FAQs

Protecting the 2025 Bundestag elections from hybrid threats, including disinformation

The
Federal Government

Contents

1. Why is it necessary to protect the Bundestag elections?

The 21st German Bundestag will be elected in 2025. The German Bundestag is the parliament of the Federal Republic of Germany, and as the supreme legislative body, its most important institution. The Bundestag is composed of representatives of the German people who are elected every four years in general, direct, free and equal elections, and by secret ballot.

Guaranteeing parliamentary elections and carrying these out securely is exceedingly important for our democracy. Neutrality of the electoral bodies and the principle of open elections, which is constitutionally guaranteed, are fundamental conditions for ensuring public trust in the organisation of elections and acceptance of the electoral results. All key steps in the electoral process are subject to public scrutiny.

Elections are the very heart of democracy, which means they deserve particular protection. Most of all, elections must be shielded from foreign interference. Around elections, foreign governments often increase illegitimate activities to sway voters. Some states, often with autocratic governments, make targeted attempts to call into question the legitimacy of our elections in order to weaken citizens' trust in democratic processes and institutions. We must make a determined effort to counter these threats.

2. What are hybrid threats?

Hybrid threats are illegitimate, often coordinated actions by state and state-directed actors to advance their own interests at the expense of another state, without resorting to conventional military attacks.

Hybrid threats target all individuals living within a state, as they aim to influence the attitudes and will of a population in the interest of a foreign government. Hybrid threats are intended to have a cognitive and communicative effect on the addressees, to limit the government's ability to act, paralyse political decision-making and weaken democratic processes and constitutional institutions.

Hybrid threats affect all levels of the political sphere and broader society. They can combine a range of means (e.g. diplomatic, military, economic or technological) to achieve a coordinated campaign. In some cases, it is difficult to identify individual incidents as part of a larger campaign and therefore to act accordingly.

The instruments used include disinformation, cyberattacks on government agencies and on companies, espionage, economic interference, for example through targeted investment in key industries, and sabotage, including of critical infrastructure.

3. What is disinformation?

Disinformation is false or misleading information which is intentionally distributed. This distinguishes it from false or misleading information that emerges and is shared in error or without the intention to deceive.

Distributors of disinformation deliberately aim to deceive the recipients and to induce them to further spread false and misleading information. Disinformation is used for various reasons by non-state actors in Germany and abroad as well as by foreign state and state-aligned actors.

If a foreign government disseminates disinformation with the intent of exerting illegitimate influence on another country (or alliance of countries), this constitutes a hybrid threat. The intention of such actions is to influence public opinion, to conceal and distract from the state's own activities, to ramp up the emotional nature of controversial debates, to increase tensions in society, and/or to undermine trust in government institutions and action, with the aim of reinforcing the foreign state's own position and pursuing its own interests.

Some foreign governments have been using their state media to spread disinformation for years, including in Germany. State-aligned media companies do not report editorially independent news; they are instead controlled by the government in question and are deliberately used for disinformation activities.

Global digital networks make it easier for foreign governments to spread targeted disinformation rapidly. For example, information may be manipulated or taken out of context for political motives, in order to influence public debate. The way that social media services operate to enable information to be shared and distributed also allows false and misleading information to spread very quickly and reach a large audience.

Foreign manipulation and influence campaigns in the information space are particularly problematic. These government-orchestrated, internet-based campaigns see various agents working in a coordinated way to plant and spread the same false information through a range of channels. Technical means are used for such campaigns to artificially induce additional coverage and to simulate credibility. For example, newspaper websites may be illegally copied, fake accounts created on social media platforms, and bots used for the automated spreading of content and manipulation of recommendation algorithms.

In addition, artificial intelligence makes it reasonably straightforward to create faked sound, image and video recordings (known as "deepfakes") that make politicians appear to say things that they have never said, for example. This is another way for foreign governments to influence our political discourse using manipulated information.

4. What is the Federal Government's assessment of the hybrid threat situation in the run-up to the 2025 Bundestag elections?

The Federal Government is looking at a range of forms in which foreign governments aim to exert illegitimate influence, particularly against the security interests or the self-determined forming of political views of the people of Germany. Key political events such as elections can always be the target of undue influence by foreign powers seeking to pursue their strategic goals. The Federal Government assumes that some foreign governments may, in principle, consider the option of carrying out interference measures in the context of the 2025 Bundestag elections. Disinformation and discreditation efforts, cyberattacks, espionage and sabotage may be expected. These governments will assess whether, and in what form, such measures may be used based on opportunity and the relevant cost-benefit analysis.

