

Desinformation

Akteure, Methoden und
Erscheinungsformen im Internet



Inhalt

1.	Was ist Desinformation?	3
1.1.	Was eine Desinformation ausmacht	3
1.2.	Desinformation als ein Aufgabenfeld fremder Staaten	3
1.3.	Beispiel: Russlands Desinformationskampagnen gegen den „Westen“	4
1.3.1.	Nach welchem Schema wird russische Desinformation generiert?	4
1.3.2.	Wie wird russische Desinformation verbreitet?	5
1.4.	Extremisten nutzen Russlands Desinformationskampagnen für ihre eigene Agenda	6
2.	Deepfakes: Der Einfluss der KI auf Desinformation	8
3.	Desinformation und „Fake News“ erkennen	10
4.	Weiterführende Links zum Thema Desinformation	11
5.	Entlarvte Desinformationen – zwei Beispiele	13
5.1.	Der angebliche Spendenaufruf der Sächsischen Landesbibliothek	13
5.2.	Vermeintliche Millionen-Abfindung für ukrainischen General	14

1. Was ist Desinformation?

Russische Narrative über ein vermeintliches „Naziregime“ in der Ukraine; ein Fake-Video, in dem der ukrainische Präsident Selenskyj seine Soldaten angeblich dazu aufruft, die Waffen niederzulegen – das sind nur zwei von zahlreichen „Fake News“ rund um den Ukraine-Krieg. Auch abseits dieses Konflikts existieren vor allem in den sozialen Netzwerken viele Desinformationen, die nur ein Ziel verfolgen: Die Nutzer zu verwirren und zu verunsichern.

Der Begriff Desinformation beschreibt das absichtliche Verbreiten falscher oder irreführender Informationen mit dem Ziel, Menschen zu manipulieren. Im Fall von Desinformation erstellt und verbreitet der Urheber also bewusst Nachrichten, die nach objektiven Maßstäben inhaltlich falsch oder sinnentstellend sind.

Mithilfe solcher Falschinformationen in Form von Texten, Bildern oder Videos wollen die Urheber die öffentliche Meinung im Sinne ihrer politischen und teils auch wirtschaftlichen Ziele beeinflussen. Desinformationen sollen negative Stimmungen in der Bevölkerung verstärken, um so Polarisierungsprozesse in offenen Gesellschaften zu befeuern. Desinformationskampagnen, die diese manipulativen Inhalte und Medienformate bündeln, zielen darauf ab, die politischen Meinungs- und Willensbildungsprozesse in demokratischen Staaten nachhaltig zu beeinflussen.

1.1. Was eine Desinformation ausmacht

Allerdings ist nicht jede Falschmeldung oder irreführende Information gleich eine Desinformation in diesem Sinne. Auf einer Informationsseite zum Thema unterscheidet die Bundesregierung¹ zwischen Des- und Fehlinformation. Zentrales Unterscheidungsmerkmal ist die Täuschungsabsicht, die nur auf Desinformationen zutrifft. Eine irrtümlich beziehungsweise versehentlich veröffentlichte Falschmeldung gilt dagegen als klassische Fehlinformation. Seriös arbeitende Medien und Journalisten korrigieren solche Fehler nach Bekanntwerden in der Regel transparent. Zu den Fehlinformationen zählt die Bundesregierung auch sogenanntes „Clickbaiting“. Bei dieser Methode kommen reißerische Überschriften und Sensationsversprechen zum Einsatz, damit Beiträge im Internet möglichst viele Klicks generieren.

In den Bereich der Desinformation fallen dagegen manipulierte Inhalte (Deepfakes, gefälschte Fotos, Imitationen seriöser Nachrichtenportale), Lügen, Gerüchte, tendenziöse oder haltlose Behauptungen sowie aus dem Kontext gerissene Informationen (stark verkürzte Zitate, fehlerhafte Statistiken).

1.2. Desinformation als ein Aufgabenfeld fremder Staaten

Zu den Urhebern und Verbreitern von Desinformation zählen Akteure fremder Staaten, zum Beispiel Nachrichtendienste, Politiker oder Staatsmedien von Ländern, die ihre strategischen Ziele auch mit unzulässigen Mitteln verfolgen.

