social media.

Here, the massive dissemination of disinformation and conspiracy narratives, for example about the Green Party and its representatives during the election campaign, led to a clear increase in aggression and radicalism. Examples of how quickly online violence can translate into real world harm are by now plentiful in Germany, such as the murder of CDU politician Walther Lübcke in 2019, the attempted storm of the Reichstag building after a demonstration by the Querdenker movement in August 2020, or the murder of a gas station employee in Idar-Oberstein by an opponent of the Corona measures in 2021.

Recommendations

All modern playbooks on election interference - regardless of whether domestic or foreign - have one thing in common: they rarely aim to influence concrete election results. Their actual target is to undermine and destroy the long-term trust of citizens in the legitimacy of their democratic institutions (government, parliament and political parties) as well as their democratic processes (elections). Consequently, the fact-based provision of information, strengthening the level of digital resilience of Germany's state institutions as well as the digital media literacy of their representatives and citizens should be a top priority for the new government and the new German Bundestag. To support these efforts, we submit the following recommendations:

Strengthening the "Guardian Role" of the German Bundestag: Parliamentarians are not only at the forefront of democracy when they run for office. They should also take special care and responsibility for defending and strengthening the integrity of democracy after they enter parliament. Transparency, freedom of expression and accountability are the cornerstones not only of democratic parliamentarianism, but also of election integrity.

In the German Bundestag, at least five different committees hold competencies on issues related to potential incidents of election interference. To ensure that the newly elected Bundestag remains vigilant against any interference in upcoming German elections, we recommend the **establishment of an institutionalised exchange format**, in which members of all relevant committees are represented.

Such a "Select Committee on Election Integrity" could meet on a biannual plus ad-hoc basis and assess the current threat level and inform the public once a year.

Improving the general awareness of Members of Parliament on threats to election integrity is critical. Almost 40% of the 20th German Bundestag is made up of first-time MPs, and many re-elected parliamentarians might also have some catching up to do on this issue. For this reason, we recommend **periodical workshops for members of parliament and their staff on topics such as cybersecurity, disinformation, and media literacy** as part of the parliamentary education program. These should be done in cooperation with other state agencies like the Federal Office for Information Security (BSI) as well as external experts and civil society organizations.

Getting Germany's (election integrity) act together: Due to its federal structure, Germany is in a less favorable position to defend itself against complex attacks on its various state organs than other countries. While some institutions look primarily outward, others look more inward. Yet there is no clearly structured supervision, tracking and incorporation of the various levels. Thanks to good coordination with all relevant state institutions, the *Bundeswahlleiter* succeeded in establishing an effective shield for the 2021 federal election. But the incoming federal government should make it its goal to solve major deficits in the existing system in a problem-oriented manner.

Evaluating the state of affairs: In order to adequately prepare for the nationwide challenge posed by further, more sophisticated attempts to erode Germany's democracy in the coming years, the new federal government, represented by the Federal Ministry of the Interior and the Federal Foreign Office, should **jointly establish an Election Integrity Commission**, building on the concept and recommendations of the *Data Ethics Commission* from 2018/2019. This new expert commission should determine and assess the extent of existing and anticipated threats and deficits in Germany's state structure and develop a holistic approach on how to foster the country's democratic resilience. Possible areas the Commission would need to analyze should range from attempts of election interference on all federal levels (regional, state and national), disinformation campaigns in traditional and social media, cyberattacks on state and quasi-state institutions and their representatives, and direct and indirect financial support of party-political representatives by foreign entities. The Commission should also place Germany's threat situation into a global perspective and evaluate best practices of other democracies.

Fostering research: Considering continued technological advancements, as well as adaptive strategies by respective adversaries, election interference operations will continue to evolve. A reactive stance on such efforts will not suffice to protect the integrity of Germany's democratic structures. Therefore, we recommend that the new government **bulks up its investment in research** on disinformation, cyber threats and related areas. Importantly, funding for research should also be extended to non-academic institutions such as think tanks and civil society organisations as well as companies which engage in relevant data-analysis like mapping of disinformation narratives.

Regulating digital campaigning: The lack of clear legal requirements for election campaigning in the digital space creates a dangerous gray area for undermining the election integrity in Germany. For this reason, we recommend that the German government should define a clear, legally binding framework for digital election campaigning in the upcoming legislative period, whether through a law or a binding code of conduct accepted and signed by all parties, including enforcement mechanisms or sanctions.

Supporting European Regulation on Election Interference: The European Commission's legislative agenda in the coming months includes a number of important proposals on how the EU and its member states can better protect themselves against election interference. The Digital Services Act (DSA) and the Digital Markets Act (DMA) are at the center of these initiatives. Other legislative efforts of the European Commission, such as the "Package to Strengthen Democracy and Integrity of Elections", also address important aspects such as transparency in the financing of parties and political foundations as well as in paid political advertising. The new German government plays an important role in advancing these legislative proposals. **We therefore call on the newly elected German government to actively support the adoption of these initiatives and strive to harmonize the DSA and DMA with the national law like the NetzDG as much as possible.**