In the context of the Bundestag elections, there is likely to be an increase in the amount of foreign disinformation circulating in Germany. It can be assumed that other governments will try to interfere with the public debate and the forming of political views. Since the beginning of the Russian war of aggression against Ukraine in February 2022, which is in breach of international law, the Federal Government has seen an increase in disinformation from official Russian sources, government-controlled and pro-Russia media, and pro-Kremlin social media accounts.

There is currently no knowledge of specific cyberattacks targeting the Bundestag elections. However, in the run-up to elections around the world in recent years, a wide range of cyberattacks has been observed. These include what are known as hack-and-leak campaigns against political parties, in which personal data, emails and documents were stolen and released into the public domain, in some cases after manipulation of their content. Attacks were also attempted on websites and servers hosting voter information or providing information about the election. Hacktivism for political motives has also increased in Germany since the start of Russia's war of aggression against Ukraine, and can go hand in hand with denial-of-service attacks on political party websites or events. These cyberattacks primarily affect information and cannot influence the actual process of voting at polling stations or by post.

The numerous current examples show that Russia, most notably, could try to exert illegitimate influence on the forming of political views prior to the Bundestag elections in Germany, primarily by means of manipulation campaigns in the information space. However, the Federal Government is keeping a close eye on other governments, too.

5. In what ways might foreign countries try to exert illegitimate influence?

Prior to the Bundestag elections, foreign campaigns of manipulation and influence in the information space are the main types of interference to be expected. Foreign governments could, for example, use the spread of false information to fuel emotionally charged discussions and to deliberately play different groups in society off against one another. Topics such as migration, the Russian war of aggression against Ukraine or climate change could be exploited for this purpose, as they are topics often closely linked to socioeconomic issues. False and misleading information could be spread by means of the targeted imitation of social media accounts or websites of individuals, political parties, media companies or authorities. In addition, images and audio and video files manipulated using artificial intelligence (known as "deepfakes") could be used with the aim of influencing public opinion.

Foreign governments can also use cyberattacks to prepare and support disinformation activities. This means we must plan for what are known as hack-and-leak operations, in which data and information are stolen from the political sphere and released into the public domain. Material that is made public in this way can also contain falsified or manipulated data with the aim, in particular, of discrediting individuals or political parties. We should also assume that attempts may be made to gain access to the social media accounts or websites of people, parties, media companies or authorities with a view to hijacking them and using them to spread disinformation and propaganda.

In regard to the Bundestag elections in Germany, disinformation may be used to the detriment of both political parties and individual politicians. However, the aim of the attacks is not to influence voters to vote for a particular party. Rather, the objective is often to undermine trust in the legitimacy of the electoral process and the results of the elections, and therefore ultimately in democracy itself. In connection with the Bundestag elections, foreign governments could carry out, commission or reinforce the spreading of false or misleading information that aims to call into question the integrity of the election and the correctness of the electoral results.

6. What is the Federal Government doing to protect the 2025 Bundestag elections from illegitimate foreign influence?

The Federal Government is pursuing a broad-based, whole-of-society approach to counter foreign interference in the Bundestag elections. This inherently requires the involvement of all federal ministries and their executive agencies. Maintaining networks among the federal, state and local governments and security authorities, and dialogue with civil society, are also key. Cooperation – with partner countries and in international networks – is another important component.

Headed by the Federal Ministry of the Interior and Community, the working group on hybrid threats coordinates the Federal Government's strategic approach to hybrid threats. The interministerial and multi-authority task force on disinformation and other hybrid threats is the driving force behind the working group on hybrid threats. The work of the task force focuses first and foremost on ways to identify narratives, reinforce fact-based communication and increase public resilience against threats from the information space.

The Federal Ministry of the Interior and Community is responsible for coordinating the protection of the Bundestag elections against hybrid threats, including disinformation. The task force, headed by the Federal Ministry of the Interior and Community, provides a forum for in-depth discussion across the different ministries and authorities. This involves close and continuous coordination of discussions with the security authorities, the Federal Chancellery, the Federal Foreign Office and the Press and Information Office of the Federal Government regarding the threat situation and the measures aimed at protecting the Bundestag elections. The authorities exchange their knowledge and react accordingly. In this way, potential foreign interference operations aimed at influencing the Bundestag elections can be systematically detected and warded off. The task force also coordinates closely with the office of the Federal Returning Officer and with the Federal Agency for Civic Education, which has compiled a range of specific information materials on the Bundestag elections.

