ISD | Institute for Strategic Dialogue

Vorsicht, manipuliert!

Ein Leitfaden für Kommunikationsverantwortliche aus Abgeordnetenbüros, Ministerien und Behörden

Mauritius Dorn & Solveig Barth

Über das Projekt AHEAD

Als Informations- und Dialogreihe trägt Projekt AHEAD dazu bei, ein integriertes Verständnis zu den Vektorthemen der Desinformation aufzubauen. Dazu gehören die Themenfelder »Globale Gesundheit«, »Migration«, »Geschlechtergerechtigkeit« und »Klimawandel« sowie die Schnittstellen zu verwandten Methoden extremistischer Bewegungen und autoritärer Staaten. Zudem unterstützt das Projekt die Stärkung der strategisch-kommunikativen Handlungsfähigkeit der Politik, um vor die Kurve hybrider Demokratiegefahren zu gelangen. Das Projekt wird als Pilot durchgeführt und soll perspektivisch skaliert werden. Wir danken der Bill & Melinda Gates Foundation für die Projektunterstützung.

Über diesen Leitfaden

Das Ausmaß an Desinformation hat in den vergangenen Jahren stark zugenommen. Vor diesem Hintergrund ermöglicht dieser Leitfaden Kommunikationsverantwortlichen aus Abgeordnetenbüros, Ministerien und Behörden einen niedrigschwelligen Einstieg in den strategisch-kommunikativen Umgang mit Informationsmanipulation. Im Gegensatz zur Desinformation umfasst Informationsmanipulation auch weitere manipulative Aktivitäten wie zum Beispiel die Verbreitung propagandistischer Inhalte oder die Einrichtung von Bot-Netzwerken. Der Leitfaden stützt sich dabei zum Teil auf wissenschaftliche Befunde, zum Teil auf normative Annahmen und Erfahrungswerte im Rahmen der Projektarbeit.

Über die Autor:innen

Mauritius Dorn ist Senior Digital Policy & Education Manager beim ISD Germany. Er leitet das Projekt AHEAD und unterstützt das Digital Policy Lab (DPL) als Experte für internationale Digitalpolitik.

Solveig Barth ist Project Coordinator beim ISD Germany. Im Rahmen von Projekt AHEAD und der CCOA unterstützt sie Politik und Gesellschaft bei der Bekämpfung von Desinformation und Antisemitismus.

Herausgeberische Verantwortung:

Huberta von Voss, Executive Director ISD Germany

ISD | Institute for Strategic Dialogue

www.isdgermany.org

Inhaltsverzeichnis

Einführung:
Informationsmanipulation als strategisches Instrument

Bereits im Jahr 1710, als Tageszeitungen an Bedeutung gewannen, kritisierte der irische Satiriker Jonathan Swift, dass die Falschheit flöge und die Wahrheit hinterherhinke. Mehr als 300 Jahre später hat sich an dieser Beobachtung wenig geändert. Zwar halten die meisten klassischen Medien aus einem tradierten Eigenanspruch heraus journalistische Gütekriterien zur Wahrheitsprüfung ein, doch können Influencer:innen und andere neue Gatekeeper des politischen Informationsflusses nach wie vor weitgehend unreguliert Inhalte verbreiten. Sie müssen sich vor allem an die Geschäftsbedingungen der digitalen Dienste – auch Gemeinschaftsstandards genannt – halten, die bislang häufig nur halbherzig durchgesetzt werden. Dies soll das neue europäische Gesetz über digitale Dienste (Digital Services Act, DSA) ändern, das nicht nur horizontale Regeln für Hostingdiensteanbieter zur Einrichtung von Meldewegen für rechtswidrige Inhalte vorschreibt, sondern von allen Anbietern von Vermittlungsdiensten auch eine sorgfältige, objektive und verhältnismäßige Durchsetzung der Standards einfordert. Zudem sollen sogenannte systemische Risiken wie zum Beispiel die Verbreitung rechtswidriger Inhalte oder negative Auswirkungen auf die gesellschaftliche Debatte endlich bewertet und gemindert werden.

Die Einführung dieser neuen Verpflichtungen ist auch eine Antwort auf die massive Zunahme gesellschaftlicher Polarisierung, extremistischer Bewegungen und abstruser Halbwahrheiten und Propagandabotschaften in den letzten Jahren. Diese boten den Hintergrund für Straftaten in der Offline-Welt und diverse terroristische Attacken. Insbesondere die Manipulation von Informationen wie zum Beispiel koordinierte Desinformationskampagnen haben sich mittlerweile zu einem bewährten Instrument extremistischer Bewegungen und autoritärer Staaten entwickelt. Diesen Akteur:innen geht es meistens darum, Oppositionelle aus dem digitalen Informationsraum zu drängen oder Misstrauen zu säen und so den politischen Meinungsbildungsprozess zu untergraben. Das bekannteste Beispiel hierfür ist die US-Präsidentschaftswahl 2016, bei der erhebliche Informationsmanipulation durch die russische Regierung nachgewiesen werden konnte.[1] Besonders in Krisensituationen wie zum Beispiel Kriege, Pandemien oder Umweltkatastrophen ist diese Strategie erfolgsversprechend. Hier neigen die Menschen dazu, außergewöhnlich aufmerksam zu sein und nehmen nicht selten einen Kontrollverlust war. Entstehende Informationsvakua werden wiederum von den Akteur:innen der Informationsmanipulation gefüllt, die dabei teilweise unterschiedliche Absichten verfolgen. Gleichzeitig überlappen sich ihre manipulativen Aktivitäten und die dabei verwendeten Inhalte zunehmend. Angesichts der Fortschritte im Bereich der Künstlichen Intelligenz (KI) wie zum Beispiel Bild- und Textgeneratoren könnte es für sie in den nächsten Jahren noch einfacher werden, Informationsräume zu manipulieren.

Für Kommunikationsverantwortliche aus Abgeordnetenbüros, Ministerien und Behörden bedeutet dies eine Herkulesaufgabe. Zum einen geht es für sie darum, eigene Botschaften so zu verbreiten, dass sie in umkämpften digitalen Informationsräumen weiterhin die Bürger:innen erreichen. Zum anderen müssen sie sich selbst vor Informationsmanipulation wie zum Beispiel koordinierten Desinformationskampagnen oder dem Diebstahl privater Informationen schützen. Dieser Leitfaden nimmt sich dieser Probleme an und unternimmt den Versuch, einen niedrigschwelligen Einstieg in den Umgang mit Informationsmanipulation zu ermöglichen. Da-

»DIESEN AKTEUR:INNEN GEHT ES MEISTENS DARUM, OPPOSITIONELLE AUS DEM DIGITALEN INFORMATIONSRAUM ZU DRÄNGEN ODER MISSTRAUEN ZU SÄEN UND SO DEN POLITISCHEN MEINUNGSBILDUNGSPROZESS ZU UNTERGRABEN.«

»DIESER LEITFADEN NIMMT SICH DIESER PROBLEME AN UND UNTERNIMMT DEN VERSUCH, EINEN NIEDRIGSCHWELLIGEN EINSTIEG IN DEN UMGANG MIT INFORMATIONSMANIPULATION ZU ERMÖGLICHEN.«

bei stützt er sich zum Teil auf wissenschaftliche Befunde, zum Teil auf normative Annahmen und Erfahrungswerte im Rahmen der Projektarbeit. Kapitel 1 führt in zentrale Begrifflichkeiten ein und grenzt diese voneinander ab. Kapitel 2 zeigt Auswirkungen von Informationsmanipulation auf die politische Arbeit auf. Kapitel 3 geht der Frage nach, welche Handlungsmöglichkeiten Kommunikationsverantwortliche überhaupt haben. Kapitel 4 führt in die systematische Erkennung von Informationsmanipulation ein. Kapitel 5 stellt wiederum ein integriertes Bewertungs- und Handlungsmodell vor, das bei der zielgerichteten Bekämpfung von Informationsmanipulation hilft.

Kapitel 1:

Relevante Begrifflichkeiten sicher verwenden

Wenn von pseudo-journalistischen Inhalten die Rede ist, fällt im allgemeinen Sprachgebrauch häufig das Stichwort »Fake News«. Fake News meint jedoch nicht nur eine Inhalte-Kategorie, sondern wird als politischer Kampfbegriff auch immer wieder zur Diffamierung unliebsamer Meinungen und Medien missbraucht. Der ehemalige US-Präsident Donald Trump etwa nutzt den Begriff seit 2016 regelmäßig, um das gegnerische Lager zu diskreditieren und sich und seine Verbündeten somit als vertrauenswürdige Akteur:innen zu inszenieren. In Deutschland wird wiederum vor allem der Begriff »Lügenpresse« als Instrument der Delegitimierung eingesetzt. Aufgrund dieser Entwicklung ist es für Kommunikationsverantwortliche ratsam von der Verwendung des Begriffs »Fake News« abzusehen und stattdessen auf Begriffe wie »Fehlinformationen«, »Desinformation«, »Malinformation« und »Informationsmanipulation« zurückzugreifen. Um eine ähnliche Entwicklung wie beim Begriff »Fake News« zu vermeiden, sollten diese dabei sparsam und treffsicher verwendet werden. Im Folgenden werden die Begriffe ausführlich erläutert und voneinander abgegrenzt.

»FAKE NEWS MEINT NICHT NUR EINE INHALTE-KATEGORIE, SONDERN WIRD ALS POLITISCHER KAMPFBEGRIFF AUCH IMMER WIEDER ZUR DIFFAMIERUNG UNLIEBSAMER MEINUNGEN UND MEDIEN MISSBRAUCHT.«

Fehlinformationen

Laut Europäischer Kommission beziehen sich Fehlinformationen auf **»falsche oder irreführende Inhalte, die ohne vorsätzliche Schädigungsabsicht weitergegeben werden, deren Auswirkungen jedoch schädlich sein können.«**[2] Fehlinformationen treten insbesondere im privaten Raum auf – beispielsweise dann, wenn falsche oder irreführende Inhalte von Personen gutgläubig an Bekannte und Familienangehörige weitergeleitet werden. Dazu gehören handwerkliche Recherchefehler, unklare Sachlagen oder Zweifelsfälle, missverständliche Formulierungen, genauso wie spielerische, witzige oder ironische Äußerungen, die satirisch gemeint sind oder einen Irrglauben in die Welt setzen.[3] Der Begriff ist dabei nicht unproblematisch. Zur Bestimmung der Wahrheit wird gemeinhin auf den Konsens unter Expert:innen und/oder die besten verfügbaren Erkenntnisse vertraut. Diese können sich jedoch mit der Zeit ändern, da Wissenschaft vom Erkenntnisgewinn lebt und sich die Grenzen zwischen Konsens und Kontroverse fortlaufend verschieben. Zum Beispiel legten die besten verfügbaren Erkenntnisse direkt nach der US-Präsidentschaftswahl 2016 nahe, dass eine Einflussnahme Russland nicht existiert habe. Dies änderte sich zu einem späteren Zeitpunkt, als mehr Beweise vorlagen. Folglich sollte bei der Verwendung des Begriffs transparent gemacht werden, welche Annahmen über Konsens und Erkenntnisse getroffen werden.[4]

»HÄUFIG WIRD AUCH DER BEGRIFF ›VERSCHWÖRUNGSTHEORIEN‹ VERWENDET. DIESER BEGRIFF SOLLTE JEDOCH NICHT GENUTZT WERDEN, DA ER FÄLSCHLICHERWEISE EINE WISSENSCHAFTLICHE GRUNDLAGE IMPLIZIERT.«

»Verschwörungserzählungen« als eine spezifische Kategorie von Fehlinformationen lassen sich kaum überprüfen, da sich die Existenz einer Verschwörung den Möglichkeiten der Wahrheitsprüfung entzieht. Dennoch können solche Erzählungen durchaus schädliche Auswirkungen auf das Individuum oder die Gesellschaft haben. Ein Beispiel ist die sogenannte QAnon-Verschwörungserzählung, die – aus den Vereinigten Staaten kommend – mittlerweile auch in souveränistischen Milieus wie zum Beispiel Reichsbürger:innen in Deutschland zunehmend rezipiert wird, was zur weiteren Radikalisierung beitragen kann.

Verschwörungserzählungen, -mythen oder -theorien?

Verschwörungserzählungen wie zum Beispiel »QAnon« beziehen sich auf sinnstiftende Annahmen, die sich meist aus übergeordneten und abstrakten »Verschwörungsmythen« wie der antisemitischen Ritualmordlegende speisen. QAnon behauptet etwa, es gebe einen geheimen Krieg zwischen einer globalen Intrige von Kinderblut trinkenden Pädophilen und dem ehemaligen US-Präsident Donald Trump, wobei anonyme Online-Beiträge als vermeintlicher Insider (»Q«) dienen. Dabei vereinen solche Erzählungen meistens auch ein loses Netzwerk von »Verschwörungsgläubigen«. Häufig wird auch der Begriff »Verschwörungstheorien« verwendet. Dieser Begriff sollte jedoch nicht genutzt werden, da er fälschlicherweise eine wissenschaftliche Grundlage impliziert. Verschwörungsideologische Milieus gebrauchen gemeinhin keine wissenschaftlichen Methoden zur Überprüfung ihrer Thesen einer angeblichen Verschwörung.[5]

Desinformation

Liegt der Umstand vor, dass es sich um eine absichtliche Verbreitung von Fehlinformationen handelt, so wird von »Desinformation« gesprochen. Entsprechend definiert die Bundesregierung Desinformation als »nachweislich falsche oder irreführende Informationen, die mit dem Ziel der vorsätzlichen Beeinflussung oder Täuschung der Öffentlichkeit verbreitet werden«.[6] Dabei liegt der Fokus wie bei Fehlinformationen auf den Inhalten selbst. Hinsichtlich der Problematik des Phänomens wird auf die Beeinflussung oder Täuschung der Öffentlichkeit verwiesen, nicht aber auf ein konkretes Schadenspotenzial.

