FAQ

Schutz der Bundestagswahl 2025 vor hybriden Bedrohungen einschließlich Desinformation

Die Bundesregierung

Inhalt

1. Warum muss die Bundestagswahl geschützt werden? 3

2. Was sind hybride Bedrohungen? 4

3. Was ist Desinformation? 5

4. Wie schätzt die Bundesregierung die hybride Bedrohungslage im Vorfeld der Bundestagswahl 2025 ein? 6

5. Welche Arten von illegitimer Einflussnahme durch fremde Staaten sind möglich? 7

6. Was tut die Bundesregierung, um die Bundestagswahl 2025 vor illegitimer Einflussnahme durch fremde Staaten zu schützen? 8

7. Wie begegnet die Bundesregierung möglichen falschen oder irreführenden Informationen bezüglich des Ablaufs der Bundestagswahl? 10

8. Ist der Ablauf der Bundestagswahl sicher und können Manipulationen bei der Stimmabgabe oder bei der Stimmauszählung ausgeschlossen werden? 11

9. Wie kann man falsche und irreführende Informationen erkennen und sich vor Desinformation schützen? 12

10. Wo kann man mehr erfahren? 13

Impressum 15

1. Warum muss die Bundestagswahl geschützt werden?

Im Jahr 2025 erfolgt die Wahl zum 21. Deutschen Bundestag. Der Deutsche Bundestag ist die Volksvertretung der Bundesrepublik Deutschland und als maßgebliches Gesetzgebungsgremium ihr wichtigstes Organ. Er besteht aus Abgeordneten des deutschen Volkes, die in allgemeiner, unmittelbarer, freier, gleicher und geheimer Wahl für vier Jahre gewählt werden.

Die Gewährleistung und damit auch die sichere Durchführung parlamentarischer Wahlen ist für unsere Demokratie von überaus hoher Bedeutung. Grundbedingungen für das Vertrauen der Bevölkerung in die Wahlorganisation und die Akzeptanz des Wahlergebnisses sind die Neutralität der Wahlorgane sowie der verfassungsrechtlich gewährleistete Grundsatz der Öffentlichkeit der Wahl. Alle wesentlichen Schritte der Wahl sind öffentlich überprüfbar.

Wahlen sind das Kernstück der Demokratie und als solches besonders schützenswert. Insbesondere müssen Wahlen vor illegitimer Einflussnahme durch fremde Staaten geschützt werden. Wahlen sind häufig Anlass für verstärkte illegitime Aktivitäten fremder Staaten, um das Wahlverhalten der Bürgerinnen und Bürger zu beeinflussen. Bestimmte, oftmals autokratische Staaten versuchen gezielt, die Legitimität unserer Wahlen in Zweifel zu ziehen und das Vertrauen der Bürgerinnen und Bürger in demokratische Prozesse und Institutionen zu schwächen. Diesen Bedrohungen muss entschlossen entgegengetreten werden.

2. Was sind hybride Bedrohungen?

Hybride Bedrohungen bezeichnen illegitime, zumeist koordinierte Handlungen staatlicher und staatlich gelenkter Akteure zur Durchsetzung eigener Interessen zum Nachteil eines anderen Staates, die außerhalb des Rahmens eines konventionellen militärischen Angriffs bleiben.

Adressaten hybrider Bedrohungen sind alle Menschen, die in einem Staat leben, denn hybride Bedrohungen zielen darauf ab, die Haltung und den Willen einer Bevölkerung im Sinne des ausländischen Staates zu beeinflussen. Hybride Bedrohungen sollen eine kognitive und kommunikative Wirkung bei den Adressaten erzeugen, um die staatliche Handlungsfähigkeit einzuschränken, den politische Entscheidungswillen zu lähmen und demokratische Prozesse und rechtsstaatliche Institutionen zu schwächen.

Hybride Bedrohungen betreffen alle politischen und gesellschaftlichen Ebenen. Dabei können verschiedene Mittel kombiniert werden (zum Beispiel diplomatische, militärische, wirtschaftliche oder technologische), sodass eine koordinierte Kampagne entsteht. Mitunter ist es schwierig, einzelne Ereignisse als Teil einer größeren Kampagne zu erkennen und so rechtzeitig zu reagieren.