¹ Vgl. <https://www.bundesregierung.de/breg-de/schwerpunkte/umgang-mit-desinformation/was-ist-desinformation-1875148>

Staatlich gesteuerte Akteure sowie auf eigene Initiative handelnde Unterstützer, zum Beispiel staatsnahe Medien, Prominente oder Blogger, verschleiern ihren wahren Hintergrund und ihre Absichten in der Regel. Für strategische Desinformationskampagnen koordinieren diese staatlichen und staatsnahen Akteure mitunter ihre offenen und verdeckten Aktivitäten. Zumindest aber verbreiten staatlich gesteuerte Stellen und Unterstützer die Desinformationen ihrer Länder regelmäßig über die eigenen Kanäle, um so deren Reichweite zu steigern.

1.3. Beispiel: Russlands Desinformationskampagnen gegen den „Westen“

Seit dem Beginn des russischen Überfalls auf die Ukraine am 24. Februar 2022 führt Russland zugleich einen hybriden „Informationskrieg“ mithilfe professioneller Desinformationskampagnen gegen die Ukraine, den „Westen“, gegen die EU, die NATO und damit auch gegen Deutschland.

Mithilfe von Desinformation versucht die russische Regierung, die öffentliche Meinung hierzulande und in anderen Staaten zu ihren Gunsten zu beeinflussen, Ängste in der Bevölkerung vor den Auswirkungen der Russland-Sanktionen zu schüren, ukrainische Flüchtlinge in ein schlechtes Licht zu rücken und zugleich im Westen lebende Russen als „Mobbing-Opfer“ darzustellen. Außerdem werden Angstszenerien im Hinblick auf eine Eskalation des Kriegsverlaufes vor dem Hintergrund „westlicher“ Waffenlieferungen an die Ukraine geschürt. Im Ergebnis sollen westliche Gesellschaften misstrauisch gegen die Entscheidungen ihrer Regierungen gestimmt und gespalten werden.

Zugleich richtet sich die russische Propaganda an die eigene Bevölkerung, um den bis vor Kurzem als „Militärische Spezialoperation“ getarnten Krieg gegen die Ukraine zu rechtfertigen und westliche Staaten als schwach und hilflos zu präsentieren. Dadurch sollen hohe Zustimmungswerte in der russischen Bevölkerung zum Vorgehen Russlands in der Ukraine generiert werden.

1.3.1. Nach welchem Schema wird russische Desinformation generiert?

Mithilfe von vier Methoden² zielt die russische Regierung darauf ab, die Deutungshoheit über den völkerrechtswidrigen Angriffskrieg gegen die Ukraine zu erlangen, Reaktionen der Staatengemeinschaft darauf sowie eine von der Öffentlichkeit getragene Solidarität mit der Ukraine zu erschweren oder ganz zu verhindern:

- Mit der Methode des „Abstreitens“ werden für Russland nachteilige objektive Informationen mit fadenscheinigen Begründungen abgetan. Die Vertrauenswürdigkeit der Quelle soll beschädigt und Unsicherheit erzeugt werden.
- Mit der Methode des „Verzerrens“ versucht die russische Regierung mittels ihrer Staatsmedien und den von ihr gelenkten nichtstaatlichen Akteuren Informationen umzudeuten. So war der Begriff „Krieg“ im Zusammenhang mit den Geschehnissen in der Ukraine bis vor Kurzem verboten. Der Krieg wurde stattdessen lange als „Spezialoperation“ dargestellt.

² Vgl. „FAQ Desinformation im Kontext des russischen Angriffskrieges gegen die Ukraine“, Bundesministerium des Innern und für Heimat, S. 6.