»DIE DEFINITION VON DESINFORMATION ALS INHALT ODER AKTIVITÄT IST ENTSCHEIDEND, DA DIES MASSGEBLICH DIE WEITERE OPERATIONALISIERUNG DES PHÄNOMENS BEEINFLUSST.«

Einen anderen Weg beschreitet die Europäische Kommission. Sie definiert Desinformation als **»die Verbreitung falscher oder irreführender Inhalte, die der Öffentlichkeit schaden können, in der Absicht, andere zu täuschen oder wirtschaftlich oder politisch daraus Kapital zu schlagen.«**[7] Damit greift sie explizit das Potenzial auf, Schäden anzurichten, und verweist auch auf wirtschaftliche und politische Motive neben der Täuschung. Diese Konkretisierung verweist auf die große Bedeutung der Monetarisierung im Bereich der Desinformation: Die Einrichtung verschwörungsideologischer Kanäle, um nebenbei überteuerte Produkte im eigenen Online-Shop zu verkaufen; die Durchführung einer gezielten Desinformationskampagne im Auftrag der Politik; oder die Einrichtung von Nachrichtenseiten und Blogs mit sensationalistischen Inhalten, um über Werbeanzeigen Geld zu verdienen. Neben diesem wichtigen Aspekt gibt es aber auch einen weniger offensichtlichen aber dennoch entscheidenden Unterschied. So macht die Europäische Kommission die Verbreitung der Inhalte zum Gegenstand ihrer Definition. Die Definition von Desinformation als Inhalt oder Aktivität ist entscheidend, da dies maßgeblich die weitere Operationalisierung des Phänomens beeinflusst. Im Strafgesetzbuch (StGB) deckt sich der Straftatbestand der »Verleumdung« (§ 187) mit einer verhaltensorientierten Definition von Desinformation. Allerdings geht es hier um Inhalte, die die Ehre einer anderen Person verletzen.

Malinformation

Potenziell schädliche Aktivitäten und Inhalte müssen nicht immer falsch oder irreführend sein, um der Öffentlichkeit oder Individuen schaden zu können. Im Dezember 2018 veröffentlichte ein 20-jähriger Hacker gestohlene Kontakt- und Kommunikationsdaten von mehr als 1000 Prominenten in Deutschland – darunter der gesamte E-Mailverkehr samt Anhängen eines Abgeordneten und persönliche Daten der ehemaligen Bundeskanzlerin Angela Merkel.[8] Dabei waren diese Inhalte teilweise manipuliert (Desinformation). Die öffentliche Verbreitung persönlicher, mitunter intimster Inhalte ohne Einwilligung der betroffenen Person wird als sogenanntes »Doxing« bezeichnet. Im beschriebenen Fall war das hintergründige Motiv Ärger über öffentliche Äußerungen der Betroffenen. Genauso wird Doxing aber auch aus rein politischen und wirtschaftlichen Motiven eingesetzt. Neben anderen Aktivitäten wie zum Beispiel »Phishing« – der Nutzung betrügerischer Mitteilungen, um an persönliche Inhalte zu gelangen – ist Doxing eine Subkategorie von »Malinformation«. Die Forscher:innen Claire Wardle und Hossein Derakhshan definieren den Begriff als **»Informationen, die auf der Realität beruhen und dazu dienen, einer Person, Organisation oder Land zu schaden.«**[9] Im Gegensatz zu Desinformation fallen hierunter alle Formen von Meinungsmache und Propaganda, die falsche Realitäten zeigen, indem Inhalte nur sehr einseitig, bruchstückhaft oder unvollständig verwendet werden.[10] Problematisch ist dabei vor allem die fehlende Kontextualisierung wahrer Inhalte, die ein Schadensrisiko herbeiführt.

»DIE ÖFFENTLICHE VERBREITUNG PERSÖNLICHER, MITUNTER INTIMSTER INHALTE OHNE EINWILLIGUNG DER BETROFFENEN PERSON WIRD ALS SOGENANNTES ›DOXING‹ BEZEICHNET.«

Informationsmanipulation

Die Begriffe »Fehlinformationen«, »Desinformation« und »Malinformation« beziehen sich allesamt auf Phänomene entlang der Dichotomie wahr/falsch. Dabei teilen sie die Fokussierung auf Inhalte oder die Verbreitung von Inhalten, die Schaden anrichten können. Andere Aktivitäten wie etwa die Produktion der Inhalte oder ausgeklügelte und koordinierte Techniken der Beeinflussung wie zum Beispiel Social Bots sind nicht explizit benannt. Um diese Leerstelle definitorisch zu schließen, haben Expert:innen der französischen Außen- und Verteidigungsministerien im Jahre 2018 den Begriff »Informationsmanipulation« eingeführt. Sie definierten diese als koordinierte Kampagne, bei der falsche oder bewusst verzerrte Inhalte mit politischer Absicht verbreitet werden, um Schaden anzurichten.

»DAMIT LIEGT DER FOKUS EINDEUTIG AUF EINER AKTIVITÄT UND NICHT AUF DEN INHALTEN, SELBST WENN WAHRE ABER SCHÄDLICHE INHALTE NICHT AUSGESCHLOSSEN WERDEN.«

Der Europäische Auswärtige Dienst (EEAS) hat diese Definition in den Folgejahren nochmals erweitert und den Begriff »Foreign Information Manipulation and Interference« (FIMI) eingeführt.[11] Unter FIMI versteht der EEAS dabei **»ein meist nicht rechtswidriges Verhaltensmuster, das Werte, Verfahren und politische Prozesse bedroht oder das Potenzial hat, diese negativ zu beeinflussen. Eine derartige Aktivität hat einen manipulativen Charakter und wird von staatlichen oder nichtstaatlichen Akteur:innen, einschließlich ihrer Stellvertreter:innen innerhalb und außerhalb ihres eigenen Hoheitsgebiets, absichtlich und in koordinierter Weise durchgeführt.«** Damit liegt der Fokus eindeutig auf einer Aktivität und nicht auf den Inhalten, selbst wenn wahre aber schädliche Inhalte nicht ausgeschlossen werden. Zudem rücken besonders solche Aktivitäten in den Vordergrund, die ein Schadenspotenzial für die Grundpfeiler der Demokratie darstellen. In Bezug auf die Akteur:innen erfolgt jedoch eine Eingrenzung. So geht es um Verhaltensmuster mit Ursprung im Ausland, die aber auch von inländischen Stellvertreter:innen angewandt werden. Der Bezug ins Ausland ist aber dennoch ein zentraler Aspekt von FIMI.

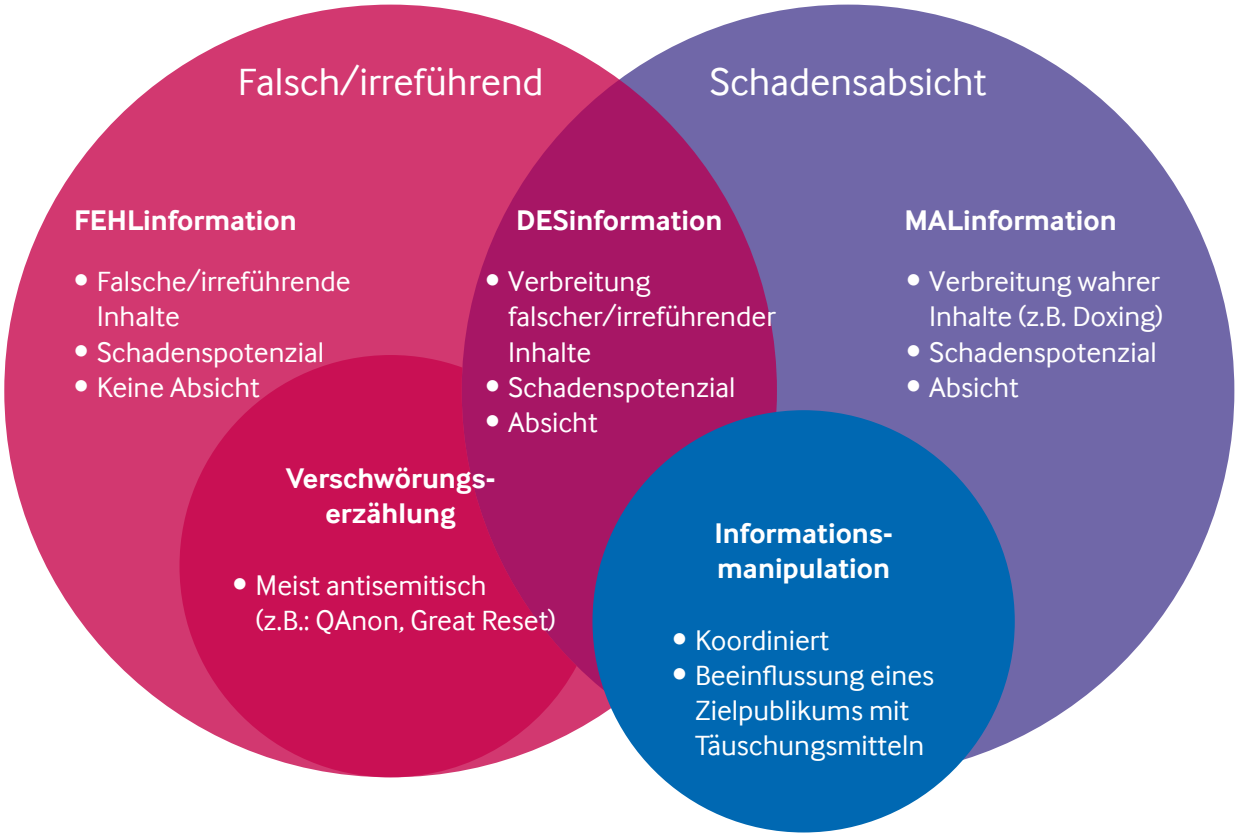


Abb. 1: Informationsordnung[12]

In Bezug auf die Vielseitigkeit der praktischen Herausforderungen für Kommunikationsverantwortliche aus Abgeordnetenbüros, Ministerien und Behörden ist der FIMI-Begriff zwar besser geeignet als die anderen Begriffe. Trotzdem sehen sich Kommunikationsverantwortliche in der Praxis – insbesondere solche aus Abgeordnetenbüros – häufig auch koordinierten Desinformationskampagnen mit Ursprung im Inland ausgesetzt. Außerdem ist es mit ansteigendem Manipulationsgrad der Vorfälle zunehmend schwieriger, den Bezug zu ausländischen Akteur:innen nachzuweisen. Um diesem praktischen Umstand gerecht zu werden, aber auch die thematische Breite von Informationsmanipulation abzudecken soll Informationsmanipulation im Kontext dieses Leitfadens folgende Eigenschaften aufweisen:

- Manipulative Aktivität
- Meist nicht rechtswidrig
- Schadenspotenzial
- Schadensabsicht
- Koordinierte Durchführung
- Ursprung im In- und Ausland

In den folgenden Kapiteln dieses Leitfadens soll sich mit der Frage beschäftigt werden, wie Kommunikationsverantwortliche mit Informationsmanipulation umgehen sollten. Eine Voraussetzung hierfür ist jedoch, dass das eigene Mandat gerade im Bereich der Öffentlichkeitsarbeit geklärt wird. Im nächsten Kapitel geht es aber zunächst um die Auswirkungen der in diesem Kapitel vorgestellten Phänomene auf die politische Arbeit.

Kapitel 2:
Auswirkungen auf die politische Arbeit wahrnehmen

Ursache-Wirkung-Beziehungen im digitalen Zeitalter sind besonders wechselseitig und entwickeln sich fortlaufend weiter. In anderen Worten: Der digitale Informationsraum prägt immer stärker gesellschaftliche Trends. Gleichzeitig spielt die Gesellschaft auch eine wichtige Rolle bei der Entwicklung des digitalen Informationsraums. Häufig ist die Rede davon, dass Online-Plattformen bestimmte gesellschaftliche Probleme verstärken würden, statt komplett neue Probleme zu erzeugen. Obgleich nach wie vor mehr Forschung in diesem Bereich dringend erforderlich ist, nimmt die Bedeutung von Informationsmanipulation für die gesellschaftliche Debatte und politische Initiativen stetig zu. Im Folgenden wird eine Übersicht über einige zentrale Befunde und Schlussfolgerungen im Hinblick auf die Beeinträchtigung der politischen Arbeit gegeben.