Zu den eingesetzten Instrumenten gehören beispielsweise Desinformation, Cyberangriffe auf staatliche Stellen und Unternehmen, Spionage, wirtschaftliche Einflussnahme, zum Beispiel durch gezielte Investition in Schlüsselindustrien, und Sabotage auch von Kritischen Infrastrukturen.

3. Was ist Desinformation?

Desinformation ist falsche oder irreführende Information, die gezielt verbreitet wird. Dies ist zu unterscheiden von falschen oder irreführenden Informationen, die irrtümlich beziehungsweise ohne Täuschungsabsicht entstehen und verbreitet werden.

Die Absender von Desinformation setzen darauf, die Empfänger zu täuschen und dazu zu verleiten, falsche und irreführende Informationen weiterzuverbreiten. Desinformation wird von nicht-staatlichen Akteuren aus dem In- und Ausland sowie von ausländischen staatlichen oder staatsnahen Akteuren aus unterschiedlichen Motivationen heraus eingesetzt.

Wird Desinformation von einem fremden Staat verbreitet, um dadurch illegitim Einfluss auf einen anderen Staat (oder auch einen Staatenverbund) auszuüben, handelt es sich um eine hybride Bedrohung. Beabsichtigt wird eine Beeinflussung der öffentlichen Meinungsbildung, Verschleierung und Ablenkung von eigenen Aktivitäten, Emotionalisierung von kontroversen Debatten, Verstärkung gesellschaftlicher Spannungen und/oder das Schüren von Misstrauen in staatliche Institutionen und Regierungshandeln, mit dem Ziel der Stärkung der eigenen Position und Durchsetzung eigener Interessen.

Einige ausländische Regierungen nutzen schon seit Jahren ihre staatlichen Medien, um Desinformation zu verbreiten, auch in Deutschland. Staatsnahe Medienhäuser berichten nicht unabhängig journalistisch, sondern werden vom jeweiligen Staat kontrolliert und auch unmittelbar für Desinformationsaktivitäten genutzt.

Die weltweite digitale Vernetzung erleichtert es fremden Staaten, Desinformation schnell und gezielt zu verbreiten. Beispielsweise werden aus politischen Motiven Informationen manipuliert oder aus dem Kontext gerissen, um öffentliche Debatten zu beeinflussen. Gerade aufgrund der Funktionsweise Sozialer Medien, die auf dem Teilen und Verbreiten von Informationen aufbaut, können sich falsche und irreführende Informationen schnell weiterverbreiten und sehr viele Menschen erreichen.

Besonders problematisch sind ausländische Manipulations- und Einflusskampagnen im Informationsraum. Bei diesen staatlich orchestrierten Kampagnen im Internet platzieren und verbreiten mehrere Akteure koordiniert und auf unterschiedlichen Kanälen dieselben Falschinformationen. Mit technischen Hilfsmitteln wird bei diesen Kampagnen zusätzlich künstlich Reichweite erzeugt und Glaubwürdigkeit vorgetäuscht. So werden zum Beispiel Webseiten von Zeitungen unrechtmäßig kopiert, Fake Accounts in Sozialen Medien erstellt und sogenannte Bots für die automatisierte Verbreitung der Inhalte und die Manipulation von Empfehlungsalgorithmen genutzt.

Zudem ist es mit Hilfe Künstlicher Intelligenz ohne große Hürden möglich, gefälschte Ton-, Bild- und Videoaufzeichnungen (sogenannte Deepfakes) zu erstellen und beispielsweise Politikerinnen und Politiker oder Journalistinnen und Journalisten Dinge sagen zu lassen, die sie so nie ausgesprochen haben. Auch auf diese Weise können fremde Staaten mit manipulierten Informationen auf unseren politischen Diskurs einwirken.

4. Wie schätzt die Bundesregierung die hybride Bedrohungslage im Vorfeld der Bundestagswahl 2025 ein?

Die Bundesregierung befasst sich mit verschiedenen Formen der illegitimen Einflussnahme fremder Staaten, die sich insbesondere gegen die Sicherheitsinteressen oder die souveräne Willensbildung Deutschlands richten. Zentrale politische Ereignisse wie die Durchführung von Wahlen können stets Zielscheibe von unzulässiger Einflussnahme fremder Mächte werden, die so ihre strategischen Ziele verfolgen wollen. Die Bundesregierung geht davon aus, dass entsprechende Einflussmaßnahmen im Kontext der Bundestagswahl 2025 für manche Staaten als Handlungsoptionen infrage kommen. Einzukalkulieren sind Aktionen der Desinformation und Diskreditierung, Cyberangriffe sowie Spionage und Sabotage. Ob und in welcher Form sie umgesetzt werden, beurteilen diese Staaten nach Opportunität sowie ihrer jeweiligen Kosten-Nutzen-Abwägung.

