



6 March 2024

Frequently asked questions

Protecting the European elections from hybrid threats,
including disinformation

Contents

1. Why is it necessary to protect the European elections?	3
2. What are hybrid threats?	3
3. What is disinformation?	3
4. What is the Federal Government's assessment of the hybrid threat situation in the run-up to the 2024 European elections?	4
5. In what ways might foreign countries try to exert illegitimate influence?	5
6. What is the Federal Government doing to protect the European elections from illegitimate foreign influence?	5
7. How does the Federal Government counter possible false or misleading information in regard to the running of the European elections?	7
8. Is the European election process secure, and is manipulation of the casting of votes and the counting of votes out of the question?	7
9. . How does the EU guarantee that European elections are free and fair?	8
10. How can I recognise false or misleading information and protect myself against disinformation?	9
11. Where can I find out more?	9

Protecting the European elections from hybrid threats, including disinformation

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

From 6 to 9 June 2024, the citizens of the European Union (EU) will go to the polls to vote for the European Parliament for the tenth time. Voting allows you to have a say in which Members of the European Parliament you want to represent you. This means that you can play a part in deciding on the direction that European policy will take in the coming years. **In Germany, the elections will be held on Sunday, 9 June.** The elections to the European Parliament are regulated by national electoral law. In Germany, the European elections take place nationwide.

Guaranteeing parliamentary elections and carrying these out securely is exceedingly important for our democracy. The legally binding 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. Elections are often a catalyst for increased levels of illegitimate activity by foreign governments, because stoking fear and spreading hate can contribute to the polarisation of society, influencing voting habits. 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?

The term hybrid threat covers a range of tactics deployed by foreign governments to exert illegitimate influence on other states. By means of the coordinated deployment of a range of instruments such as disinformation and cyberattacks, sometimes executed by non-state actors, these foreign governments try to push through their own objectives, whether openly or covertly, against our interests and values. Their aim is to weaken and destabilise our democracy. **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 of critical infrastructure.**

Hybrid threats affect all levels of the political sphere and broader society. They can combine a range of means, such as 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.

3. What is disinformation?

Disinformation is false or misleading information that 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. Non-state actors in Germany and abroad as well as foreign state actors use disinformation for various reasons.

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.

Global digital networks make it easier for foreign governments to spread precisely 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 easily also allows false and misleading information to spread very quickly and reach a large audience.

Foreign information manipulation and interference represents a particular problem. The government-orchestrated, internet-based campaigns see numerous 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 2024 European 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. **The Federal Government assumes that numerous foreign governments may, in principle, consider interference measures associated with this year's European elections as a possible course of action.** 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 European elections, there is likely to be an increase in the amount of foreign disinformation circulating in Germany, among other things. It can be assumed that other governments will try to interfere with the public debate and the forming of political views in Germany. Since the beginning of the Russian war of aggression against Ukraine, 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.

To date, there have not been any specific cyberattacks targeting the European elections. However, in the run-up to elections around the world in recent years, a wide range of

cyberattacks have been observed. These include what are known as hack-and-leak campaigns against political parties, in which 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 on 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.

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

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

Prior to the European elections, foreign information manipulation and interference is 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 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.**

In regard to the European 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 only 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 European 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 European elections from illegitimate foreign influence?

The Federal Government is pursuing a broad-based, whole-of-society approach to counter foreign interference in the European elections. This inherently requires the involvement of every federal ministry and the agencies within their remits. 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 represent further important components.

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 inter-ministerial task force against disinformation is the powerhouse of 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 European elections in Germany against hybrid threats, including disinformation. The task force against disinformation, 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 particularly close 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 European elections in Germany. The authorities exchange their respective knowledge and react accordingly. **In this way, potential foreign interference operations aimed at influencing the European 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.

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 with 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, the enhanced observation of the situation and, if necessary, the provision of warnings, malware scans and incident support.

Prevention measures and measures to increase the resilience of the entire state and society are a particular priority 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 literacy. Each and every one of us has a part to play in combating disinformation.

Protecting the European elections is also a high priority at EU level. The meetings of the Horizontal Working Party on Enhancing Resilience and Countering Hybrid Threats are regularly used as a platform for EU member states to share their experiences, examples of best practice, and research findings related to handling disinformation in the context of elections, among other things.

Dialogue with the providers of online platforms is also a key element of the approach to disinformation at both European and national level; social media providers 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 in regard to the running of the European elections?

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, nonpartisan 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 running of the European elections 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 on the European elections. The Federal Agency for Civic Education will address and discuss the European elections through its social media channels in a range of formats. The Federal Agency for Civic Education website will also provide a dossier on the topic of disinformation in the context of the European elections. In addition, a chatbot will provide trustworthy information on the European elections.