Untergrabung des gesellschaftlichen Debattenklimas

Immer dann, wenn Ereignisse eintreten, für die es keine einfachen Erklärungen gibt und die eine wichtige Rolle für das alltägliche Leben spielen, sind die Erfolgschancen für manipulative Aktivitäten groß. Während der COVID-19-Pandemie konnten russische Staatsmedien sich etwa bei rechtsextremen, impfskeptischen und verschwörungsideologischen Milieus in Deutschland als wichtige Nachrichtenquelle etablieren.[13] Dabei griffen sie gezielt COVID-19- und impfskeptische Narrative auf, während die russische Regierung im Inland parallel ihre eigene Impfkampagne bewarb.[14] Diese manipulativen Aktivitäten dürften die öffentliche Gesundheit in Deutschland nega-

tiv beeinflusst haben. In einer Übersichtsstudie vom September 2022 kam die Weltgesundheitsorganisation (WHO) zum Schluss, dass die »Verbreitung unzuverlässiger Erkenntnisse über Gesundheitsfragen der Impfskepsis Vorschub [geleistet] und Behandlungen [begünstigt hat], deren Wirkung nicht nachgewiesen ist.«[15]

Wichtig ist dabei nicht, dass Regierungsmaßnahmen kritisiert wurden, sondern, dass die Inhalte koordiniert und mit Schadensabsicht verbreitet wurden. Zu einem späteren Zeitpunkt wurde das aufgebaute Medienvertrauen dann instrumentalisiert, um Kriegspropaganda zu verbreiten und gegen die Bundesregierung insgesamt aufzuwiegeln.[16] Ähnliches lässt sich bei anderen herausfordernden Themen wie »Geschlechtergerechtigkeit«, »Migration« und »Klimawandel« beobachten. Hier stellt Informationsmanipulation ebenfalls ein großes Problem für die Lösung der Herausforderungen dar. So heißt es in einem Bericht des anerkannten Weltklimarates (IPCC), dass »Rhetorik und Fehlinformationen über den Klimawandel und die absichtliche Untergrabung der Wissenschaft dazu beigetragen [haben], dass der wissenschaftliche Konsens falsch wahrgenommen wird, dass Ungewissheit herrscht, dass Risiken und Dringlichkeit missachtet werden und dass es zu Meinungsverschiedenheiten kommt«.[17] Dabei greifen autoritäre Staaten wie Russland zunehmend in die gesellschaftlichen Debatte über den Klimawandel ein.[18] Eigene Narrative knüpfen hierbei immer wieder an existierende Verschwörungserzählungen an. Aus gutem Grund: Laut einer repräsentativen Befragung unter wahlberechtigten Deutschen vom 11.07. bis 09.08.2022 stimmten 54 Prozent der Befragten mindestens einer Verschwörungserzählung zu, mehr als ein Drittel zwei Erzählungen.[19] Damit sind Verschwörungserzählungen wie extremistisches Gedankengut längst in der Mitte der Gesellschaft angekommen. Die Verbreitung einzelner Fehlinformationen ist dabei unproblematisch. Laut Verfassungsschutz kann Desinformation aber durch »das Zusammenwirken der vielfältigen Desinformationsaktivitäten und wenn es einem Akteur gelingt, Themen frühzeitig zu besetzen [...] dazu beitragen, ein Klima von Ablehnung, Skepsis oder Misstrauen aufzubauen oder anzufachen.«[20] Dies trägt zur Verzerrung des Meinungsbildungsprozesses bei.

»ZU EINEM SPÄTEREN ZEITPUNKT WURDE DAS AUFGEBAUTE MEDIENVERTRAUEN DANN INSTRUMENTALISIERT, UM KRIEGSPROPAGANDA ZU VERBREITEN UND GEGEN DIE BUNDESREGIERUNG INSGESAMT AUFZUWIEGELN.«

Diffamierung von Politikerinnen

Laut Oxford Internet Institute haben im Jahre 2020 81 Staaten organisierte Desinformationskampagnen und andere manipulative Aktivitäten durchgeführt, um Wahlen im Inland zu beeinflussen, oder um geopolitisch daraus Kapital zu schlagen.[21] Dabei wurde Informationsmanipulation insbesondere auch von politischen Parteien eingesetzt, um politische Gegner:innen zu diffamieren. Manipulative Aktivitäten, die sich gegen Personen richten, sind besonders dann erfolgreich, wenn sie verwurzelte Vorurteile und Stereotype aufgreifen. Damit verwundert es nicht, dass häufig Frauen und Minderheiten betroffen sind.[22] Im Vorfeld der Bundestagswahl 2021 wurde vor allem Annalena Baerbock, damalige Spitzenkandidatin von BÜNDNIS 90/DIE GRÜNEN, wesentlich öfter von rechtsextremen und verschwörungsaffinen Milieus angegriffen, abqualifiziert, mit sexuellen Herabsetzungen und Androhungen von Gewalt überzogen wurde als ihre männlichen Wettbewerber der anderen politischen Parteien.

»VON INFORMATIONSMANIPULATION IST JEDOCH NICHT NUR DIE BUNDESEBENE BETROFFEN, SONDERN AUCH POLITIKER:INNEN AUF LANDES- UND KOMMUNALEBENE.«

Dabei wurden gerade solche Narrative eingesetzt, welche an die Verschwörungserzählung »The Great Reset« anknüpften.[23] Diese suggerierten, Baerbock sei Mitglied einer globalen Verschwörung «dunkler Kräfte«, mit dem Ziel, eine »neue Weltordnung« einzurichten. Im Jahre 2022 wurde Baerbock erneut zum Ziel, indem Kreml-nahe Konten dekontextualisierte und manipulierte Versionen eines Baerbock-Zitats koordiniert verbreiteten.[24] Wenig später trendeten die Hashtags

#Hochverrat und #BaerbockRuecktritt auf den Online-Plattformen. Ein klassisches Leitmedium teilte ebenfalls zunächst eine falsche Version des Zitats als Schlagzeile, bevor diese später korrigiert wurde. Von Informationsmanipulation ist jedoch nicht nur die Bundesebene betroffen, sondern auch Politiker:innen auf Landes- und Kommunalebene. Im Sommer 2022 wurde Franziska Gifffey, damalige Berliner Bürgermeisterin, sowie andere europäische Politiker:innen in einen Video-Call mit einem manipulierten Video von Vitali Klitschko, Bürgermeister von Kiew, verwickelt (siehe Abb. 2). Nachträglich bekannten sich die russischen TV-Unterhalter Kusnezow und Stoljarow zu dem Vorfall. Diese unterhalten wiederum eine eigene Show auf Rutube, der russischen YouTube-Alternative, die zum Imperium des staatlich beaufsichtigten Gazprom-Konzerns gehört. Damit ist zumindest von einer Mitwisserschaft der russischen Regierung auszugehen.

Die meisten solcher Aktivitäten und Inhalte bewegen sich im Rahmen der Legalität. Dennoch können manipulative Aktivitäten wie die Verbreitung manipulierter Videos oder gar Deepfakes – täuschend echt wirkende, synthetische Medieninhalte, die mithilfe von KI generiert werden – einen erheblichen Beitrag zur Reputationsschädigung der Betroffenen leisten. Es gibt nachweisliche Fälle von Politiker:innen, die sich in der Folge solcher digitalen Angriffe bei bestimmten Themengebieten selbst zensieren, diese komplett meiden oder sich gar komplett aus dem digitalen Informationsraum zurückziehen.[25] Ein solches »Silcencing« kann die Meinungsvielfalt beeinträchtigen und stellt damit eine Gefahr fürs Funktionieren liberaler Demokratien dar.

Für Kommunikationsverantwortliche bedeuten diese Entwicklungen, dass sie sich mit Blick auf die politische Arbeit ihres Abgeordnetenbüros, Ministerium oder Behörde auf potenzielle Informationsmanipulation wie zum Beispiel koordinierte Desinformationskampagnen vorbereiten müssen. Bevor es dabei um konkrete Schritte und den Kapazitätsaufbau geht, müssen jedoch zunächst die Handlungsspielräume beim kommunikativen Umgang mit Informationsmanipulation dingend definiert werden, um das eigene Vorgehen auf eine stabile Grundlage zu stellen. Im nächsten Kapitel wird diese Thematik daher näher beleuchtet.

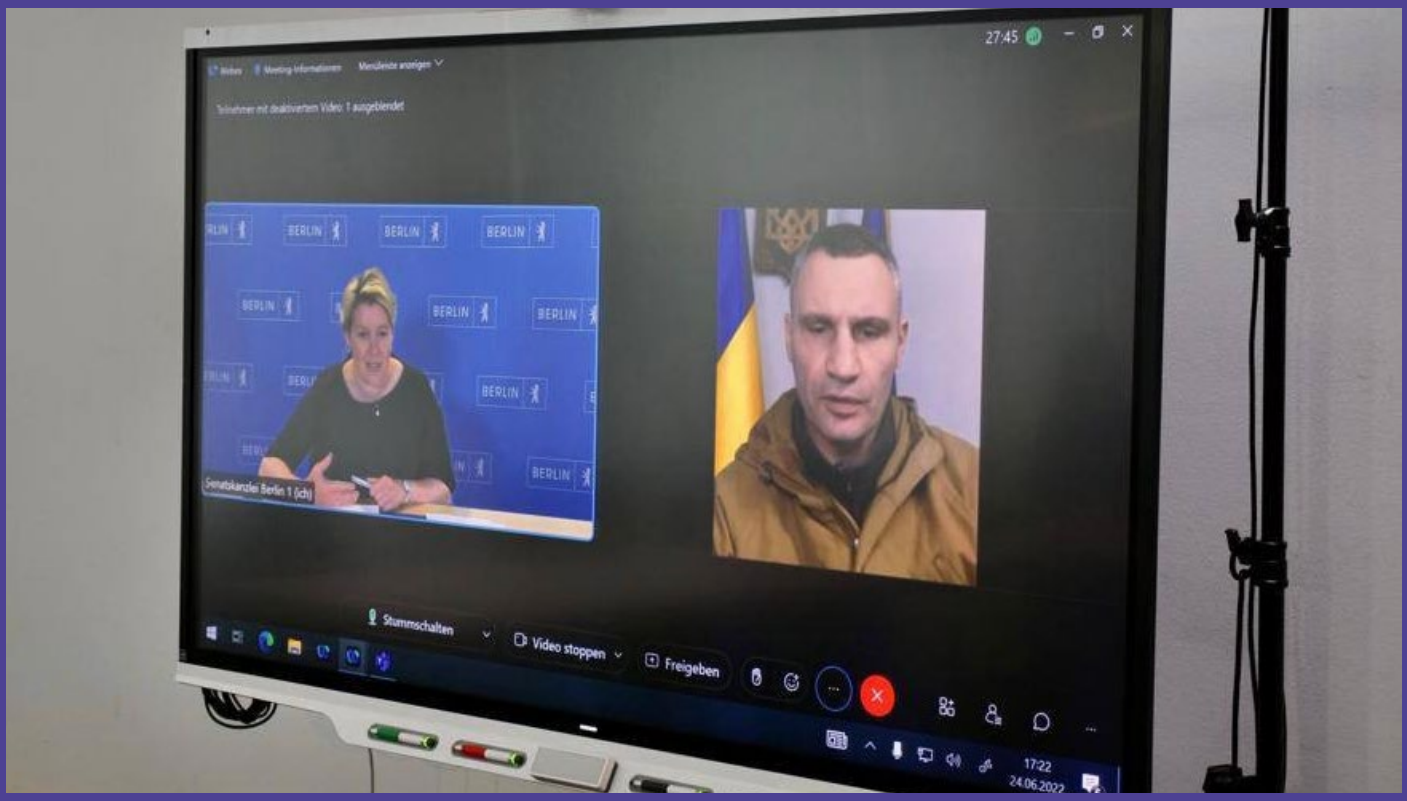


Abb. 2: Manipuliertes Video von Vitali Klitschko[26]

Kapitel 3:

Grenzen der eigenen Handlungsspielräume definieren

Die Strategische Kommunikation (StratKom) – die mittel- bis langfristig geplante Kommunikation im Rahmen der Öffentlichkeitsarbeit gegenüber In- und Ausland – ist eines der Hauptinstrumente von Kommunikationsverantwortlichen. Denn StratKom kann dazu beitragen, den Akteur:innen der Informationsmanipulation nicht die Deutungshoheit über bestimmte Themen, Werte oder Ziele zu überlassen. Trotzdem unterliegen insbesondere staatliche Organisationen in liberalen Demokratien Einschränkungen bei ihren Handlungsspielräumen, die je nach Organisation und Land variieren.

»GEHT ES UM DEN STRATEGISCH-KOMMUNIKATIVEN UMGANG MIT INFORMATIONSMANIPULATION SOLLTEN KOMMUNIKATIONSVERANTWORTLICHE DAHER DIE GRENZEN DES EIGENEN MANDATS KLAR DEFINIEREN.«

In Deutschland verbietet wie in vielen liberalen Demokratien das Gebot der Staatsferne einen staatlich gesteuerten Rundfunk. Die Öffentlichkeitsarbeit der Regierung findet außerdem dort ihre Grenzen, wo Wahlwerbung beginnt.[27] Gemeinhin sollte die Öffentlichkeitsarbeit dabei einen »sachlich informativen, auf die Organtätigkeit der Regierung bezogenen Inhalt« haben.[28] In Großbritannien existiert hingegen ein relativ breites Mandat. So soll die Öffentlichkeitsarbeit hier explizit auch auf Änderungen des Verhaltens der Bevölkerung hinwirken.[29] Zwar sind laut einer repräsentativen Umfrage unter EU-Bürger:innen im März 2023 85 Prozent der Befragten der Meinung, dass die Politik mehr gegen Desinformation unternehmen sollte.[30] Dies darf aber nicht dazu führen, dass die Mandatsgrenzen unangemessen überschritten werden. In der Regel fällt die Beobachtung manipulativer Aktivitäten von politischen Parteien im Inland in den Bereich des Verfassungsschutzes, sofern die rechtlichen Voraussetzungen erfüllt sind.[31] Geht es um den strategisch-kommunikativen Umgang mit Informationsmanipulation sollten Kommunikationsverantwortliche daher die Grenzen des eigenen Mandats klar definieren und klären, inwiefern StratKom bei der Bekämpfung von Informationsmanipulation eingesetzt werden darf.