(<https://www.bmi.bund.de/SharedDocs/faqs/DE/themen/heimat/desinformation/faq-liste-desinformation.html>)

- Mit der Methode des „Ablenkens“ stellt die russische Regierung beispielsweise die Ukraine als vermeintlichen Aggressor oder „neonazistisches“ Unrechtsregime dar. Der Kreml will auf diese Weise von der Tatsache ablenken, dass Russland einen demokratischen Staat mit einem Präsidenten jüdischer Herkunft völkerrechtswidrig angegriffen hat. Für Russland nachteilige Informationen im Kontext des Krieges werden durch falsche Informationen verdrängt und somit aus dem Fokus der Öffentlichkeit genommen.
- Die Methode des „Verunsicherns“ soll ein Bedrohungsszenario konstruieren und in den jeweiligen Zielstaaten ein Klima von Ablehnung, Skepsis oder Misstrauen verursachen oder anfachen. Auf diese Weise kann dann die öffentliche Meinung derart gelenkt werden, dass dies wiederum auf politische Entscheidungen und Handlungsspielräume rückwirkt. So können den politisch Handelnden Kommunikation und Entscheidungen erschwert werden. Dazu gehört das Narrativ einer atomaren Eskalation ebenso wie die Behauptung der russischen Regierung, dass die westlichen Gesellschaften „russophob“ geworden und daher russischstämmige Menschen hier nicht mehr sicher seien.

Die Grenzen zwischen diesen Methoden sind fließend. Mitunter streitet eine Desinformation die allgemein anerkannte Faktenlage ab, um zugleich das eigene verzerrte Weltbild als vermeintlich logischen Gegenentwurf zu präsentieren. Zudem wiederholen Desinformationen oft die immer gleichen Narrative russischer Propaganda. So behaupten Vertreter der russischen Regierung mit Verweis auf ihre Kriegsziele stets, die ukrainische Regierung „entnazifizieren“ zu wollen.

1.3.2. Wie wird russische Desinformation verbreitet?

Um Desinformationen gezielt, gleichzeitig, koordiniert und in möglichst großer Anzahl zu verbreiten, nutzen staatliche Akteure Äußerungen offizieller Stellen, Veröffentlichungen von Staatsmedien oder Einzelbeiträge von Personen in den sozialen Medien. Diese werden wiederum von staatlich gesteuerten Akteuren aufgegriffen und über deren eigene Kanäle gesteuert. So werden beispielsweise russische Staatsmedien wie „Russia Today“ (RT) oder „Sputnik“ für Desinformationskampagnen genutzt.

Daneben gibt es bekannte deutsch-russische Influencer oder Blogger, die über ihre Kanäle prorussische Narrative verbreiten und suggerieren, sie seien „Experten“ mit entsprechender Reputation. In einer Studie zum russischen „Informationskrieg“ im Kontext des Ukraine-Krieges konstatiert das Institute for Strategic Dialogue (ISD), dass nichtstaatliche Akteure in einigen Fällen anscheinend versuchten, ihre Aktivitäten zu koordinieren, um so die gesunkene Reichweite russischer staatlicher Einrichtungen, eine Folge der westlichen Sanktionen, zu kompensieren³.

Welchen Stellenwert die sozialen Netzwerke für die Verbreitung von Desinformationen haben, wird am Beispiel eines Berichts des US-Konzerns „Meta“, Betreiber von „Facebook“ und „Instagram“, deutlich. Dieser gab am 27. September 2022 bekannt, eine groß angelegte Kampagne zur Verbreitung russischer Desinformation in Europa gestoppt zu haben. Wie „Meta“ in seinem Bericht ausführt, sollten „prorussische“ und „antiwestliche“ Narrative unter anderem über ein ausgedehntes Netzwerk von über 60 Webseiten vor allem Menschen in Deutschland, aber auch in Frankreich, Italien, der Ukraine und im Vereinigten Königreich erreichen. Diese seit Mai 2022 aufgesetzten Webseiten ahmten bekannte Nachrichtenportale wie jene von „Spiegel“, „Bild“, „t-online“, der „Frankfurter Allgemeinen Zeitung“ und des „Neuen Deutschland“ täuschend echt nach. Diese nachgebauten Seiten verbreiteten Desinformationen unter anderem über ukrainische