Im Kontext der Bundestagswahl ist unter anderem mit einer Zunahme ausländischer Desinformation in Deutschland zu rechnen. Es ist davon auszugehen, dass andere Staaten versuchen werden, illegitim Einfluss auf die öffentliche Debatte und die politische Willensbildung zu nehmen. Bereits seit dem Beginn des völkerrechtswidrigen russischen Angriffskrieges gegen die Ukraine im Februar 2022 beobachtet die Bundesregierung ein erhöhtes Aufkommen von Desinformation durch russische offizielle Stellen, staatliche und staatsnahe Medien sowie Kreml-nahe Accounts in Sozialen Medien.

Derzeit sind keine konkreten Cyberangriffe bekannt, die sich gezielt gegen die Bundestagswahl richten. Allerdings hat sich in den vergangenen Jahren weltweit gezeigt, dass im Vorfeld von Wahlen ein breites Spektrum an Cyberangriffen zu beobachten ist. Dazu gehören sogenannte Hack-and-Leak-Kampagnen gegen Parteien, bei denen persönliche Daten, E-Mails und Dokumente gestohlen und dann – teilweise manipuliert – veröffentlicht wurden. Hinzu kamen Angriffsversuche auf Webseiten und Server, die Wählerdaten enthielten oder Informationen zur Wahl zur Verfügung stellten. Politisch motivierter Hacktivismus hat seit dem Beginn des russischen Angriffskrieges gegen die Ukraine auch in Deutschland zugenommen und kann mit Überlastungsangriffen auf Webseiten oder Veranstaltungen von Parteien einhergehen. Die genannten Cyberangriffe entfalten vor allem im Informationsumfeld ihre Wirkung und können den engeren Wahlprozess der Urnen- beziehungsweise Briefwahl nicht beeinflussen.

Die vielen aktuellen Beispiele legen nahe, dass vor allem Russland versuchen könnte, vorrangig mittels Manipulationskampagnen im Informationsraum illegitim Einfluss auf die politische Meinungsbildung im Vorfeld der Bundestagswahl in Deutschland zu nehmen. Die Bundesregierung behält jedoch auch andere Staaten genau im Blick.

5. Welche Arten von illegitimer Einflussnahme durch fremde Staaten sind möglich?

Im Vorfeld der Bundestagswahl sind insbesondere ausländische Manipulations- und Einflusskampagnen im Informationsraum zu erwarten. Fremde Staaten könnten beispielsweise die Verbreitung von Falschinformationen nutzen, um emotional aufgeladene Diskussionen anzuheizen und gesellschaftliche Gruppen gezielt gegeneinander auszuspielen. Instrumentalisiert werden könnten Themen wie Migration, der russische Angriffskrieg gegen die Ukraine oder Klimawandel, also Themen, die oft auch mit sozioökonomischen Fragen verbunden sind. Über gezielte Fälschungen von Social Media Accounts und Webseiten von Personen, Parteien, Medienunternehmen oder Behörden könnten falsche und irreführende Informationen verbreitet werden. Außerdem könnten mit Künstlicher Intelligenz manipulierte Bilder sowie Audio- und Video-Dateien (sogenannte Deepfakes) eingesetzt werden, um die öffentliche Meinung zu beeinflussen.

Auch mittels Cyberangriffen können fremde Staaten Desinformationsaktivitäten vorbereiten und unterstützen. So müssen sogenannte Hack-and-Leak-Operationen einkalkuliert werden, also Veröffentlichungen von gestohlenen Daten und Informationen aus dem politischen Umfeld. Solche Veröffentlichungen können auch gefälschte oder manipulierte Daten beinhalten, um insbesondere Personen oder Parteien zu diskreditieren.