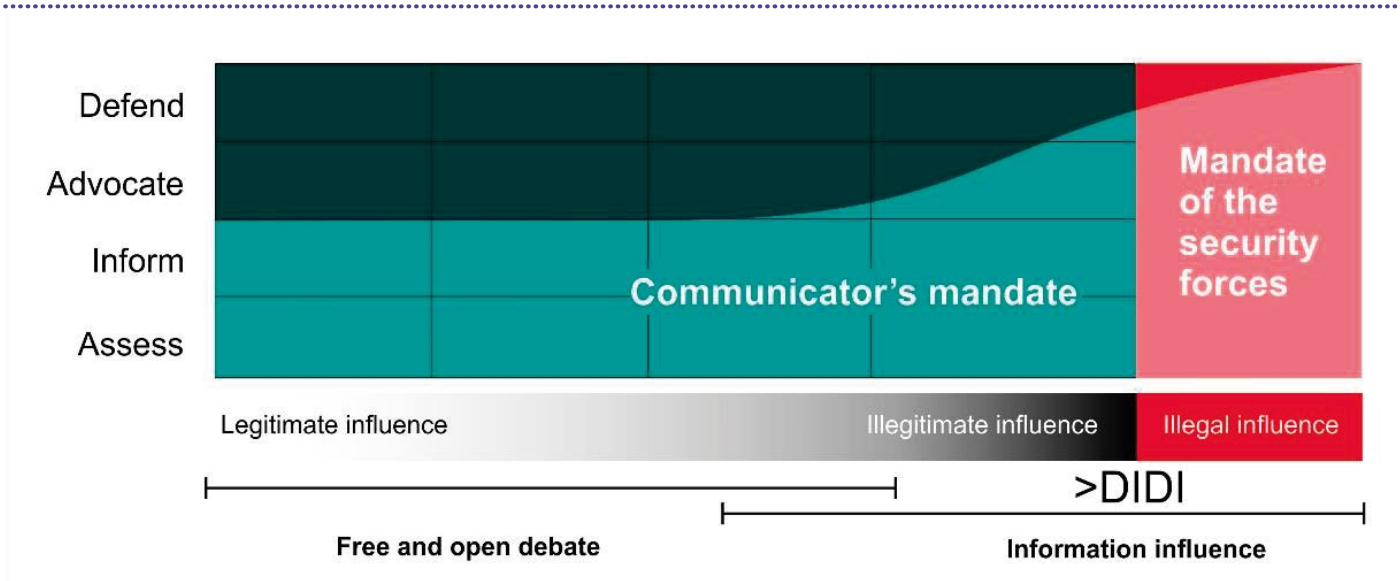


Abb. 3: Modell zur Bestimmung des eigenen Mandats[32]

Im Auftrag der schwedischen Behörde für Zivilschutz und Bereitschaft haben Forscher:innen um den britischen Experten James Pamment ein Modell zur Bestimmung des Mandats staatlicher Organisationen im Umgang mit Vorfällen der Einflussnahme ausländischer Akteur:innen und ihrer Stellvertreter:innen im Inland entwickelt (siehe Abb. 3). Demnach fallen rechtswidrige Vorfälle in den Verantwortungsbereich der Sicherheitsbehörden, die über weitreichende Abwehrmöglichkeiten wie zum Beispiel die Cyber- und Spionageabwehr verfügen. Für die Bestimmung potenzieller Rechtswidrigkeit kann dabei das sogenannte DIDI-Modell[33] herangezogen werden. Dieses sieht eine Evaluierung über die Kategorien »Täuschung« (Deception), »Absicht« (Intention), »Störung« (Disruption) und »Einflussnahme« (Interference) hinweg vor, wobei in jeder Kategorie die Frage nach potenzieller Rechtswidrigkeit zu stellen ist. Handelt es sich um ein rechtmäßiges Verhaltensmuster, so sollte dieses laut Modell wiederum ins Mandat der Kommunikationsverantwortlichen fallen.

»DABEI SETZT DER UMGANG MIT INFORMATIONSMANIPULATION VORAUS, DASS ABGEORDNETENBÜROS NICHT SELBST MANIPULATIVE AKTIVITÄTEN WIE ZUM BEISPIEL DES- ODER MALINFORMATION EINSETZEN.«

Im Gegensatz zu Kommunikationsverantwortlichen aus Ministerien und Behörden besitzen Kommunikationsverantwortliche aus Abgeordnetenbüros gemeinhin wesentlich größere Freiheiten beim strategisch-kommunikativen Umgang mit Informationsmanipulation – einschließlich solcher, die ihren Ursprung bei politischen Parteien im Inland hat. Dabei setzt der Umgang mit Informationsmanipulation voraus, dass Abgeordnetenbüros nicht selbst manipulative Aktivitäten wie zum Beispiel Des- oder Malinformation einsetzen. Darum sollte der Begriff »Informationsmanipulation« unter keinen Umständen als politischer Kampfbegriff eingesetzt werden. Im digitalen Zeitalter ist eine faire politische Auseinandersetzung nicht immer leicht, da der Wettbewerb um Aufmerksamkeit immer stärker wird. Um sich daher an eine faire politische Auseinandersetzung – insbesondere im Wahlkampf – zu halten, sollten eigene Regeln freiwillig eingehalten werden. Wie solche Regeln aussehen können, veranschaulicht der Leitfaden Digitale Demokratie[34], der vor der Bundestagswahl 2021 von einem zivilgesellschaftlichen Bündnis veröffentlicht wurde. Dieser fordert eine »Firewall für die Demokratie«, indem politische Parteien u. a. eigene Werbeanzeigen und Seiten klar kennzeichnen; das Targeting der Werbeanzeigen auf Ort und Zeit beschränken; auf den Bot-Einsatz verzichten; keine Desinformation betreiben; eigene Beiträge auf inhaltliche Richtigkeit überprüfen; und intervenieren, wenn Menschen auf den eigenen Seiten, Profilen oder unter eigenen Beiträgen zur Zielscheibe werden.

Basierend auf dem eigenen Mandat und den Grenzen der Handlungsspielräume sollten Kommunikationsverantwortliche ihre StratKom-Kapazitäten im Hinblick auf Informationsmanipulation weiterentwickeln. An erster Stelle steht dabei die Frage, wie Informationsmanipulation überhaupt erkannt werden kann. Im nächsten Kapitel wird in die systematische Erkennung eingeführt.

Exkurs: Welche regulativen Maßnahmen gegen Informationsmanipulation gibt es?

Nach einem juristischen Gutachten der Landesanstalt für Medien NRW ist eine Regulierung von Desinformation zwar grundsätzlich möglich, unmittelbare Eingriffe in die kommunikative Chancengleichheit dürfen jedoch nur auf wenige und extreme Erscheinungsformen begrenzt sein.[35] Entsprechend setzt auch der europäische Digital Services Act (DSA) auf mittelbare Sorgfaltspflichten für die Anbieter von sehr großen Online-Plattformen und Suchmaschinen wie zum Beispiel die Durchführung unabhängiger Audits, die Einrichtung des Datenzugangs für Forscher:innen oder koregulative Mechanismen zur Übernahme von Verhaltenskodizes wie dem Code of Practice on Disinformation. Damit obliegt es vor allem den Anbietern selbst, zu bestimmen, wie mit manipulativen Aktivitäten und Inhalten verfahren wird. Die Politik kann aber die Einhaltung der Verpflichtungen überprüfen. Abseits des DSA ging die EU im Zuge der russischen Invasion auch unmittelbar gegen Informationsmanipulation vor, indem etwa bestimmte russische Staatsmedien wie RT und Sputnik verboten wurden.[36]

Kapitel 4:
Informationsmanipulation systematisch erkennen

Für die Erkennung von Informationsmanipulation ist die Einrichtung einer Monitoring-Umgebung und die Verifizierung von Inhalten und Konten grundlegend. Diese können dazu beitragen, manipulative Aktivitäten frühzeitig zu identifizieren und den Grundstein für zielgenaue StratKom-Maßnahmen zu legen. Selbstverständlich gibt es Unterschiede unter Abgeordnetenbüros, Ministerien und Behörden hinsichtlich der bereits genutzten Monitoring-Umgebungen und verfügbaren Ressourcen. Außerdem sind manche Organisationen bereits wesentlich stärker für Informationsmanipulation sensibilisiert als andere. Dieser Leitfaden bietet daher eine niedrigschwellige Einführung und richtet sich vor allem an diejenigen, die sich bislang noch nicht mit Informationsmanipulation auseinandergesetzt haben. In diesem Kapitel werden einige generelle Aspekte der Funktionsweise von Informationsmanipulation erklärt, bevor schrittweise die Einrichtung einer Monitoring-Umgebung erläutert werden soll.

Funktionsweise von Informationsmanipulation

Um potenzielle Informationsmanipulation im Rahmen des Monitorings zu erkennen, ist es wichtig, sich zunächst über einige generelle Aspekte der Funktionsweise von Informationsmanipulation und des digitalen Informationsraums bewusst zu werden. Das digitale Zeitalter ist gekennzeichnet durch unterschiedlichste digitale Dienste und fortlaufend neue Trends im Nutzungsverhalten. Gleichzeitig fließen Informationen fortwährend über die nationalen Grenzen vieler Staaten. Entsprechend komplex ist die Funktionsweise des digitalen Informationsraums und entsprechend vielseitig sind auch die manipulativen Aktivitäten die Akteur:innen der Informationsmanipulation einsetzen können.

»DIE AKTEUR:INNEN DER INFORMATIONSMANIPULATION IDENTIFIZIEREN DIE SCHWACHSTELLEN DIGITALER DIENSTE PROAKTIV UND SUCHEN NACH MÖGLICHKEITEN ZUR INAUTHENTISCHEN NUTZUNG, UM ZUM BEISPIEL DEN DIGITALEN INFORMATIONSRAUM MIT PROBLEMATISCHEN INHALTEN ZU FLUTEN.«

Ein wichtiges Element bei der Verbreitung von Inhalten im digitalen Informationsraum sind die Empfehlungssysteme der Online-Plattformen, die auf Algorithmen beruhen. Diese zielen gemeinhin darauf ab, die Interaktion der Nutzer:innen zu maximieren, um die daraus generierten Daten für die Verbesserung der Werbeanzeigen zu verwenden. Dabei geht es darum, solche Inhalte in den News-Feeds der Nutzer:innen auszuspielen, die eine hohe Interaktionsrate versprechen. Wie die Enthüllungen der Facebook-Whistleblowerin Frances Haugen gezeigt haben, kann dies problematische Auswirkungen für die gesellschaftliche Debatte haben. So führte eine Änderung des News-Feed-Algorithmus von Facebook Anfang 2018 zugunsten von Interaktionskriterien wie zum Beispiel Kommentaren und Reshares dazu, dass einige klassische Medien und politische Parteien ihre Inhalte sensationalistischer oder negativer gestalteten.[37] Die Ursache hierfür lag vor allem darin, dass gerade solche Inhalte grundsätzlich mehr Interaktion generieren und folglich von den Algorithmen ausgewählt wurden. Dies zeigt laut Marc Zuckerberg, dem CEO von Meta, auch die Forschung von Facebook. So beschäftigen sich Menschen durchschnittlich mehr mit einem Inhalt, wenn er sich der Grenze des Erlaubten nähert.[38] Das Beispiel verdeutlicht, inwiefern digitale Dienste direkte Auswirkungen auf klassische Medien und Politik haben können. Dabei existieren solche Risiken in vielen unterschiedlichen Märkten und Kontexten.

Abb. 4: Sceenshot des Mercola-Artikels

Die Akteur:innen der Informationsmanipulation identifizieren die Schwachstellen digitaler Dienste proaktiv und suchen nach Möglichkeiten zur inauthentischen Nutzung, um zum Beispiel den digitalen Informationsraum mit problematischen Inhalten zu fluten. Der Möglichkeitsspielraum eingesetzter Taktiken und Techniken ist dabei immens. Zudem schaffen neue Plattformen und Technologien wie zum Beispiel Generative KI fortlaufend neue Möglichkeiten der Informationsmanipulation. Um manipulative Aktivitäten in ihrer Vielschichtigkeit zu identifizieren, hat die Organisation Alliance4Europe DISARM entwickelt.[39] Der DISARM Framework Explorer bietet dabei einen umfassenden Überblick über »Taktiken« (Tactics), »Techniken« (Techniques) und »Verfahrensweisen« (Procedures) (TTPs).[40] Eine häufig beobachtete Technik ist die Nutzung alternativer Nachrichtenseiten. Dabei kommt es zunehmend zur Überlappung der Aktivitäten unterschiedlicher Akteur:innen – eine Hybridisierung des Ökosystems der Informationsmanipulation.