³ Vgl. „Two Years on. An Analysis of Russian State and Pro-Kremlin Information Warfare in the Context of the Invasion of Ukraine“, Institute for Strategic Dialogue, S. 11f. (<https://www.isdglobal.org/isd-publications/two-years-on-an-analysis-of-russian-state-and-pro-kremlin-information-warfare-in-the-context-of-the-invasion-of-ukraine/>)

Flüchtlinge („Undankbare Menschen, die sich über ihr Leben in Deutschland beschweren“) und Auswirkungen der Russland-Sanktionen auf Deutschland („Sanktionen gegen Russland schaden nur Deutschland“, „Ein Teenager wird in Berlin wegen Einsparungen bei der Straßenbeleuchtung getötet“).

Die Fake-Inhalte wurden in Form von Artikeln, Videos und Memes mithilfe ebenfalls gefälschter Nutzerkonten über „Facebook, „Instagram, „Telegram“ oder „X“ (vormals Twitter) in verschiedenen Sprachen gezielt weiterverbreitet und kommentiert. In Reaktion auf diese Kampagne löschte „Meta“ bei „Facebook“ 1.633 Nutzerkonten, 703 Seiten mit rund 4.000 Followern sowie eine Gruppe mit weniger als zehn Mitgliedern. Bei „Instagram waren es 29 Nutzerkonten mit rund 1.500 Followern. In einigen Fällen seien die Inhalte des Netzwerkes auch über Facebook-Seiten russischer Botschaften in Europa und Asien weiterverbreitet worden, schreibt „Meta“ in seinem Analysebericht⁴.

Ein weiteres bedeutendes Instrument im hybriden „Informationskrieg“ ist das Hacken von Computersystemen, von Social-Media-Konten, von seriösen Nachrichtenportalen sowie Blogs bekannter Journalisten oder Politiker. Cyberangriffe zielen darauf ab, entsprechend gewichtige Informationen zu erlangen und diese gefälscht oder aus dem Kontext gerissen weiterzuverbreiten.

1.4. Extremisten nutzen Russlands Desinformationskampagnen für ihre eigene Agenda

Ein Teil der Desinformation richtet sich gezielt an politische Ränder unserer Gesellschaft. Rechtsextremisten und sog. „Delegitimierer“, die grundsätzlich empfänglich für Verschwörungsideologien sind, greifen solche Inhalte in ihren Social-Media-Kanälen dankbar auf und instrumentalisieren sie für die Verbreitung ihrer eigenen verfassungsfeindlichen Agenda bis in die gesellschaftliche Mitte hinein.

Immerhin gleichen die von der russischen Regierung verbreiteten Narrative über die „böse NATO“, die ebenfalls „böse EU“ sowie eine insgesamt „russophobe“, sich gegen Russland verschworene westliche Staatengemeinschaft den Feindbildern hiesiger Extremisten. Desinformationskampagnen, welche die Auswirkungen der westlichen Sanktionen gegen Russland für die deutsche Bevölkerung in übertriebenem Maße darstellen, waren und sind geeignet, Existenzängste zu schüren und breite Teile der Gesellschaft gegen politische Entscheidungsträger aufzubringen. Extremisten nutzen entsprechende Szenarien nicht nur, um Politiker zu diffamieren, sondern um das Narrativ von den gegen das eigene Volk arbeitenden politischen Eliten unablässig zu wiederholen.

Extremisten verfolgen mit der Weiterverbreitung von Desinformationen folglich das gleiche Ziel wie der Kreml: Die deutsche Bevölkerung soll an der Richtigkeit politischer Entscheidungen des Westens zweifeln, ihr Vertrauen in die Demokratie soll nachhaltig erschüttert und zugleich der Irrglaube genährt werden, dass in autokratischen Systemen wie Russland „die Welt in Ordnung sei“.

Das LfV Sachsen stellt fest, dass Themen wie die Corona-Pandemie und der Ukraine-Krieg die oben dargestellten Entwicklungen beschleunigt haben, nicht wenige Menschen das Vertrauen in Politiker und Medien offenkundig verloren haben.