Being more transparent on cyber threats: While the German government has demonstrated during the 2021 elections that it is equipped to protect and defend against cyberattacks which target parliamentarians or critical election infrastructure, the nature and origin of cyberattacks often remain mostly unknown to the public. While a certain degree of secrecy might be necessary to defend against such malign interference practices, **we nonetheless call on the incoming German government to enhance transparency on this issue.** The annual report on the state of IT Security in Germany, published by the BSI, is a good starting point in this regard, however ad hoc publications on respective cyberattacks which occurred against German institutions during the elections would be advisable. **Thereby, the German public, civil society, but also parliamentarians would be better equipped to understand the nature of those threats, and devise strategies to protect appropriately.**

Investing in digital media literacy: The level of media literacy among German citizens remains insufficient for these to navigate through the digital information jungle. To ensure that citizens are able to distinguish between true and false information in connection with elections, whether at the national, state or local level, improved digital media literacy is crucial. **We therefore call on the new federal government to significantly increase its investment in media literacy training, targeting different age groups and their specific needs, from preschoolers to older citizens.**

About the Alliance of Democracies

The Alliance of Democracies Foundation is a non-profit organization founded in 2017 by Anders Fogh Rasmussen, the former NATO Secretary General and former Prime Minister of Denmark. The vision of the Alliance of Democracies Foundation is to become the world's leading "megaphone" for the cause of democracy. The Foundation is dedicated to the advancement of democracy and free markets across the globe and runs three programs:

- *The Copenhagen Democracy Summit*
  An annual conference bringing together political and business leaders, including current and former heads of government, from the world's democracies. The goal of the Summit is to be the top international forum for analysis on the security and economic challenges facing the democratic world as well as a forum for analysis on the interplay between technology and democratic norms.

- *The Expeditionary Economics Program*
  The program supports successful entrepreneurial projects in emerging democracies and post-conflict areas, proving the universal appeal and potential of democracy and entrepreneurship. The purpose is to solidify at-risk democracies through locally driven economic growth.

- *The Campaign for Democracy*
  The Campaign for Democracy engages supporters of democracy worldwide and builds a powerful intellectual movement for the cause of democracy through online presence, media engagement, and moral support for dissidents. The program includes the Transatlantic Commission on Election Integrity that works to prevent election interference.

About the TCEI

The Transatlantic Commission on Election Integrity (TCEI) was launched in early 2018, its first plenary meeting took place at the Copenhagen Democracy Summit in June 2018.

Transatlantic and bipartisan in nature, the TCEI seeks to help share best practices between decision-makers and institutions across the globe, raise public awareness about the risks of interference, and apply on the ground new models of cooperation and technologies to empower civil society and governments to defend democracy against malign interference.

Since its launch, the TCEI has established itself as an important global voice and player on the risks and solutions to combat foreign meddling. The TCEI brings together more than a dozen eminent persons from backgrounds in politics, media and the private sector with one shared goal: to ensure people decide freely, based on independent information, who should represent them.

TCEI initiatives during the German Election 2021

During the 2021 Federal Election in Germany, the Alliance of Democracies Foundation (AoD), through its Transatlantic Commission on Election Integrity (TCEI), launched a series of initiatives to raise public awareness on election interference, to engage with parliamentary candidates and support German civil society groups and think tanks:

At the core of our engagement was the **Pledge for Election Integrity**, the flagship initiative of Transatlantic Commission on Election Integrity. The pledge calls on all signatories to commit to take no action to aid and abet those who seek to undermine our democracies. The Alliance of Democracies invited all members of parliament from all major political parties in Germany, as well as candidates for the Bundestag to take the pledge.

The W.I.P. Talks is a podcast series organised by the Alliance of Democracies on a variety of topics relevant to the threat of foreign and domestic election interference. Over a series of hour-long podcast episodes, we invited stakeholders from government, media, academia and the think tank community, as well as the private sector to discuss topics like disinformation, digital media literacy, cyber attacks or the role of social media platforms during elections on Twitter Spaces.

Alongside the W.I.P. talks, we developed a **series of infographics** for each topic discussed in the podcast. These infographics describe and illustrate the respective topic in an easily understandable manner, with particular focus being placed on the dissemination of the infographics to the wider public. This initiative was conducted in partnership with the *Alfred Herrhausen Gesellschaft*.

The Disinformation Diaries is an online game which allows players to better understand how disinformation and deepfakes can interfere with democratic elections. Players take on the role of a fictional politician who lost an election to her political rival due to the impact of a deepfake and disinformation campaign deployed against her. The idea behind this game is to increase the media literacy of political candidates and their staff by helping them develop practical skills to respond to disinformation campaigns. The German translation of the Disinformation Diaries was launched ahead of the Bundestagswahl.

We furthermore launched a public **Facebook group**, which served as a central platform for exchange and discussion between experts and interested Facebook users regarding information, tools, resources, and expertise on topics such as election integrity, disinformation, cybersecurity, and media literacy.

In cooperation with *Microsoft's Berlin office*, the Alliance of Democracies hosted a virtual **"Election Integrity"-workshop** for Members of Parliament on specific threats candidates may face during their election campaign. The modules of the workshop focused particularly on potential cyberattacks, how to increase campaign cybersecurity, as well as upcoming disinformation narratives, and how to react to information influence operations.

Alliance of Democracies

Election Risk Monitor: Germany 2021
Authors: Carlo Zensus, Olaf Boehnke
Design: Danielle Piatkiewicz