Im November 2020 wurde zum Beispiel der Artikel »Riesen Skandal aufgedeckt: Covid-19-Impfung zerstört unser Immunsystem nachhaltig« des US-amerikanischen Arztes Joseph Mercola auf der Internetseite »Anonymousnews« veröffentlicht (siehe Abb. 4). Während Mercola selbst als dubioser Geschäftsmann und Vordenker der impfskeptischen Bewegung gilt, existieren starke Indizien für eine enge Verbindung von Anonymousnews ins rechtsextremistische Milieu und zu pro-russischer Informationsmanipulation.[41] Ausgehend von Anonymousnews verbreitete sich der Text in kürzester Zeit auf Internetseiten wie zum Beispiel »Unsere Natur« und »2020 News«, sowie auf Facebook, Twitter, Telegram und in E-Mails. Dieser **Bottom-up-Prozess** (siehe Abb. 5) ist ein wiederkehrendes Muster der Informationsmanipulation. Im Allgemeinen kann dabei zwischen drei Verbreitungsstufen mit unterschiedlich starken Reichweiten unterschieden werden.

Nische	Die Inhalte erhalten wenig Interaktion oder zirkulieren innerhalb von Nischenöffentlichkeiten, in der die Nutzer:innen eine relativ ähnliche Weltanschauung teilen. Dies können z. B. einzelne Seiten oder Gruppen auf Online-Plattformen oder Kanäle auf Messenger-Diensten sein. Häufig werden dabei Inhalte von alternativen Nachrichtenseiten oder Blogs aufgegriffen.
Trend	Nutzer:innen innerhalb von Nischenöffentlichkeiten sind potenzielle Brücken zur Außenwelt. Sobald einige Beiträge mit Interaktionen oder auch Beiträge mit Gegenargumenten außerhalb der Nischenöffentlichkeit stattfinden, so liegt ein Trend vor. Dazu gehören auch Hashtags und Themen die von den Online-Plattformen als Trend ausgewiesen werden.
Mainstream	Die Inhalte erhalten erste Berichterstattung in den klassischen Medien mit den größten Leserzahlen bzw. Einschaltquoten oder es ist eine Headline-Story zu erwarten. Dabei ist auch die Wahrscheinlichkeit groß, dass die Berichterstattung wiederum weiterführende Online-Diskussionen nach sich zieht, wodurch die Viralität von Inhalten weiter zunimmt.

Abb. 5: Bottom-up-Prozess

Doch nicht immer werden Inhalte wie im Fall des Mercola-Artikels in einem Bottom-up-Prozess verbreitet. Es existieren ausgewiesene Fälle, in denen Akteur:innen der Informationsmanipulation in klassischen Medien zu Wort kommen und sich ihre Inhalte von dort aus im digitalen Informationsraum verbreiten. Bei diesem **Top-Down-Prozess** funktionieren die Auftritte als Referenzpunkte für nachgelagerte Online-Diskussionen. Aufgrund dieser Dynamik ist es besonders wichtig, dass Politiker:innen die Regeln fairer politischer Auseinandersetzung einhalten. Kommunikationsverantwortliche aus Abgeordnetenbüros, Ministerien und Behörden sollten sich über beide Verbreitungswege genauso bewusst sein, wie über die Vielfalt möglicher TTPs. Es ist daher ratsam, dass sie sich mit dem DISARM Framework Explorer vertraut machen. Dieser umfasst neben TTPs auch mögliche Gegenmaßnahmen, einschließlich StratKom-Maßnahmen. Damit ergriffene Maßnahmen auch zielgerichtet sein können, müssen manipulative Aktivitäten frühzeitig erkannt und bewertet werden. Im Folgenden wird daher auf die Einrichtung einer niedrigschwelligen Monitoring-Umgebung eingegangen.

Einrichtung einer Monitoring-Umgebung

Die Möglichkeiten für Kommunikationsverantwortliche, Informationsmanipulation aufzudecken, sind begrenzt. So ist die Aufdeckung manipulativer Aktivitäten wie zum Beispiel gezielt verbreiteter Fehlinformationen oder Deepfakes eine anspruchsvolle und zeitaufwändige Aufgabe, die meistens von Expert:innen der Open Source Intelligence (OSINT) übernommen wird. Diese versuchen auf Grundlage frei verfügbarer Informationen Beweise für Informationsmanipulation zu sammeln.

»DIE EINRICHTUNG EINER MONITORING-UMGEBUNG, DIE SICH AUF DIE POTENZIELLEN AUSWIRKUNGEN VON INFORMATIONSMANIPULATION AUF DIE EIGENE POLITISCHE ARBEIT FOKUSSIERT, IST HIERFÜR ZENTRAL.«

Dennoch gibt es auch niedrigschwellige OSINT-Tools, die sich für die Nutzung durch Kommunikationsverantwortliche eignen. Damit solche Tools jedoch überhaupt zum Einsatz kommen können, sollten an erster Stelle potenzielle manipulative Aktivitäten identifiziert werden. Die Einrichtung einer Monitoring-Umgebung, die sich auf

die potenziellen Auswirkungen von Informationsmanipulation auf die eigene politische Arbeit fokussiert, ist hierfür zentral. Grundlage einer jeden Monitoring-Umgebung sollte dabei wiederum eine **Keyword-Liste** mit Begriffen, Ausrücken, Hashtags und Konten sein, nach denen anschließend gesucht wird. Die Keywords sollten die Prioritäten der politischen Arbeit und Risikobereiche beschreiben. Gemeinhin kann zwischen Debattenklima (z. B. zu relevanten Gesetzen), Stakeholder:innen (z. B. Interessens- und Wählergruppen) und der eigenen Reputation unterschieden werden. Dabei ist es auch möglich, dass unterschiedliche Bereiche gleichzeitig durch einen bestimmten Vorfall betroffen sind. Bei der Identifizierung der Keywords kann es helfen, die Prioritäten und Risikobereiche anhand der Fragen des Prioritätenschemas (siehe Abb. 6) zu definieren.

	Prioritäten	Risikobereiche
Debattenklima	Was sind unsere relevantesten Themengebiete und Narrative?	• Was sind die vorherrschenden Einstellungen unserer Zielgruppen zu den Themengebieten und Narrativen, die ausgenutzt werden könnten? • Sind die Themengebiete und Narrative bereits manipulativen Verhaltensweisen und Narrativen ausgesetzt? Und falls ja, welche sind problematisch?
Stakeholder	Wer sind unsere relevantesten Zielgruppen?	• Was sind die Interessen und Werte unserer Zielgruppen, mit wem interagieren sie und wem hören sie zu? • Welche Aspekte der Beziehung zu ihnen sind anfällig für manipulativen Verhaltensweisen und Narrativen?
Reputation	Was sind die Grundwerte, für die wir stehen und die wir darstellen möchten?	• Was sind die vorherrschenden Einstellungen unserer Zielgruppen und der allgemeinen Öffentlichkeit zu uns, die ausgenutzt werden könnten? • Welche manipulativen Verhaltensmuster und Narrative könnten unser Ansehen und Ruf negativ beeinflussen?

Abb. 6: Prioritätenschema[42]

Basierend auf der Keyword-Liste sollten anschließend unterschiedliche Datenquellen durchsucht werden. Ein solches Monitoring kann – in Abhängigkeit von den zur Verfügung stehenden Kapazitäten – regelmäßig (pro Monat/Woche/Tag) oder in besonders relevanten Zeiträumen (z. B. Wahlkampf, Krisensituationen) durchgeführt werden. Während Ministerien und Behörden gemeinhin über größere Kapazitäten und bereits vorhandene Datenquellen verfügen, sind die Kapazitäten und Ressourcen von Abgeordnetenbüros – insbesondere auf kommunaler Ebene – in der Regel stark limitiert. Je nach verfügbaren Kapazitäten muss daher auch nicht bei jedem Monitoring nach allen Keywords gesucht werden. Dennoch sollte das regelmäßige Monitoring dazu genutzt werden, die Keyword-Liste kontinuierlich zu überarbeiten, um noch präzisere Keywords und Kombinationen zu identifizieren. Die Datenquellen selbst lassen sich vereinfacht in direkte Datenquellen (siehe Abb. 7) und indirekte Datenquellen (Abb. 8) untergliedern. Während erstere ein unmittelbares Monitoring des digitalen Informationsraums erlauben, stützen sich letztere auf bereits durchgeführte Analysen anderer Organisationen.

Direkte Datenquelle	Beschreibung
Social-Listening-Dienste	Dienste wie Brandwatch, Meltwater oder Talkwater sind kostenpflichtig, verfügen aber über Schnittstellen zu den relevanten Online-Plattformen und ermöglichen so eine systematische und plattformübergreifende Suche mit umfassenden Suchkriterien.
Google Alerts	Google Alerts ist kostenlos und ermöglicht die Anlage von Suchaufträgen für Keywords und Kombinationen. Damit können Internetseiten, einschließlich Online-Plattformen, durchsucht werden. Über die Optionen kann u. a. eingestellt werden, in welcher Frequenz die Suchergebnisse via E-Mail zugeschickt werden sollen (täglich/wöchentlich/monatlich). Boolesche Operatoren ermöglichen verfeinerte Suchaufträge: ● **ODER** Suche nach X oder Y. Die Ergebnisse beziehen sich auf X oder Y oder beides. (z. B. Skandal OR Mercola) ● **Leerzeichen [_]** Suche nach X und Y, bei der die Schnittmenge gebildet wird. (z. B. Skandal Mercola) ● **Minuszeichen [-]** Suche nach X, nicht nach Y. So kann ein Keyword oder Keyword-Kombination ausgeschlossen werden. (z. B. Skandal -Mercola) ● **Anführungszeichen »...«** Sucht exakte Keyword-Reihenfolge (z. B. »Riesen Skandal aufgedeckt: Covid-19-Impfung zerstört unser Immunsystem nachhaltig«) ● **Sternchen (*)** Fungiert als Platzhalter für Buchstabenfolgen. (z. B. Covid*) ● **Klammern [(...)]** Gruppiert Keywords oder Operatoren für Suchaufträge (z. B. (»Riesen Skandal« OR Mercola) Covid*) ● **site:** Sucht alle indexierten Seiten einer Domain (z. B. site:facebook.com/pages Mercola Skandal) ● **related:** Sucht nach Internetseiten, die sich auf die angegebene Seite beziehen und umgekehrt (z. B. related:anonymousnews.org) ● **link:** Sucht Internetseiten, die auf die Seite verlinken (z. B. link: anonymous-news.org/gesundheit/covidimpfung-zerstoert-immunsystem)
Google Trends	Google Trends ist ein kostenloses Angebot von Google, das es ermöglicht, in Echtzeit zu untersuchen, wie häufig Keywords bei Google Suche, Google News und YouTube eingegeben werden. Über die »Aktuelle Trends«-Funktion wird außerdem eine Übersicht über die am häufigsten gesuchten Themen der letzten Tage bereitgestellt.
Plattformsuchen	Plattformeigene Dienste wie z. B. TweetDeck und CrowdTangle ermöglichen umfassende Plattformsuchen. Allerdings sind diese häufig kostenpflichtig oder sind nur für bestimmte Organisationen zugänglich. Alterativ bieten die Suchfunktionen selbst bereits einige Möglichkeiten zur strukturierten Suche durch Filteroptionen.
News-Aggregatoren	Mit RSS-Diensten wie z. B. Feedly kann eine Vielzahl an Internetseiten, Blogs oder Newsletter in einem gebündelten Feed beobachtet werden, sofern RSS verfügbar ist.

Abb. 7: Übersicht direkter Datenquellen

	Indirekte Datenquelle	Beschreibung	URL
Faktencheck-Seiten	Fact Check Explorer	Google-Dienst, um nach Faktenchecks zu bestimmten Themen oder Personen zu suchen; über »list:recent« werden die aktuellsten Faktenchecks angezeigt.	https://toolbox.google.com/factcheck/explorer
	CORRECTIV.Faktencheck	Faktenchecks zu aktuellen, reichweiten-starken und schädlichen potenziellen Fehlinformationen; Schwerpunktthemen: Aktuelle Krisen; Klima; Europa; Gesellschaft; Medizin & Gesundheit; Justiz, Migration, Militär, Polizei, Wirtschaft & Umwelt.	https://correctiv.org/faktencheck/
	ARD-Faktenfinder	Faktenchecks zu tagesaktuellen Themen sowie Hintergrundberichte zu Trends und Akteur:innen.	https://www.tagesschau.de/faktenfinder
	#Faktenfuchs	Faktenchecks, die für BR-Nutzer:innen sowie Social-Media-Redakteur:innen relevant erscheinen; Schwerpunktthemen: Politik; Umwelt; Wirtschaft; Gesellschaft; Landwirtschaft; Medizin.	https://www.br.de/nachrichten/faktenfuchs-faktencheck,QzSIzI3
	MIMIKAMA	Faktenchecks zu tagesaktuellen Themen, die von von Internetnutzer:innen zur Prüfung eingereicht werden.	https://www.mimikama.org/category/mimikama-faktenchecks/faktencheck/
	AFP Faktencheck	Faktenchecks zu viralen Fehlinformationen mit Auswirkungen auf die Öffentlichkeit, Gesundheit, demokratischen Prozesse und Personengruppen; Schwerpunktthemen: Gesundheit; Politik (Regionen: Deutschland; Österreich; Schweiz; Europa; Nordamerika)	https://faktencheck.afp.com/list
	dpa Faktencheck	Faktenchecks zu Fehlinformationen mit gesellschaftlichen Auswirkungen; Schwerpunktthemen: Politische Themen, Wirtschaft, Wissenschaft, Panorama.	https://www.dpa.com/de/dpa-factchecking
	Volksverpetzer	Teilweise satirische und weniger neutrale Hintergrundberichte zu Narrativen von Extremist:innen und Verschwörungserzählungen.	https://www.volksverpetzer.de/
Datenbanken	DeSmog Climate Disinformation Database	Datenbank zu Akteur:innen, die Desinformation über den Klimawandel verbreiten.	https://www.desmog.com/climate-disinformation-database/
	DisinfoWatch Database	Datenbank zu Fehlinformationen, Desinformation, Verschwörungserzählungen und Informationsmanipulation mit einem Schwerpunkt auf COVID-19.	https://disinfowatch.org/database/
	EUvsDisinfo Database	Datenbank zu weltweiten Vorfällen von Desinformation, die ihren Ursprung in pro-Kreml-Medien haben.	https://euvsdisinfo.eu/disinformation-cases/
	Database of Known Fakes	Datenbank, die Faktenchecks kategorisch auflistet und die Möglichkeit bietet, bestimmte Inhalte auf vorliegende Faktenchecks zu prüfen.	https://weverify-de-mo.ontotext.com/#!/searchViewResults
	Fakten gegen Fake News	Übersicht zu bekannten Fehlinformationen, die im Wahlkontext verbreitet werden.	https://www.bundeswahlleiterin.de/bundestagswahlen/2021/fakten-fakenews.html
	Hamilton 2.0 Dashboard	Datenbank, die Beiträge chinesischer, iranischer und russischer Kanäle auf Online-Plattformen und Internetseiten dokumentiert.	https://securingdemocracy.gmfus.org/hamilton-dashboard/
	Veridica Database	Datenbank, die Fehlinformationen und Desinformation aus Zentral- und Osteuropa sammelt.	https://www.veridica.ro/en/database