Es ist ebenfalls damit zu rechnen, dass versucht werden könnte, Zugang zu Social Media Accounts beziehungsweise Webseiten von Personen, Parteien, Medienunternehmen oder Behörden zu erlangen, um diese zu kapern und hierüber Desinformation oder Propaganda zu verbreiten.

Im Hinblick auf die Bundestagswahl in Deutschland ist Desinformation zum Nachteil von Parteien sowie Politikerinnen und Politikern denkbar. Das Ziel der Angriffe besteht aber nicht nur darin, dass Wahlen zugunsten einer bestimmten Partei beeinflusst werden sollen. Vielmehr geht es oftmals darum, das Vertrauen in die Legitimität des Wahlprozesses und der Wahlergebnisse – und damit letztlich in die Demokratie an sich – zu untergraben. In Bezug auf die Bundestagswahl könnte durch fremde Staaten die Verbreitung von falschen oder irreführenden Informationen betrieben, beauftragt oder verstärkt werden, die darauf abzielen, die Integrität der Wahl und die Korrektheit der Wahlergebnisse in Frage zu stellen.

6. Was tut die Bundesregierung, um die Bundestagswahl 2025 vor illegitimer Einflussnahme durch fremde Staaten zu schützen?

Die Bundesregierung verfolgt einen breiten gesamtgesellschaftlichen Ansatz gegen illegitime Einflussnahme fremder Staaten. Grundsätzlich sind hierbei alle Ressorts der Bundesregierung sowie deren Geschäftsbereiche beteiligt. Von hoher Bedeutung ist zudem die Vernetzung von Bund und Ländern einschließlich ihrer Kommunen und den Sicherheitsbehörden sowie der Austausch mit der Zivilgesellschaft. Die Kooperation mit Partnerstaaten und in internationalen Netzwerken ist ein weiterer wichtiger Baustein.

Unter Leitung des Bundesministeriums des Innern und für Heimat (BMI) koordiniert die Arbeitsgruppe Hybride Bedrohungen (AG Hybrid) den strategischen Umgang der Bundesregierung mit hybriden Bedrohungen. Als „Arbeitsmuskel" der AG Hybrid dient die ressort- und behördenübergreifende Task Force gegen Desinformation und weitere hybride Bedrohungen. Im Mittelpunkt der Arbeit der Task Force stehen vor allem Maßnahmen zur Identifizierung von Narrativen, zur Stärkung der proaktiven, faktenbasierten Kommunikation und zur Erhöhung der gesellschaftlichen Resilienz gegen Bedrohungen aus dem Informationsraum.

Das BMI koordiniert den Schutz der Bundestagswahl vor hybriden Bedrohungen einschließlich Desinformation. Im Rahmen der vom BMI geleiteten Task Force findet ein enger ressort- und behördenübergreifender Austausch statt. Dabei stimmt sich das BMI intensiv und kontinuierlich insbesondere mit den Sicherheitsbehörden, dem Bundeskanzleramt, dem Auswärtigen Amt (AA) und dem Bundespresseamt (BPA) über die Bedrohungslage und die jeweiligen Maßnahmen zum Schutz der Bundestagswahl ab. Die Behörden tauschen ihre Erkenntnisse aus und reagieren entsprechend. Auf diese Weise können potenzielle Einflussnahmeaktivitäten fremder Staaten auf die Bundestagswahl konsequent erkannt und abgewehrt werden. Eine intensive Abstimmung erfolgt zudem mit dem Büro der Bundeswahlleiterin und der Bundeszentrale für politische Bildung (BpB), die verschiedene Informationsangebote zur Bundestagswahl bereitstellt.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) unterstützt unter anderem die Bundes- und Landeswahlleitungen, Kandidierende und Parteien in Belangen der Informationssicherheit mit verschiedenen Informations-, Hilfs- und Beratungsangeboten. Dies betrifft insbesondere den Schutz von Social Media Accounts, digitaler Identitäten und Webseiten, die Anwendung von Künstlicher Intelligenz, eine erweiterte Lagebeobachtung und gegebenenfalls Warnung, Schadsoftwarescans und Vorfallsunterstützung.