The Federal Office for Information Security supports the Federal Returning Officer and the Land (federal state) Returning Officers, candidates, and political parties in matters of information security by providing a range of information, assistance and advisory services. This work concerns, in particular, the protection of social media accounts, digital identities and websites, the use of artificial intelligence, enhanced observation of the situation and, if necessary, the provision of warnings, malware scans and incident support.

The Federal Office for the Protection of the Constitution helps protect elections to the German Bundestag as part of its statutory mandate. Illegitimate influence and espionage are the traditional fields of activity of foreign intelligence services. The Federal Office for the Protection of the Constitution monitors such activities in close dialogue with its national and international partners and informs the Federal Government and the public about possible threats.

Prevention measures and reinforcing resilience at all levels of government and in society as a whole are particular priorities for the Federal Government. Increasing public awareness of the topic and promoting public debate on how to handle disinformation are essential components of this. Targeted work is carried out in all age groups to foster and consolidate media and information literacy. The aim is to increase people's ability to detect misinformation and reduce their vulnerability to disinformation. Each and every one of us has a part to play in combating disinformation.

In addition, cooperation – with partner countries and in international networks – is an important component in addressing hybrid threats, including disinformation. Cooperation within the European Union (EU) is especially important.

Dialogue with the providers of online platforms is also a key element of the approach to disinformation; the operators of social media platforms play an important role in implementing measures to combat the spreading of false or misleading information.

7. How does the Federal Government counter possible false or misleading information regarding the Bundestag election process?

Raising awareness and emphasising the principle of openness in the electoral process are the most important measures against disinformation. To counter disinformation, the Federal Returning Officer is active in providing comprehensive information through a range of channels (including through her website, on social media platforms, in the form of press releases, and in interviews) on preparations for the election, the running of the election and the regulations in place to guarantee that the election and the counting of votes take place correctly and properly.

The Federal Returning Officer is the official, non-partisan source for information on the electoral process. She is responsible for identifying and combating disinformation if the information in question is related to her remit or the electoral process in general. Her team monitors the situation in the media, so that they can identify disinformation and act to counter it. This includes actively correcting false or misleading statements that are spread on social media regarding the Bundestag election process in Germany, for example.

In addition, the Federal Returning Officer works with the Federal Agency for Civic Education, which provides a wide variety of information on all political topics and has compiled a range of specific information materials on the Bundestag elections. Through its social media accounts, the Federal Agency for Civic Education will address and discuss the Bundestag elections in different formats. People can also use the Wahl-O-Mat app to learn more about the Bundestag elections. The Federal Agency for Civic Education will launch specific activities and services to explain the role and dangers of disinformation during the Bundestag elections.

8. Is the Bundestag election process secure, and is manipulation of the casting of votes and the counting of votes out of the question?

The Federal Returning Officer and all other electoral bodies are implementing a wide range of measures to ensure secure elections, with support from the Federal Office for Information Security. In addition, various security mechanisms provided for in electoral law ensure that elections are carried out properly and protect against manipulation.

Voting will take place both in polling stations and by post, with postal voting only possible using official ballot papers. Voting machines and online voting procedures like those used in other countries such as the USA, which could be the target of cyberattacks, are not used in Germany.

Both the casting of votes in polling stations and the sending of postal voting packs are recorded in the electoral register, ensuring that each voter can only vote once. Electoral fraud is a punishable offence. Votes cast in polling stations and by post are counted by volunteer election assistants from among the electorate. The count takes place in public and can be verified by anyone who wishes.

When establishing the results, only express reports of the provisional election result on election night may be communicated in electronic form. Appropriate, state-of-the-art information security measures are in place to protect this sensitive data. In order to ensure that the provisional election result is established correctly in good time and to counter potential threats in cyberspace, back in December 2022, a joint federal and state working group of the Federal Office for Information Security worked alongside the federal state core team, the Land Returning Officers and the Federal Returning Officer. Together they compiled an IT-Grundschutz-Profil (baseline protection profile) for information security when establishing the provisional result of national parliamentary elections. This profile has been updated in the run-up to the 2025 Bundestag elections.

The final election result is established by the Constituency and Land Electoral Committees, and then by the Federal Election Committee, based on the election records of the Electoral Boards in the polling stations and the Postal Ballot Board. The technical measures in place make it impossible to influence the final official results of the elections by means of cyberattacks. Where there are reasonable grounds to doubt the result, the option exists to hold a recount of the results in polling districts.

9. How can I recognise false or misleading information and protect myself against disinformation?

Think critically instead of just sharing

False or misleading news items, images and videos are often shared by private individuals not because they want to cause harm, but because they are concerned. But news items or images like this may help create uncertainty or spread panic. The more emotional or dramatic the content, the more often it is shared. That is why it is so important to remain calm and not to add to the confusion. Don't share content without checking it first. And don't share any content that seems questionable. This is particularly important before elections.