	Indirekte Datenquelle	Beschreibung	URL
Forschungsberichte	**Amadeu-Antonio-Stiftung**	Berichte, Handreichungen und Infoblätter zu Rechtsextremismus, Rassismus und Antisemitismus.	https://www.amadeu-antonio-stiftung.de/publikationen/
	Center für Monitoring, Analyse und Strategie (CeMas)	Berichte zu Rechtsextremismus, Desinformation, Verschwörungserzählungen und Antisemitismus.	https://cemas.io/publikationen/
	Climate Action against Disinformation (CAAD)	Berichte und Infoblätter zu Desinformation über den Klimawandel und Monetarisierung.	https://caad.info/analysis/
	EU DisinfoLab	Berichte und Infoblätter zu Desinformation in Europa.	https://www.disinfo.eu/publications/
	Hans-Bredow-Institut	Berichte zum Medienwandel und den damit verbundenen strukturellen Veränderungen öffentlicher Kommunikation.	https://www.hans-bredow-institut.de/de/publikationen
	HateAid	Analysen zu den Phänomenen digitaler Gewalt.	https://hateaid.org/category/phaenomene-digitaler-gewalt/
	Institute for Strategic Dialogue (ISD)	Berichte und aktuelle Kurzanalysen zu Extremismus, Desinformation, Polarisierung und Hass, sowie zur Digitalpolitik und Regulierung.	https://isdgermany.org/publikationen/

Abb. 8: Übersicht indirekter Datenquellen

Beinhalten die Monitoring-Suchergebnisse einen Vorfall potenzieller Informationsmanipulation geht es im nächsten Schritt darum, die Suchergebnisse strukturiert zu dokumentieren. Eine solche **Ergebnisdokumentation** ist wiederum die Grundlage für eine umfassende Bewertung und StratKom-Maßnahmen. Für die Dokumentation selbst eignet sich zum Beispiel das **ABCDE-Framework**. Dieses ist eine weiterentwickelte Version des ABC-Frameworks von Camille François und zerlegt das Phänomen »Desinformation« in kleinere operative Kategorien: »Akteur« (Actor); »Verhalten« (Behaviour); »Inhalt« (Content); »Ausmaß« (Degree); und »Wirkung« (Effect), die auch als Fragen operationalisiert werden können (siehe Abb. 9). Beim Ausmaß geht es vor allem um die Verbreitung von Inhalten. Bei der Wirkung sollen wiederum die Auswirkungen erfasst werden. Beide Kategorien sind zentral für die Bewertung eines Vorfalls. Das ABCDE-Framework lässt sich ohne Schwierigkeiten aufs Phänomen der Informationsmanipulation anwenden.

Akteur:in	Welche Akteurstypen sind involviert? Diese Frage kann helfen festzustellen, ob der Vorfall ausländische staatliche Akteur:innen involviert.
Verhalten	Welche Aktivitäten sind zu erkennen? Diese Frage kann dazu beitragen, Beweise für Koordination und Inauthentizität zu finden.
Inhalt	Welche Arten von Inhalten werden erstellt und verbreitet? Diese Frage kann helfen festzustellen, ob die verbreiteten Informationen manipulativ sind.
Ausmaß	Welche Auswirkung hat der Vorfall insgesamt und wen betrifft er? Diese Frage kann dazu beitragen, den tatsächlichen Schaden und die Schwere des Vorfalls zu ermitteln.
Wirkung	Welche Auswirkung hat der Vorfall insgesamt und wen betrifft er? Diese Frage kann dazu beitragen, den tatsächlichen Schaden und die Schwere des Vorfalls zu ermitteln.

Abb. 9: ABCDE-Framework[43]

Weiterführende Materialien:

- DRI: Guide to Monitoring Image and Video-based Social Media.
- FirstDraft: Nachrichtenbeschaffung und Monitoring sozialer Netzwerke.
- WHO: How to build an infodemic insights report.

Verifizierung von Inhalten und Konten

Wie bereits dargelegt, können Vorfälle der Informationsmanipulation sehr verdeckt und manipulativ ablaufen. Indirekte Datenquellen wie zum Beispiel Faktenchecks oder Forschungsberichte liefern zwar häufig bereits Hinweise darauf, wer hinter bestimmten manipulativen Aktivitäten stecken könnte. Dennoch werden diese meistens erst veröffentlicht, wenn bereits ein starker Trend bestimmter Inhalte vorliegt. Daher sollten sich Kommunikationsverantwortliche mit niedrigschwelligen OSINT-Tools vertraut machen, um eigene Erkenntnisse zur Inauthentizität eines Inhalts oder eines Kontos zu generieren. In der Anleitung zu Verifizierungstools (siehe Abb. 10) werden zwei Tools vorgestellt. Bei der Anwendung sollte berücksichtigt werden, dass solche Tools selbst Limitationen aufweisen und lediglich einen von mehreren Faktoren bei der Verifizierung von Inhalten und Konten darstellen. Unsere Anleitung spiegelt nur einen kleinen Teil der verfügbaren Tools wider, die kontinuierlich weiterentwickelt und ergänzt werden. Dabei gilt es zu beachten, dass viele Tools auf frei zugänglichen Programmierschnittstellen der Anbieter basieren, weswegen eine Verfügbarkeit nicht immer garantiert ist.

Anwendung

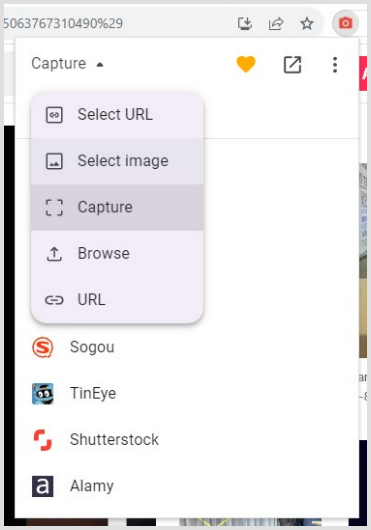
Verifizierungstool	Beschreibung	URL
Search by image (u. a. für Chrome, Firefox, Safari)	Browser-Erweiterung, die es ermöglicht, nachzuforschen, ob ein Bild oder Video bereits zuvor verwendet wurde.	https://chromewebstore.google.com/detail/search-by-image/cnojnbdhbhnkbcieeekonklommdnndci

Schritt 1: Fügen Sie die Browser-Erweiterung hinzu.

Tipp: Sollte »Search by Image« für Sie nicht in Frage kommen, nutzen Sie z. B. TinEye, ReVEye, InVID oder die Google Reverse Image Search.

Schritt 2: Öffnen Sie den visuellen Inhalt, der untersucht werden soll. Klicken Sie anschließend auf das Plugin-Symbol in der Navigationsleiste und wählen Sie »Capture« sowie eine Suchmaschine aus.

Tipp: Bei Videoinhalten sollte ein Standbild ausgewählt werden, das nicht zu unscharf oder verwackelt ist.



Schritt 3: Wählen Sie anschließend das Bild oder den Bildausschnitt aus und klicken Sie auf »Search«. In den Suchergebnisse finden Sie unter Umständen eine Version, die bereits zu einem früheren Zeitpunkt veröffentlicht wurde, oder Faktenchecks.

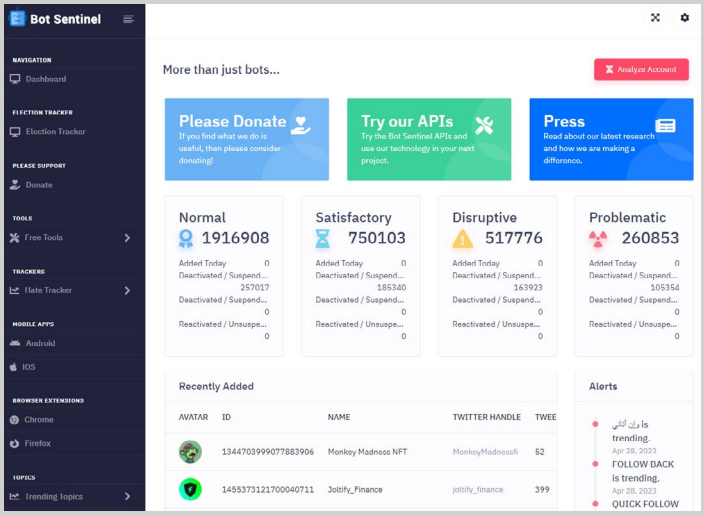
Weiterführende Materialien:

- OSINT Essentials: Where do I begin?
- RAND: Tools That Fight Disinformation Online.
- First Draft: Verifizierung von Online-Informationen.
- LMA NRW: Überprüfung von Desinformation und Medienmanipulation.

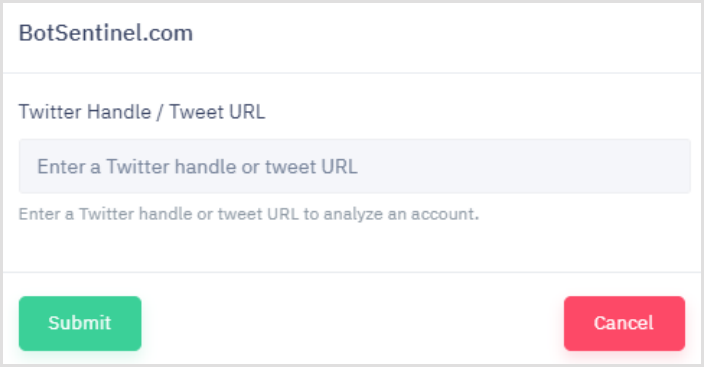
Verifizierungstool	Beschreibung	URL
Bot Sentinel	Web-Anwendung und Browser-Erweiterung, die Konten und Beiträge auf X auf ihre Authentizität hin analysiert und auf einer Skala von »Normal« bis »Problematisch« einstuft.	https://botsentinel.com/

Anwendung

Schritt 1: Öffnen Sie die Web-Anwendung oder fügen Sie die Browser-Erweiterung hinzu.



Schritt 2: Klicken Sie auf das Symbol »Analyze Account« und geben Sie anschließend den Nutzernamen oder die vollständige URL des X-Kontos ein, das untersucht werden soll.



Schritt 3: BotSentinel bewertet das Konto auf einer Skala von 0% bis 100%. Je höher die Zahl, desto wahrscheinlicher ist es, dass das Konto manipulativen Aktivitäten nachgeht. Über »View Profile« können zusätzliche Details des Kontos, einschließlich des Erstellungsdatums des Kontos und häufig geteilter Phrasen, Hashtags und URLs eingesehen werden.

Tipp: Tools wie BotSentinel können einen Faktor bei der Erkennung von Bots darstellen. Sie sollte aber durch nicht-technische Bewertungsverfahren ergänzt werden.

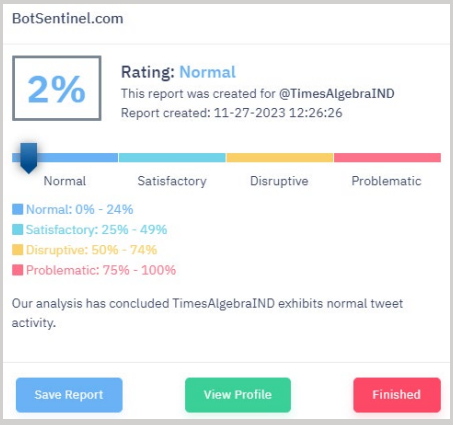


Abb. 10: Anleitung zu Verifizierungstools

Kapitel 5:
Informationsmanipulation zielgenau bekämpfen

Nach der Dokumentation der Suchergebnisse des Monitorings, einschließlich möglicher Verifizierungen von Inhalten und Konten, geht es abschließend darum, die Ergebnisse zu bewerten und gezielte StratKom-Maßnahmen abzuleiten. In diesem Kapitel wird dafür unter Berücksichtigung der bisherigen Ausführungen ein **integriertes Bewertungs- und Handlungsmodell** vorgestellt. Dieses ist idealtypisch und lässt sich daher nicht auf jeden Vorfall von Informationsmanipulation anwenden. Vielmehr dient es als Orientierungspunkt, um eigene Lösungen zum Umgang mit Informationsmanipulation zu erarbeiten. Im Folgenden soll zunächst auf die Bewertung eingegangen werden, bevor anschließend Empfehlungen für zielgerichtete Handlungen vorgestellt werden.