Diese Menschen tummeln sich zuhauf in den unmoderierten Blasen sozialer Medien, nehmen tagtäglich unreflektiert eine Masse auch an falschen Informationen auf und bestärken sich durch entsprechende

⁴ Vgl. <https://about.fb.com/news/2022/09/removing-coordinated-inauthentic-behavior-from-china-and-russia>

Kommentare untereinander in ihrer ablehnenden Haltung gegenüber dem Verfassungsstaat. Mit ihrem Verhalten sind sie die „idealen“ Empfänger und Verbreiter von Desinformationen und spielen so ungewollt dem Kreml in die Hände. Zugleich stärken sie extremistische Positionen mitten in unserer Gesellschaft.

Menschen, die bei Versammlungen Russlandfahnen schwingen oder Plakate mit der Aufschrift „Putin – hilf uns!“ zeigen, sind Belege dafür, dass russische Desinformationskampagnen seit Beginn der Asylkrise 2014 ihre Wirkung auch bei realweltlichen Protesten entfalten.

2. Deepfakes: Der Einfluss der KI auf Desinformation

Ein „Spielfeld“ für Desinformation, das sich vor allem durch die rasante Entwicklung Künstlicher Intelligenz (KI) vergrößert, ist das Erstellen und Verbreiten sogenannter Deepfakes. Der Begriff beschreibt künstlich erstellte, jedoch täuschend echt wirkende Fotos, Videos oder Audioaufnahmen. Dabei kann es sich um das Verfälschen bzw. Imitieren realer Menschen (z. B. Schauspieler oder Politiker) oder um das Erschaffen ganz neuer Personen, Gesichter oder Stimmen (z. B. für Fake-Profile in sozialen Netzwerken) handeln. Dementsprechend kann ein Deepfake sowohl das Verändern einer vorhandenen Video- oder Sprachaufzeichnung sein als auch die künstliche Erstellung neuen Video- und Audiomaterials, ohne dass ein echter Protagonist beteiligt ist.

Noch vor einigen Jahren ließen sich verdächtige Fotos, Videos oder Audioaufnahmen noch recht zuverlässig durch hölzerne Bewegungen, entsprechende Bildfehler oder eine blechern klingende Stimme als Deepfakes enttarnen. Dank frei verfügbarer KI-Tools lassen sich heute hochwertige Fälschungen auch ohne umfassende technische Kenntnisse erstellen. Damit sind Deepfakes zu einem Massenprodukt geworden, was in einem Beitrag für die Stiftung Wissenschaft und Politik⁵ zum Thema auf drei Entwicklungen zurückgeführt wird: die kontinuierliche Verbesserung der KI, eine stetige Zunahme verfügbarer Rechenleistung und der Zugang zu immer mehr Trainingsdaten für KI-Anwendungen.

Der Beitrag führt aus, dass die sogenannte generative KI den Einsatz gefälschter Inhalte in Desinformationskampagnen auf drei Ebenen grundlegend verändert⁶:

- **Quantität:** Auf dem Markt verfügbare Apps ermöglichen die massenhafte, schnelle und kostengünstige Erstellung von Deepfakes. Dadurch können auch Staaten bzw. Gruppen mit begrenzten Ressourcen eigene Desinformationskampagnen im großen Maßstab durchführen.
- **Qualität:** Deepfakes werden qualitativ immer besser, also authentischer, wodurch sie schwerer zu erkennen sind.
- **Qualifikation:** Während die Erstellung eines Deepfakes so gut wie keine Qualifikation voraussetzt, wird die Expertise zum Erkennen der Fälschungen immer umfangreicher.

Das Fraunhofer-Institut für Angewandte und Integrierte Sicherheit sieht in manipulierten Aussagen von Politikern und bekannten Entscheidungsträgern eine besondere Herausforderung⁷. Der Grund dafür ist, dass es von Personen des öffentlichen Lebens genügend frei verfügbare Audio- und Videoaufnahmen als KI-Trainingsmaterial für die Produktion von Deepfakes gibt.