Das Bundesamt für Verfassungsschutz (BfV) bringt sich im Rahmen seines gesetzlichen Auftrags in den Schutz der Wahlen zum Deutschen Bundestag ein. Illegitime Einflussaktivitäten und Spionage sind klassische Betätigungsfelder ausländischer Nachrichtendienste. Das BfV beobachtet solche Aktivitäten im engen Austausch mit seinen nationalen und internationalen Partnern und informiert die Bundesregierung und die Öffentlichkeit über etwaige Bedrohungen.

Besonders wichtig sind der Bundesregierung Prävention und der Aufbau von gesamtstaatlicher und gesellschaftlicher Resilienz. Die Sensibilisierung der Öffentlichkeit für die Thematik und eine gesellschaftliche Debatte zum Umgang mit Desinformation sind dabei essenziell. Nachrichten- und Medienkompetenz werden gezielt in allen Altersgruppen gefördert und ausgebaut. Auf diese Weise soll die Fähigkeit zum Erkennen von Falschinformationen gesteigert und die Anfälligkeit für Desinformation reduziert werden. Bei der Bekämpfung von Desinformation kommt es auf jede Einzelne und jeden Einzelnen an.

Darüber hinaus ist die Kooperation mit Partnerstaaten und in internationalen Netzwerken ein wichtiger Baustein beim Umgang mit hybriden Bedrohungen einschließlich Desinformation. Besondere Bedeutung hat dabei auch die Kooperation innerhalb der Europäischen Union (EU).

Auch der Austausch mit den Online-Plattformen ist zentraler Bestandteil des Umgangs mit Desinformation, denn die Betreiber Sozialer Medien nehmen eine wichtige Rolle bei Maßnahmen gegen die Verbreitung von falschen oder irreführenden Informationen ein.

7. Wie begegnet die Bundesregierung möglichen falschen oder irreführenden Informationen bezüglich des Ablaufs der Bundestagswahl?

Aufklärung und der Grundsatz der Öffentlichkeit im Wahlverfahren sind die wichtigsten Maßnahmen gegen Desinformation. Um Desinformation entgegenzuwirken, informiert die Bundeswahlleiterin aktiv, umfassend und auf verschiedenen Kanälen (unter anderem über die Webseite, Soziale Medien, Pressemitteilungen und Interviews) über die Wahlvorbereitung, den Wahlablauf und die den integren Ablauf der Wahl und der Stimmauszählung gewährleistenden Regelungen.

Die Bundeswahlleiterin ist die offizielle und überparteiliche Quelle für Informationen rund um das Wahlverfahren. Sie ist für das Erkennen und Bekämpfen von Desinformation zuständig, wenn die Information ihren Aufgabenbereich oder das Wahlverfahren allgemein betrifft. Ihr Team beobachtet die Lage in den Medien, um Desinformation zu erkennen und ihr zu begegnen. Dazu gehört auch die aktive Richtigstellung von falschen oder irreführenden Aussagen, die beispielsweise in den Sozialen Medien über den Ablauf der Bundestagswahl in Deutschland verbreitet werden.

Außerdem arbeitet die Bundeswahlleiterin mit der BpB zusammen, die ein sehr breites Spektrum an Informationen zu allen politischen Themen bietet und verschiedene Informationsangebote zur Bundestagswahl bereitstellt. Über ihre Social Media Accounts wird die BpB die Bundestagswahl in unterschiedlichen Formaten aufgreifen und diskutieren. Zudem können sich Nutzerinnen und Nutzer über den Wahl-O-Mat zur Bundestagswahl informieren. Die Rolle und Gefahren von Desinformation bei der Bundestagswahl werden in ausgewählten Maßnahmen und Angeboten der BpB thematisiert.

8. Ist der Ablauf der Bundestagswahl sicher und können Manipulationen bei der Stimmabgabe oder bei der Stimmauszählung ausgeschlossen werden?

Die Bundeswahlleiterin und alle anderen Wahlorgane setzen mit Unterstützung des BSI vielfältige Maßnahmen zur Gewährleistung sicherer Wahlen um. Darüber hinaus gewährleisten verschiedene wahlrechtliche Sicherungsmechanismen eine ordnungsgemäße Wahl und schützen vor Manipulationen.

Die Stimmabgabe findet sowohl in den Wahllokalen als auch per Briefwahl ausschließlich mit amtlichen Stimmzetteln statt. Wahlgeräte oder Online-Wahlverfahren, die in anderen Staaten wie zum Beispiel den USA zum Einsatz kommen und Ziel von Cyberangriffen sein könnten, werden in Deutschland nicht genutzt.