Check sources and senders of information

It is always helpful to check questionable content against at least two other sources. Current news is available from the news media and daily and weekly newspapers and magazines. You can also consult the official websites and social media accounts of relevant institutions. Always check who published the video, image or news item. Is it the same person who created the content, or has the content already been repeatedly reposted by others? If a social media account uses the account holder's real name, that can be an indication that the account is authentic.

Platform providers may indicate whether individual accounts are independent or government-sponsored, which can also help in determining how reliable the content is. When using social media, rely on the verified accounts of official bodies and institutions. Look at the publication data on websites. This should include the name of the person responsible for the website, along with a full postal address, not just an anonymous email address, for example.

Use fact-checking services

There are numerous research institutions, non-governmental organisations and independent media organisations that pick up on news items and claims that are currently circulating and check them so that they can bring false information to light and correct it.

10. Where can I find out more?

The Federal Returning Officer provides comprehensive information on the European elections: https://www.bundeswahlleiterin.de/en/bundestagswahlen/2025.html

The Federal Ministry of the Interior and Community provides more detailed information on hybrid threats (in German): www.bmi.bund.de/DE/themen/heimat-integration/wehrhafte-demokratie/abwehr-hybrider-bedrohungen/abwehr-hybrider-bedrohungen-node.html

The Federal Ministry of the Interior and Community provides comprehensive information on the different aspects of disinformation as a hybrid threat: https://www.bmi.bund.de/SharedDocs/schwerpunkte/EN/disinformation/article-disinformation-hybrid-threat.html

The Press and Information Office of the Federal Government has a web page where you can learn more about dealing with disinformation: https://www.bundesregierung.de/breg-de/aktuelles/dangerous-fake-news-2244420

Through the federal programme "Live Democracy!", the Federal Ministry for Family Affairs, Senior Citizens, Women and Youth funds the Competence Network against Online Hate Speech. It provides extensive information on disinformation (in German): https://kompetenznetzwerk-hass-im-netz.de/infografik-desinformation/

In addition, the federal association against online hate speech, also funded under the "Live Democracy!" programme, provides sophisticated visualisations of online debates (in German): https://bag-gegen-hass.net/

Information about recent projects against disinformation can be found, for example, at www.demokratie-leben.de (in German)

The Federal Agency for Civic Education provides extensive information on the Bundestag elections (in German): https://www.bpb.de/themen/bundestagswahlen/

The Federal Office for the Protection of the Constitution has addressed potential threats to the Bundestag elections through illegitimate foreign interference in a recent article (in German): https://www.verfassungsschutz.de/SharedDocs/hintergruende/DE/spionage-und-proliferationsabwehr/gefaehrdung-der-bundestagswahl-2025-durch-unzulaessige-auslaendische-einflussnahme.html

The Federal Office for Information Security has issued various recommendations on information security:

https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Leitfaden-Kandidierende.html (in German)

https://www.bsi.bund.de/EN/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Spam-Phishing-Co/Passwortdiebstahl-durch-Phishing/passwortdiebstahl-durch-phishing_node.html

https://www.bsi.bund.de/EN/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Wie-geht-Internet/Identitaetsdiebstahl-Social-Media/identitaetsdiebstahl-social-media_node.html

https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Kuenstliche-Intelligenz/kuenstliche-intelligenz_node.html

The Digital Services Coordinatorat the Federal Network Agency provides a website for filing complaints against online platforms that violate their due diligence and transparency obligations: https://www.dsc.bund.de/DSC/DE/3Verbraucher/3VB/start.html (in German)

If internet users disagree with decisions of online platforms on removing content or disabling accounts, they can contact out-of-court dispute settlement bodies. A list of dispute settlement bodies working in German can be found on the website of the Digital Services Coordinator (in German): https://www.dsc.bund.de/DSC/DE/5Streitb/start.html

Publication details

Published by
Federal Ministry of the Interior and Community, 11014 Berlin
Website: www.bmi.bund.de/en

Version of
December 2024

Design and layout
familie redlich AG – Agentur für Marken und Kommunikation
KOMPAKTMEDIEN – Agentur für Kommunikation GmbH

Item number: BMI25009

Additional Federal Government publications can be downloaded or ordered here:
www.bundesregierung.de/pp-en

www.bmi.bund.de/en

social.bund.de/@bmi
x.com/BMI_Bund
youtube.com/@BMIBund
instagram.com/bmi_bund
threads.net/@bmi_bund
linkedin.com/company/bundesinnenministerium