Dass Deepfakes mittlerweile Teil von Desinformationskampagnen sind, zeigt ein Vorfall zu Beginn des russischen Überfalls auf die Ukraine: Nachdem am 15. März 2022 der ukrainische TV-Sender „Ukraine 24“ gehackt wurde, erschien zunächst dort und später in den sozialen Netzwerken ein gefälschtes Video des ukrainischen Präsidenten Wolodymyr Selenskyj, in dem dieser angeblich seine Soldaten aufforderte, die Waffen niederzulegen. Die ukrainische Regierung war auf eine solche Aktion vorbereitet und reagierte

⁵ Vgl. „Deepfakes – wenn wir unseren Augen und Ohren nicht mehr trauen können“, SWP-Aktuell, S. 1f. (<https://www.swp-berlin.org/publikation/deepfakes-wenn-wir-unseren-augen-und-ohren-nicht-mehr-trauen-koennen>)

⁶ Vgl. ebd., S. 2f.

⁷ Vgl. „Deepfakes: Mit KI-Systemen Audio- und Videomanipulationen verlässlich entlarven“, Fraunhofer-Institut für Angewandte und Integrierte Sicherheit (<https://www.aisec.fraunhofer.de/de/das-institut/wissenschaftliche-exzellenz/Deepfakes.html>)

umgehend mit einem Dementi, zudem war das Deepfake qualitativ minderwertig. Die Aktion verpuffte. Mit der Weiterentwicklung der Technik steigen jedoch auch die Einsatzmöglichkeiten dieses Instruments.

3. Desinformation und „Fake News“ erkennen

Manipulierte Videos bekannter Politiker mit absurdem Inhalt oder eine Meldung, die Vorurteile gegen ukrainische Flüchtlinge zu bestätigen scheint – Desinformation reiht sich in die unüberschaubare Zahl an täglichen Neuigkeiten ein, die die Menschen vor allem über die sozialen Netzwerke erreichen. Aus Sicht des Absenders fällt den Konsumenten der manipulative Charakter der Desinformation im Idealfall gar nicht auf und sie teilen die Inhalte ungeprüft. Dadurch können Deepfakes oder „Fake News“ hohe Reichweiten und letztendlich auch ihre Wirkungskraft erzielen.

Hier stellt sich die Frage: Wie kann ich Desinformation erkennen? Eine wichtige Grundregel lautet, Inhalte nicht einfach ungeprüft weiterzuverbreiten. Das gilt vor allem für stark emotionalisierende Beiträge. Die Bundesregierung⁸ und die Bundeszentrale für politische Bildung⁹ geben auf ihren Webseiten folgende Tipps, um Inhalte zu hinterfragen:

- Text: Stimmen Überschrift und Fließtext inhaltlich überein? Ist der Beitrag widerspruchsfrei? Gibt der Text Fakten wieder oder ist er einfach nur reißerisch geschrieben?
- Quellen: Wird der ursprüngliche Absender des Inhalts angegeben? Kann der Beitrag einer seriösen Quelle zugeordnet werden? Wird die Nachricht von anderen seriösen Medien (mit übereinstimmenden Fakten) aufgegriffen?
- Bild: Passt das Bild inhaltlich zum Beitrag? Ist eine Fotoquelle angegeben? Findet man das Bild online noch in einem anderen Kontext (z. B. durch Verwenden einer Bilder-Rückwärtssuche bei Suchmaschinen)?

Aufklärung und weitere Tipps rund um das Thema Desinformation bieten Webseiten, die sich auf Faktenchecks spezialisiert haben. Dazu gehören das EU-Projekt EUvsDisinfo¹⁰, das von der East StratCom Task Force geleitet wird und seit 2015 Desinformation aufdeckt und analysiert, sowie das German-Austrian Digital Media Observatory (GADMO)¹¹, ein Zusammenschluss von Faktencheck-Organisationen und Forschungsteams mit dem Ziel, Desinformation zu bekämpfen.