Bewertung von Monitoring-Erkenntnissen

Monitorings werden gemeinhin erst dann wertvoll, wenn sie in konkrete Erkenntnisse übersetzt werden – in Analysen mit interessanten und verwertbaren Daten.[44] Im Kern geht es bei der Bewertung darum, aufkommende Trends frühzeitig zu erkennen, Verbreitungsmechanismen zu verstehen, zu warnen und zielgerichtete Handlungsempfehlungen zu ermöglichen. Für dieses Anliegen sollten die beobachteten Vorfälle potenzieller Informationsmanipulation zunächst im Hinblick auf folgende Fragen abschließend bewertet werden: Wie groß ist die Reichweite? Welche Auswirkungen auf die eigene politische Arbeit gibt es? Liegen stichhaltige Beweise für eine Schadensabsicht vor?

»IM KERN GEHT ES BEI DER BEWERTUNG DARUM, AUFKOMMENDE TRENDS FRÜHZEITIG ZU ERKENNEN, VERBREITUNGSMECHANISMEN ZU VERSTEHEN, ZU WARNEN UND ZIELGERICHTETE HANDLUNGSEMPFEHLUNGEN ZU ERMÖGLICHEN.«

Anhand der **Bewertungsmatrix** (siehe Abb. 11) sollte dabei eine Bewertung jeder Kategorie des Vorfalls auf einer Skala erfolgen (dunkelviolett = hohe Priorität; violett = mittlere Priorität; hellviolett = niedrige Priorität). Die Matrix basiert auf der Annahme, dass die Relevanz eines Vorfalls mit der Reichweite, den Auswirkungen und der Beweislast zunimmt. Dabei wurde außerdem angenommen, dass in der politischen Arbeit die Auswirkungen auf die Reputation am relevantesten sind, während Auswirkungen auf die Stakeholder und das Debattenklima als relativ weniger relevant eingeschätzt werden. Letztlich kann dies aber je nach Kontext und eigenen Prioritäten variieren.

	Reichweite	Auswirkungen	Beweislast
Niedrig	**Nische** Zirkulation innerhalb einer Nischenöffentlichkeit	**Debattenklima** Untergrabung des Debattenklimas	**Indikationen** Einzelne Indikatoren für eine Schadensabsicht
Mittel	**Trend** Einige Beiträge außerhalb der Nischenöffentlichkeit	**Stakeholder** Nachteilig für Wählerschaft oder Interessensgruppen	**Indirekte Beweise** Evidenzen für eine Schadensabsicht
Hoch	**Mainstream** Berichterstattung in den Leitmedien	**Reputation** Nachteilig für Ruf oder Sicherheitsrisiken	**Direkte Beweise** Starke Evidenzen für Schadensabsicht

Abb. 11: Bewertungsmatrix[45]

Sobald die abschließende Bewertung finalisiert ist, sollte damit begonnen werden einen **Trendbericht** anzufertigen. Dieser sollte den jeweiligen Vorfall der Informationsmanipulation (Akteur, Verhalten, Inhalt) kurz zusammenfassen, die abschließende Bewertung beinhalten und Empfehlungen für zielgerichtete StratKom-Maßnahmen umfassen. Im Folgenden wird ein Überblick über allgemeine Handlungsempfehlungen für unterschiedliche Prioritätsstufen gegeben.

StratKom: Empfehlungen für zielgerichtete Handlungen

StratKom zeilt darauf ab, die Deutungshoheit im digitalen Informationsraum nicht den Akteur:innen der Informationsmanipulation zu überlassen. Insbesondere bei Vorfällen mit geringerer Reichweite kann es aber auch sinnvoll sein, gar nicht zu reagieren, um der weiteren Verbreitung eines Inhalts vorzubeugen. In der **Handlungsmatrix** (siehe Abb. 12) wird grundsätzlich zwischen reaktiven und proaktiven Handlungen unterschieden, die jeweils taktisch oder strategisch ausgerichtet sein können. Reaktiv-taktische Handlungen eignen sich insbesondere für Vorfälle hoher Priorität, bei denen zum Beispiel ein Online-Trend beobachtet wird und potenzielle Auswirkungen für die Reputation bestehen. Bei Vorfällen geringer Priorität wie zum Beispiel das Aufkommen vereinzelter manipulativer Aktivitäten in einer Nischenöffentlichkeit, ist es wiederum ratsam, den Vorfall zunächst weiter zu beobachten und vorzusorgen.

»INSBESONDERE BEI VORFÄLLEN MIT GERINGERER REICHWEITE KANN ES ABER AUCH SINNVOLL SEIN, GAR NICHT ZU REAGIEREN, UM DER WEITEREN VERBREITUNG EINES INHALTS VORZUBEUGEN.«

Bei den StratKom-Maßnahmen ist es außerdem entscheidend, die passenden Kanäle, Formate und Absender:innen auszuwählen: Welche Zielgruppen sollen erreicht werden und wo kommunizieren diese? Welche Absender:innen werden bei der Zielgruppe als vertrauenswürdig wahrgenommen? Welche Inhalte (Audio, Bild, Video) sind für die Kommunikation und ihre Ziele am besten geeignet? Grundsätzlich existieren viele unterschiedliche Handlungsmöglichkeiten, die unterschiedlich hilfreich sind. Die in diesem Leitfaden angeführten StratKom-Maßnahmen sind normative Handlungsempfehlungen, die auf Annahmen und Erfahrungswerten im Rahmen der Projektarbeit basieren. Sie stellen jedoch keine wissenschaftlich getesteten Maßnahmen dar.

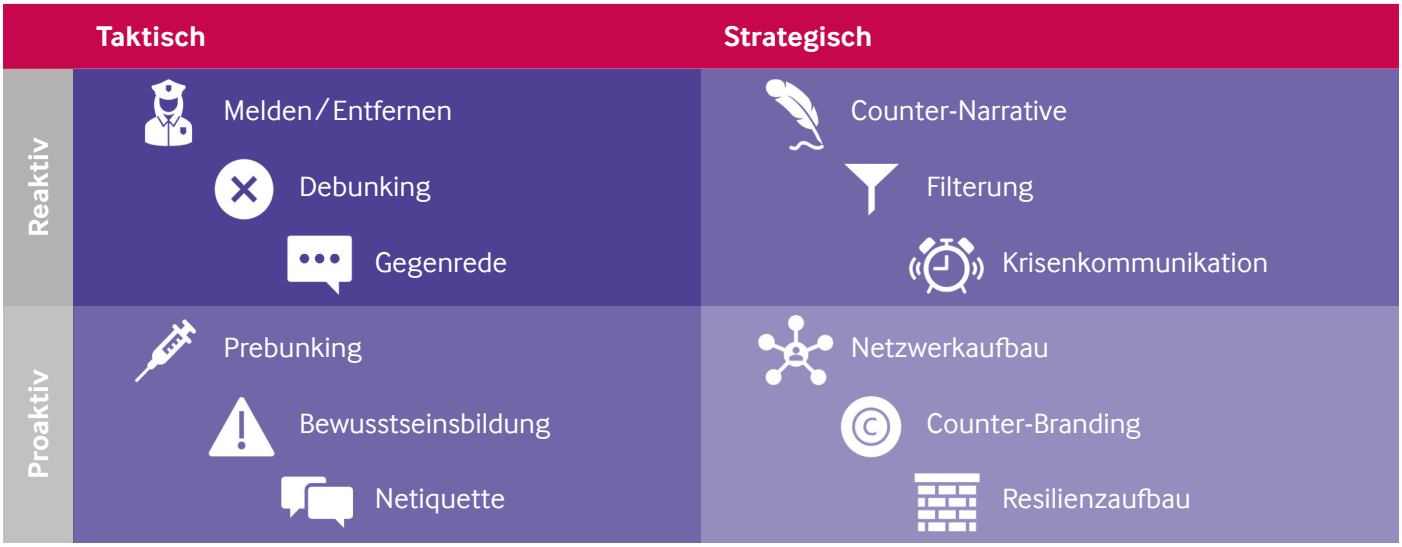


Abb. 12: Handlungsmatrix[46]

Reaktive Maßnahmen

Melden/Entfernen: Ab Februar 2024 müssen alle Hostingdiensteanbieter in der EU sogenannte Melde- und Abhilfeverfahren für rechtswidrige Inhalte einrichten. Dadurch sollten Melde-Funktionen auch auf kleineren Online-Plattformen verfügbar sein und beim Vorgehen nicht unberücksichtigt bleiben. Das Melden von Inhalten kann aber auch auf Grundlage der Gemeinschaftsstandards der Online-Plattformen erfolgen. Es ist ein taktisches Instrument, um direkt auf Vorfälle der Informationsmanipulation zu reagieren. Im Hinblick auf Fehlinformationen sind in der Regel nur bestimmte Arten mit hohem Schadenspotenzial in den Gemeinschaftsstandards als unzulässig aufgelistet (z. B. wahl- oder gesundheitsbezogene Fehlinformationen). Zur rechtswidrigen Desinformation gehört laut StGB insbesondere die »Verleumdung« (§ 187). Beim Melden sollte antizipiert werden, dass die Bearbeitung der Meldung einige Tage oder sogar Wochen in Anspruch nehmen kann. Potenziell rechtswidrige Inhalte können zudem über Meldestellen wie zum Beispiel HessenGegenHetze (unabhängig vom eigenen Standort) an die Strafverfolgung gemeldet werden.

Weiterführende Materialien:

- HateAid: Deine Rechte im Netz. Wie du gegen digitale Gewalt vorgehen kannst.
- Hans-Bredow Institut & HateAid: Wahl-Watching.
- HessenGegenHetze: Was kann ich tun?

Debunking: Beim sogenannten »Debunking« geht es darum, falsche oder irreführende Inhalte durch korrekte Inhalte zu korrigieren. Diese reaktiv-taktische Maßnahme kann dabei helfen, dem Glauben an eine bestimmte Fehlinformation und damit auch einer weiteren Verbreitung des Inhalts gegenzusteuern. Dabei sollte aber beachtet werden, dass die Wiederholung von Fehlinformationen auch zu einer weiteren Verankerung in den Gedächtnissen der Nutzer:innen beitragen kann. Jedes Debunking sollte deshalb die Fakten in den Vordergrund stellen. Existiert bereits ein Faktencheck kann dieser zum Beispiel als Kommentar direkt unter dem Inhalt geteilt werden.

Weiterführende Materialien:

- Skeptical Science: Widerlegen, aber richtig.
- NATO StratKom CoE: Fact-checking and debunking.
- Truth in Journalism: Fact-Checking Guide.

Gegenrede: Häufig werden propagandistische oder hasserfüllte Inhalte eingesetzt, um Debatten koordiniert zu unterminieren oder Personen(gruppen) zu delegitimieren. Weniger spezifisch als Debunking eignet sich Gegenrede (oder »Counterspeech«) als taktische Reaktionsmöglichkeit auf problematische Inhalte mit großer Reichweite. Bei der Gegenrede geht es in erster Linie darum, die mitlesenden Nutzer:innen zu erreichen, indem mit plausiblen Argumenten dem problematischen Inhalt gezielt widersprochen wird. Da Behauptungen im Internet häufig auf etablierten Mythen und Narrativen aufbauen, sollte eine Sammlung von Argumenten vorgehalten werden.

Weiterführende Materialien:

- HateAid: Hassrede im Netz kontern: So geht Counterspeech.
- ndm: HELPDESK. Anti-Hass-Strategien.
- ShePersisted: Persisting and Fighting Back Against Misogyny and Digital Platforms' Failures.

Argumentationshilfen:

- Nichts gegen Juden: »Ich habe ja nichts gegen Juden, aber…«
- Amadeo Antonio Stiftung: Rechtspopulistische Gesprächsstrategien.
- Amadeo Antonio Stidtung: Sprechen und Berichten über Sinti und Roma.
- ProAsyl et al.: Pro Menschenrechte. Contra Vorurteile.
- #respecktcheck. Homosexuellen- und transfeindlichen Vorwürfe.

Counter-Narrative: Storytelling – die Mitteilung von Botschaften in einer Geschichte – kann einen möglichen Weg darstellen, um Zielgruppen emotional anzusprechen. Mit Counter-Narratives sollte jedoch vorsichtig umgegangen werden, um keinen Backlash zu riskieren. Zentraler Ansatz ist es, den Gruppen, die Informationsmanipulation ausgesetzt sind, eigene Werte zu vermitteln und dabei Schwachstellen der Akteur:innen der Informationsmanipulation aufzudecken.

Weiterführende Materialien:

- OECD: Good practice principles for public communication responses to mis- and sisinformation.
- Doublethink Lab: How to build a Counter-narrative?
- ISD: The Counter Narrative Handbook.