Sowohl die Stimmabgabe im Wahllokal als auch die Übersendung von Briefwahlunterlagen wird im Wählerregister vermerkt, so dass jede Wählerin und jeder Wähler nur einmal abstimmen kann. Wahlbetrug ist strafbar. Die in den Wahllokalen und die per Briefwahl abgegebenen Stimmen werden von ehrenamtlichen Wahlhelfenden aus der Wählerschaft öffentlich und für alle kontrollierbar ausgezählt.

Bei der Ergebnisermittlung erfolgen nur die Schnellmeldungen für das vorläufige Endergebnis am Wahlabend auch in elektronischer Form. Der Schutz dieser sensiblen Daten wird durch eine angemessene Informationssicherheit nach dem aktuellen Stand der Technik sichergestellt. Um eine korrekte und zeitgerechte Ermittlung des vorläufigen Wahlergebnisses bei bundesweiten Wahlen zu gewährleisten und den Gefährdungen im Cyberraum zu begegnen, hat eine Bund-Länder-Arbeitsgruppe des BSI gemeinsam mit dem Länder-Kern-Team, den Landeswahlleitungen und der Bundeswahlleitung bereits im Dezember 2022 ein IT-Grundschutz-Profil zur Informationssicherheit bei der Ermittlung des vorläufigen Wahlergebnisses bundesweiter parlamentarischer Wahlen (Informationssicherheit bei Schnellmeldungen) erarbeitet und vor der Bundestagswahl 2025 aktualisiert.

Das endgültige Wahlergebnis wird anhand der Niederschriften der Wahlvorstände in den Urnen- und Briefwahlbezirken durch die Kreis- und Landeswahlausschüsse und anschließend durch den Bundeswahlausschuss ermittelt. Eine Beeinflussung des endgültigen amtlichen Ergebnisses der Wahl durch Cyberangriffe ist technisch ausgeschlossen. Bei berechtigten Zweifeln besteht die Möglichkeit der Nachzählung der Ergebnisse in Wahlbezirken.

9. Wie kann man falsche und irreführende Informationen erkennen und sich vor Desinformation schützen?

Kritisch hinterfragen statt weiterleiten

Falsche oder irreführende Nachrichten, Bilder oder Videos werden von Privatpersonen oft nicht böswillig verbreitet. Im Zweifel führen solche Meldungen aber dazu, dass Verunsicherung geschürt oder Panik verbreitet wird. Je emotionaler oder dramatischer eine Meldung ist, umso häufiger wird sie verbreitet. Deshalb ist es wichtig, sich nicht daran zu beteiligen und Ruhe zu bewahren. Leiten Sie Inhalte daher nicht ungeprüft weiter. Teilen Sie keine Inhalte, die Ihnen zweifelhaft erscheinen. Dies ist gerade vor Wahlen besonders wichtig.

Quellen und Absender der Nachricht prüfen

Es hilft immer, fragliche Nachrichten mit mindestens zwei weiteren Quellen zu vergleichen. Die aktuelle Nachrichtenlage bilden die Nachrichtensender und Tages- und Wochenzeitungen ab. Informieren Sie sich zudem auf den offiziellen Webseiten und Social Media Accounts der Institutionen. Prüfen Sie immer, wer das Video beziehungsweise das Bild oder die Nachricht veröffentlicht hat. Ist er oder sie der Urheber des Materials oder wurde es bereits mehrfach weitergeleitet? Die Angabe eines Klarnamens kann ein Indiz für die Echtheit eines Accounts sein.

Auch mögliche Angaben der Plattformbetreiber zur Unabhängigkeit oder Regierungsnähe einzelner Accounts können eine Entscheidungshilfe darstellen. Halten Sie sich in den Sozialen Medien an die verifizierten Accounts der offiziellen Stellen und Institutionen. Sehen Sie sich bei Webseiten das Impressum an. Es sollte eine für die Inhalte verantwortliche Person und eine vollständige Anschrift umfassen, nicht nur zum Beispiel eine anonyme E-Mail-Adresse.

Faktenchecks nutzen

Zahlreiche Forschungseinrichtungen, Nichtregierungsorganisationen und unabhängige Medien greifen kursierende Meldungen und Behauptungen auf und unterziehen sie einer Überprüfung, um über Falschinformationen aufzuklären und sie richtigzustellen.