⁸ Vgl. „Woran Sie Falschmeldungen erkennen können“, Bundesministerium für Bildung und Forschung (<https://www.bundesregierung.de/breg-de/schwerpunkte/umgang-mit-desinformation/falschmeldungen-erkennen-1750146>)

⁹ Vgl. „#StopFakeNews – Fake News erkennen“, Bundeszentrale für politische Bildung (<https://www.bpb.de/themen/medien-journalismus/stopfakenews/>)

¹⁰ <https://euvsdisinfo.eu>

¹¹ <https://gadmo.eu/>

4. Weiterführende Links zum Thema Desinformation

Links zum Thema Desinformation allgemein:

- <https://www.bundesregierung.de/breg-de/schwerpunkte/umgang-mit-desinformation/was-ist-desinformation-1875148>
- <https://www.verfassungsschutz.de/SharedDocs/hintergruende/DE/spionage-und-proliferationsabwehr/desinformation.html>
- <https://www.bpb.de/themen/medien-journalismus/desinformation/>
- <https://www.slpb.de/themen/gesellschaft/desinformation>
- <https://www.bertelsmann-stiftung.de/de/themen/aktuelle-meldungen/2024/februar/grosse-mehrheit-erkennt-in-desinformation-eine-gefahr-fuer-demokratie-und-zusammenhalt>

Desinformation im Kontext der Bundestagswahl 2025

- <https://www.bmi.bund.de/SharedDocs/schwerpunkte/DE/desinformation-bei-bt-wahl/desinfo-bei-bt-wahl-artikel.html>
- <https://www.bundeswahlleiterin.de/bundestagswahlen/2025/fakten-desinformation.html>
- <https://www.verfassungsschutz.de/SharedDocs/hintergruende/DE/spionage-und-proliferationsabwehr/gefahrdung-der-bundestagswahl-2025-durch-unzulaessige-auslaendische-einflussnahme.html>

Links zu Desinformation im Kontext des russischen Überfalls auf die Ukraine:

- <https://www.bmi.bund.de/SharedDocs/faqs/DE/themen/heimat/desinformation/faq-liste-desinformation.html>
- https://germany.representation.ec.europa.eu/13-mythen-uber-den-krieg-russlands-der-ukraine-und-die-wahrheit_de
- <https://www.isdglobal.org/isd-publications/two-years-on-an-analysis-of-russian-state-and-pro-kremlin-information-warfare-in-the-context-of-the-invasion-of-ukraine/>

Faktenchecks und Hintergründe:

- <https://www.bundesregierung.de/breg-de/schwerpunkte/umgang-mit-desinformation/falschmeldungen-erkennen-1750146>
- <https://euvsdisinfo.eu/de/>
- <https://www.bpb.de/themen/medien-journalismus/stopfakenews/>
- <https://dpa-factchecking.com/germany/>
- <https://www.tagesschau.de/faktenfinder>
- <https://www.zdf.de/nachrichten/thema/zdf-investigativ-100.html>

Deepfakes und generative KI:

- <https://www.swp-berlin.org/publikation/deepfakes-wenn-wir-unseren-augen-und-ohren-nicht-mehr-trauen-koennen>
- <https://www.aisec.fraunhofer.de/de/das-institut/wissenschaftliche-exzellenz/Deepfakes.html>
- <https://faktencheck.afp.com/doc.afp.com.33C62E6>

5. Entlarvte Desinformationen – zwei Beispiele

5.1. Der angebliche Spendenaufruf der Sächsischen Landesbibliothek

Russische Bücher als Heizmaterial? Was absurd klingt, war im September 2022 tatsächlich Inhalt einer Desinformation über die Sächsische Landesbibliothek – Staats und Universitätsbibliothek Dresden (SLUB). In sozialen Netzwerken und Messenger-Diensten wie Facebook, TikTok, „X“ (vormals Twitter) und Telegram wurde das Foto eines gefälschten Schreibens geteilt, das den Eindruck erwecken sollte, die Generaldirektorin der SLUB bitte um die Spende von Büchern russischer Autoren, um diese für Heizzwecke in der Bibliothek zu verwenden. Um dessen Echtheit vorzutäuschen, enthielt das ausschließlich online kursierende Schreiben das Logo der SLUB und als Absender die Adresse der Bibliotheksverwaltung sowie den Kontakt der Generaldirektorin. Der gefälschte Aufruf zu Bücherspenden schloss mit der Bemerkung: „Auf diese Weise können Sie auch dann noch gute Bücher lesen, wenn Putin die Gaszufuhr unterbricht.“