8. Is the European 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 the security of the 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 voting only possible using official ballot papers. **Voting machines and online voting** 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 the express report of the provisional election result on election night is also 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 to compile an IT-Grundschutz (baseline protection) profile for information security regarding the establishment of the provisional results of national parliamentary elections.

The final election result is established based on the election records of the Electoral Boards in the polling stations, the Postal Ballot Board, and the Constituency and *Land* Electoral Committees. **It is 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 does the EU guarantee that European elections are free and fair?

Protecting the European elections is a key aspect of the work of all EU bodies and institutions.

Following the 2019 European elections, the European Commission analysed the elections in a report and determined on this basis areas where there was a need for action. To address these areas, **in 2020 the European Commission presented a European Democracy Action Plan. Since then, the implementation of the plan has seen numerous initiatives carried out that are intended to contribute to a more resilient democracy and to greater security of elections.** A focus of the Action Plan is the protection of Europe's democracies from disinformation and foreign interference in the information space. To implement this, the European Commission notably supported the revision of the Code of Practice on Disinformation. The European Commission works together with online platforms on the basis of the Code of Practice to counter disinformation.

In addition, in December 2023, the European Commission presented a recommendation on inclusive and resilient electoral processes in the European Union and the efficient conduct of the elections to the European Parliament, which also addresses the issue of generally protecting elections from cyber threats, disinformation and hybrid threats. In November 2023, the European Commission had already organised a joint cybersecurity exercise for the EU institutions and the EU member states in order to prepare for the upcoming elections to the European Parliament.

Since January 2024, the Belgian Presidency of the Council of the European Union has been championing the protection of democracy and the promotion of free and fair European elections. The Horizontal Working Party on Enhancing Resilience and Countering Hybrid Threats is key in this regard. The Horizontal Working Party has a central role in the European Union coordinating the common EU reaction to hybrid threats, including disinformation. **The development of two toolboxes represented a decisive step in enhancing the EU's ability to react to hybrid threats and disinformation:** one of the toolboxes is designed to provide a framework for a coordinated response to hybrid threats (EU Hybrid Toolbox), while the other is intended to provide an approach to foreign information manipulation and interference (Foreign Information Manipulation and Interference (FIMI) Toolbox).

Online platforms and search engines have become important settings for societal discourse and the shaping of public opinion and voting behaviour. **The Digital Services Act (DSA), which came into effect on 25 August 2023, requires very large online platforms and search engines** to diligently identify, analyse, and assess risks linked to the design or functioning of their services,

including all actual or foreseeable negative effects on civic debate and on electoral processes. The DSA provides the European Commission with far-reaching investigation and supervisory competences, including the possible imposition of fines. The European Commission has proposed draft guidelines intended to support very large online platforms and search engines in meeting their obligations to reduce systemic risks related to electoral processes.

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

a) 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 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.

b) 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. It is also helpful to look at the official website of any institution mentioned in a news item, as well as at the institution's social media channels. 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.

c) 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.

11. Where can I find out more?

The Federal Returning Officer provides comprehensive information on the European elections: <https://www.bundeswahlleiterin.de/en/europawahlen/2024.html>

The Federal Returning Officer presents facts about disinformation linked to the European elections: <https://www.bundeswahlleiterin.de/en/europawahlen/2024/fakten-desinformation.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 provides information on the Federal Government site on how to deal with disinformation (in German):

<https://www.bundesregierung.de/breg-de/themen/umgang-mit-desinformation>

The Press and Information Office of the Federal Government also warns of the increase in disinformation and deepfakes related to the marathon election year in 2024 (in German):

<https://www.bundesregierung.de/breg-de/schwerpunkte/umgang-mit-desinformation/desinformation-wahlen-2253208>

The Federal Office for Information Security has issued numerous recommendations on information security (in German):

<https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Broschueren/Leitfaden-Kandidierende.html>

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

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

The European Parliament provides information on the European election on a site it has created for this purpose: <https://elections.europa.eu/en/>

Publication data

Published by:

Federal Ministry of the Interior and Community, 11014 Berlin, Germany

Website: www.bmi.bund.de

Last revised:

March 2024

Article number: BMI24010

You can also find further publications of the Federal Government to download or order at:

www.bundesregierung.de/publikationen

This publication is issued by the Federal Government as part of its public relations work. The publication is distributed free of charge and is not intended for sale. It may not be used by political parties or by election campaigners or election assistants during an election campaign for the purpose of election advertising. This applies to elections to the Bundestag, the Landtag and local elections as well as to elections to the European Parliament.