10. Wo kann man mehr erfahren?

Die Bundeswahlleiterin bietet umfangreiche Informationen rund um die Bundestagswahl: https://www.bundeswahlleiterin.de/bundestagswahlen/2025.html

Das BMI stellt nähere Informationen zu hybriden Bedrohungen bereit: www.bmi.bund.de/DE/themen/heimat-integration/wehrhafte-demokratie/abwehr-hybrider-bedrohungen/abwehr-hybrider-bedrohungen-node.html

Das BMI informiert umfassend über die unterschiedlichen Facetten von Desinformation als hybride Bedrohung: https://www.bmi.bund.de/SharedDocs/schwerpunkte/DE/desinformation/artikel-desinformation-hybride-bedrohung.html

Das BPA informiert auf der Seite der Bundesregierung zum Umgang mit Desinformation: https://www.bundesregierung.de/breg-de/aktuelles/umgang-mit-desinformation-1905340

Das Bundesministerium für Familie, Senioren, Frauen und Jugend (BMFSFJ) fördert im Rahmen des Bundesprogramms „Demokratie leben!“ das Kompetenznetzwerk gegen Hass im Netz. Dieses informiert umfangreich über Desinformation: https://kompetenznetzwerk-hass-im-netz.de/infografik-desinformation/

Im Rahmen der ebenfalls über das Bundesprogramm „Demokratie leben!“ geförderten Bundesarbeitsgemeinschaft gegen Hass im Netz werden außerdem visuell umfangreich aufbereitet Debattenströme im Netz nachgezeichnet: https://bag-gegen-hass.net/

Aktuelle Projekte zur Arbeit gegen Desinformation finden sich u. a. auf www.demokratie-leben.de

Die BpB stellt umfangreiche Informationen zur Bundestagswahl bereit: https://www.bpb.de/themen/bundestagswahlen/

Das BfV thematisiert in einem aktuellen Beitrag mögliche Gefährdungen der Bundestagswahl durch unzulässige ausländische Einflussnahme: https://www.verfassungsschutz.de/SharedDocs/hintergruende/DE/spionage-und-proliferationsabwehr/gefaehrdung-der-bundestagswahl-2025-durch-unzulaessige-auslaendische-einflussnahme.html

Das BSI bietet verschiedene Empfehlungen zur Informationssicherheit:

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

Der Digital Services Coordinator (DSC) bei der Bundesnetzagentur stellt ein Beschwerdeportal zur Verfügung, das insb. bei Verstößen gegen die Sorgfalts- und Transparenzpflichten der Online-Plattformen genutzt werden kann: https://www.dsc.bund.de/DSC/DE/3Verbraucher/3VB/start.html

Sollten Internetnutzende mit der Entscheidung von Online-Plattformen bezüglich einer Entfernung von Inhalten oder der Sperrung von Konten nicht einverstanden sein, kann sich an außergerichtliche Streitbeilegungsstellen gewendet werden. Eine Auflistung der in deutscher Sprache tätigen Streitbeilegungsstellen ist auf der Internetseite des DSC zu finden: https://www.dsc.bund.de/DSC/DE/5Streitb/start.html

Impressum

Herausgeber
Bundesministerium des Innern und für Heimat, 11014 Berlin
Internet: www.bmi.bund.de

Stand
Dezember 2024

Gestaltung
familie redlich AG – Agentur für Marken und Kommunikation
KOMPAKTMEDIEN – Agentur für Kommunikation GmbH

Artikelnummer: BMI25003

Weitere Publikationen der Bundesregierung zum Herunterladen finden Sie ebenfalls unter:
www.bundesregierung.de/publikationen

Diese Publikation wird von der Bundesregierung im Rahmen ihrer Öffentlichkeitsarbeit herausgegeben. Die Publikation wird kostenlos abgegeben und ist nicht zum Verkauf bestimmt. Sie darf weder von Parteien noch von Wahlwerbern oder Wahlhelfern während eines Wahlkampfes zum Zwecke der Wahlwerbung verwendet werden. Dies gilt für Bundestags-, Landtags- und Kommunalwahlen sowie für Wahlen zum Europäischen Parlament.

www.bmi.bund.de

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