Die SLUB entlarvte die Desinformationskampagne, indem sie sich umgehend an die Öffentlichkeit (in deutscher, englischer und russischer Sprache) wandte und Strafanzeige erstattete. „Bitte verbreiten Sie die Falschinformation nicht weiter und unterstützen sie uns, indem Sie dafür sensibilisieren, dass es sich hierbei um eine gezielte Desinformation handelt“, schrieb die Bibliothek in ihrer Klarstellung kurz nach Bekanntwerden des gefälschten Schreibens. Den bisherigen Ermittlungen zufolge erfolgte die erste Veröffentlichung des Fake-Schreibens über einen russischen Telegram-Kanal.

- <https://blog.slub-dresden.de/beitrag/2022/9/2/fake-news-zur-slub-in-den-sozialen-netzwerken>

5.2. Vermeintliche Millionen-Abfindung für ukrainischen General

Der General Walerij Saluschnyj wurde im Februar 2024 als Oberbefehlshaber der ukrainischen Streitkräfte entlassen. In den sozialen Netzwerken tauchte daraufhin ein gefälschtes Nachrichtenvideo im Stil der britischen BBC auf, in dem behauptet wird, Saluschnyj habe eine inoffizielle Abfindung in Höhe von 53 Millionen US-Dollar erhalten. Das Video beruft sich dabei auf angebliche Informationen des internationalen Recherchenetzwerks „Bellingcat“. Demnach sei die Zahlung Teil einer Vereinbarung, damit General Saluschnyj seine politischen Ambitionen begrabe und die Ukraine verlasse. In dem gefälschten Nachrichtenvideo ist links das BBC-Logo zu sehen.

Dass das vermeintliche BBC-Video eine Fälschung ist, stellte der BBC-Journalist Shayan Sardarizadeh auf der Social-Media-Plattform „X“ (vormals Twitter) klar. Auch die Organisation „Bellingcat“ meldete sich auf „X“ zu Wort und erklärte, das Video und die angebliche Recherche seien gefälscht. Ein authentischer Bericht zu der vermeintlichen Abfindung des ukrainischen Oberbefehlshabers findet sich auf keiner Webseite der beiden Organisationen. Nach Recherchen der dpa ließen sich auch unabhängig von dem gefälschten Video keine Hinweise über eine angebliche Millionenabfindung für den ukrainischen General finden. Korrekt ist stattdessen, dass Walerij Saluschnyj neuer ukrainischer Botschafter in Großbritannien werden soll. Laut dem ukrainischen Außenministerium habe sich Präsident Wolodymyr Selenskyj für die Berufung Saluschnyjs ausgesprochen.

- <https://dpa-factchecking.com/germany/240314-99-337531/>

Herausgeber

Landesamt für Verfassungsschutz Sachsen
Referat Presse- und Öffentlichkeitsarbeit
Neuländer Straße 60
01129 Dresden
www.verfassungsschutz.sachsen.de

Titelbild

pixabay.com/viarami

Redaktionsschluss

April 2024 (aktualisiert im Januar 2025)

Hinweis

Diese Publikation wird im Rahmen der Öffentlichkeitsarbeit vom Landesamt für Verfassungsschutz Sachsen kostenlos herausgegeben. Sie ist nicht zum Verkauf bestimmt und darf nicht zur Wahlwerbung politischer Parteien oder Gruppen eingesetzt werden.

Diese Maßnahme wird mitfinanziert durch Steuermittel auf der Grundlage des vom Sächsischen Landtag beschlossenen Haushaltes.

Copyright

Diese Veröffentlichung ist urheberrechtlich geschützt. Alle Rechte, auch die des Nachdruckes von Auszügen und der fotomechanischen Wiedergabe, sind dem Herausgeber vorbehalten