Filterung: Administrator:innen besitzen häufig die Möglichkeit, über die Einstellungen Filter – Listen mit Begriffen, Konten oder Emoji-Reaktionen (z. B. Clown, Erbrechen, Kothaufen oder Zorn) – für Kommentare auf ihren Seiten oder Gruppen auf Online-Plattformen anzulegen, um problematische Inhalte automatisch zu verbergen. Dies ist ein effektives Mittel, um proaktiv gegen Informationsmanipulation vorzugehen. Dabei gilt es jedoch zu berücksichtigen, dass Akteur:innen ihre Inhalte in der Regel schnell anpassen und auch unproblematische Inhalte zensiert werden können. Im Falle eines Shitstorms kann es außerdem sinnvoll sein, die Kommentar-Funktion auf der eigenen Seite oder Gruppe so lange zu deaktivieren, bis sich die Krisensituation beruhigt hat. In der Zwischenzeit können Maßnahmen der Krisenkommunikation definiert und umgesetzt werden.

Weiterführende Materialien:

- LMA NRW: Hasskommentare moderieren lernen.
- Facebook: Blockieren und Moderation.
- LinkedIn: Kommentare zu einem neuen LinkedIn-Seitenbeitrag deaktivieren.

Krisenkommunikation: Krisenkommunikation beschreibt Öffentlichkeitsarbeit bzw. den Informationsaustausch während einer Krise, um Schadensrisiken zu verhindern oder zu bewältigen. Im Kontext der Informationsmanipulation geht es darum, im Zuge eines erheblichen Vorfalls wie zum Beispiel eines Shitstorms, die Zuständigkeiten und Verantwortlichkeiten für die Kommunikation im Team zu klären und eindeutige Argumentationslinien aufzustellen. Es ist daher ein umfassenderes strategisches Instrument, um auf einen (erwartbaren) Vorfall zu reagieren.

Weiterführende Materialien:

- ndm: Wetterfest durch den Shitstorm.
- CEPPS: Crisis communication planning for disinformation threats.
- UNCCT: Crisis communication.

Proaktive Maßnahmen

Prebunking: Manipulative Verhaltensweisen und Narrative weisen nicht selten Ähnlichkeiten auf. Beim sogenanntes Prebunking geht es darum, diese Schwachstelle von Informationsmanipulation auszunutzen und relevante Zielgruppen durch gezielte Vorbeugung für die Informationsmanipulation zu sensibilisieren. Dies funktioniert nur, wenn eine Sensibilisierungskampagne zum Beispiel mit Kurzvideos oder Schaubildern durchgeführt wird, bevor sich Narrative bereits stark verbreitet haben. Prebunking setzt ein effektives Monitoring voraus, um potenzielle Risiken frühzeitig zu erkennen.

Weiterführende Materialien:

- Inoculation Science: Inoculation Theory: A beginners Guide.
- ISD: Narrative über den Krieg Russlands gegen die Ukraine.
- Tilt: Bad News.

Bewusstseinsbildung: Bei der Bewusstseinsbildung (oder »Awareness Raising«) geht es darum, ein grundlegendes Verständnis eines bestimmten Themengebiets unter den relevanten Ziel- und Interessensgruppen zu fördern und Verhaltensänderungen herbeizuführen. Dieses Instrument ist umfassender und strategischer angelegt als Prebunking und beinhaltet zum Beispiel zielgruppenorientierte Informationskampagnen.

Weiterführende Materialien:

- GCS: Guide to campaign planning: OASIS.
- Zivile Helden: Wie viel Zivilcourage steckt in Dir?
- EUvsDisinfo: Learn.

Netiquette: Für die eigenen Kanäle im digitalen Informationsraum sollte eine sogenannte Netiquette erarbeitet und öffentlich einsehbar gemacht werden. Dies kann ein strategisches Instrument sein, um auf eine zunehmende Anzahl kleinerer Vorfälle von Informationsmanipulation auf den eigenen Kanälen strategisch zu reagieren. Der Vorteil: Abhängig von den eigenen Einstellungen zu den Grenzen der Meinungsäußerungsfreiheit können Leitplanken für die Debatte aufgestellt werden. Damit wird eine transparente Grundlage für die Moderation eigener Internetauftritte, Seiten und Gruppen geschaffen.

Weiterführende Materialien:

- HateAid: Ein Leitfaden zum Umgang mit Digitaler Gewalt.
- wb-web: Die Netiquette – Eine Vorlage für Regeln zur legalen und fairen Kommunikation.
- Deutscher Bundestag: Netiquette.

Netzwerkaufbau: Der proaktive Aufbau von Unterstützungsnetzwerken ist ratsam, um in Krisensituationen auf zusätzliche Kapazitäten zum Umgang mit Informationsmanipulation zurückgreifen zu können. So kann das Netzwerk zum Beispiel das Melden von Inhalten, Debunking und Gegenrede unterstützen. Außerdem können gemeinsame Counter-Narratives entwickelt und verbreitet werden. Ein solches Netzwerk kann sowohl mit Mitgliedern der eigenen Organisation als auch aus externen Organisationen aufgebaut werden. Es gibt zudem bereits Initiativen, die sich auf die direkte Unterstützung von Betroffenen im Internet fokussieren.

Weiterführende Materialien:

- Ichbinhier: Digitale Zivilcourage – Gemeinsam für eine bessere Diskussionskultur.
- #NetzCourage.
- Aspen Institute Germany: Engaging German Influencers.

Counter-Branding: Anders als beim Prebunking oder der Bewusstseinsbildung stehen beim Counter-Branding explizit die Akteur:innen der Informationsmanipulation im Fokus. Counter-Branding bezieht sich dabei auf faktenbasierte und legitime Kommunikationsmaßnahmen, die den Akteur:innen der Informationsmanipulation einen potenziellen Reputationsschaden zufügen können. Dabei werden relevante Zielgruppen über die Absichten und Verhaltensweisen der Akteur:inne aufgeklärt.

Weiterführende Materialien:

- GCS: RESIST 2. Counter-disinformation toolkit.
- GEC: Three Ways to Counter Disinformation.
- GEC: Ukraine and the power of "we".

Resilienzbildung: Um Informationsmanipulation langfristig die Stirn zu bieten, bedarf es einer digitalen Resilienz und Medienkompetenz. Diese sollte mithilfe von Bildungsmaßnahmen und Kampagnen in allen Teilen der Gesellschaft aufgebaut werden. Zum Beispiel können die Zielgruppen bzw. potenzielle Multiplikator:innen auf Schulungen oder pädagogische Leitfäden hingewiesen werden. Zudem können eigene Veranstaltungen zur Thematik in Zusammenarbeit mit Faktencheck- oder Forschungsorganisationen abgehalten werden.

Weiterführende Materialien:

- BC4D: Neue Allianzen für das digitale Zeitalter.
- Facing Facts: Courses.
- LOVE-Storm: Angebote für Lehrende gegen Hass im Netz.

Ausblick:

Warum es jetzt wichtig ist, Kapazitäten aufzubauen

Informationsmanipulation wie zum Beispiel koordinierte Desinformationskampagnen hat sich unter den Bedingungen des digitalen Zeitalters zu einem wichtigen strategischen Instrument extremistischer Bewegungen und autoritärer Staaten weltweit entwickelt. Diese Akteur:innen verfolgen dabei teilweise unterschiedliche Absichten, dennoch überlagern sich ihre manipulativen Aktivitäten zunehmend. Dabei geht es ihnen häufig darum, gezielt Einfluss auf das Debattenklima, wichtige Stakeholder oder die Reputation politischer Gegner:innen zu nehmen, um die gesellschaftliche Polarisierung anzuheizen und hieraus (geo)politisches Kapital zu schlagen. Ihre Aktivitäten nutzen dabei oft existierende Unstimmigkeiten, Vorurteile und Stereotype aus, knüpfen an bereits etablierte Verschwörungserzählungen an und verstärken so Stimmen an den Rändern der Gesellschaft.

Hierbei profitieren sie außerdem von der zunehmenden Monetarisierung der Informationsmanipulation. So gibt es zum Beispiel immer mehr Dienstleister:innen, die im Auftrag manipulative Aktivitäten durchführen und somit zu einer noch stärkeren Verschleierung solcher Aktivitäten beitragen. Gleichzeitig schreitet die Entwicklung im Bereich der KI rasant voran, wodurch die Produktion und Verbreitung synthetischer Medieninhalte wie zum Beispiel Deepfakes noch schneller und in noch größerer Quantität stattfinden kann. In diesem Kontext sollten Kommunikationsverantwortliche aus Abgeordnetenbüros, Ministerien und Behörden – nach Definition ihres Mandats – StratKom-Kapazitäten in Bezug auf den Umgang mit Informationsmanipulation aufbauen. Dazu gehört die Einrichtung oder Weiterentwicklung einer Monitoring-Umgebung einschließlich der Nutzung direkter Datenquellen; die Klärung der Verantwortlichkeiten und Zuständigkeiten im Team; die Vorbereitung möglicher StratKom-Maßnahmen für einen relevanten Vorfall sowie der kontinuierliche Aufbau von Nachrichten- und Wissenskompetenz bei wichtigen Stakeholdern und in der Bevölkerung im Allgemeinen. Dabei ist es wichtig, sich auf die eigenen Prioritäten und Prioritätsbereiche zu fokussieren, um potenzielle Vorfälle der Informationsmanipulation frühzeitig identifizieren und bewerten zu können. Im Hinblick auf StratKom-Maßnahmen sollten Kommunikationsverantwortliche – insbesondere solche aus Abgeordnetenbüros – auch darauf achten, nicht selbst zu Akteur:innen der Informationsmanipulation zu werden, indem sie zum Beispiel vorsorglich Regeln für die faire politische Auseinandersetzung annehmen. Darüber hinaus sollte bei der StratKom sorgfältig abgewogen werden, wann überhaupt auf einen Vorfall mit taktischen Handlungen reagiert werden sollte, um die Verbreitung problematischer Inhalte nicht weiter zu befördern. Grundsätzlich existieren viele Handlungsmöglichkeiten auf Vorfälle strategisch-kommunikativ zu reagieren, die von sachlich-informativen Kampagnen bis zu verhaltensorientierten Kommunikationsstrategien reichen. Der eigene Umgang mit Informationsmanipulation hängt damit stark vom eigenen Mandat, der Art und Priorität eines Vorfalls sowie den zur Verfügung stehenden Kapazitäten ab.

»GLEICHZEITIG SCHREITET DIE ENTWICKLUNG IM BEREICH DER KI RASANT VORAN, WODURCH DIE PRODUKTION UND VERBREITUNG SYNTHETISCHER MEDIENINHALTE WIE ZUM BEISPIEL DEEPFAKES NOCH SCHNELLER UND IN NOCH GRÖSSERER QUANTITÄT STATTFINDEN KANN.«

Endnoten

1 Entous, A., Nakashima, E., FBI in agreement with CIA that Russia aimed to help Trump win White House, The Washington Post, 16.12.2016, https://www.washingtonpost.com/politics/clinton-blames-putins-personal-grudge-against-her-for-election-interference/2016/12/16/12f36250-c3be-11e6-8422-eac61c0ef74d_story.html, Letzter Aufruf: 05.12.2023.

2 Europäische Kommission, Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen: Europäischer Aktionsplan für Demokratie COM(2020) 790 final, 03.12.2020, IMMC.COM%282020%29790%20final.DEU.xhtml.1_DE_ACT_part1_v3.docx (europa.eu), Letzter Aufruf 05.12.2023.

3 Landesanstalt für Medien NRW, Eine Regulierung von Desinformation ist möglich, 10.11.2021, Eine Regulierung von Desinformation ist möglich - Pressemitteilungen - die medienanstalten (die-medienanstalten.de), Letzter Aufruf: 05.12.2023.

4 Vraga, E. K., Defining Misinformation and Understanding its Bounded Nature: Using Expertise and Evidence for Describing Misinformation, 06.02.2020, https://www.tandfonline.com/doi/full/10.1080/10584609.2020.1716500, Letzter Aufruf: 05.12.2023.

5 bpb, Zwischen Theorien und Mythen: eine kurze begriffliche Einordnung, 11.11.2020, Zwischen Theorien und Mythen: eine kurze begriffliche Einordnung | Verschwörungserzählungen | bpb.de, Letzter Aufruf 05.12.2023.

6 Deutscher Bundestag, Antwort der Bundesregierung, Drucksache 19/20908, 08.07.2020, Drucksache 19/20908 (bundestag.de), Letzter Aufruf: 05.12.2023.

7 Europäische Kommission, Mitteilung der Kommission an das Europäische Parlament, den Rat, den Europäischen Wirtschafts- und Sozialausschuss und den Ausschuss der Regionen: Europäischer Aktionsplan für Demokratie COM(2020) 790 final, 03.12.2020, IMMC.COM%282020%29790%20final.DEU.xhtml.1_DE_ACT_part1_v3.docx (europa.eu), Letzter Aufruf 05.12.2023

8 Garzke, R., Daten deutscher Politiker veröffentlicht: Was über den Datenklau bekannt ist, Tagesspiegel, 04.01.2019, Daten deutscher Politiker veröffentlicht: Was über den Datenklau bekannt ist (tagesspiegel.de), Letzter Aufruf: 05.12.2023.

9 Wardle, C., Derakhshan, H., Information Disorder: Toward an interdisciplinary framework for research and policy making, Council of Europe report DGI(2017)09, 27.09.2017, 168076277c (coe.int), Letzter Aufruf: 05.12.2023.

10 Landesanstalt für Medien NRW, Was ist Desinformation? Betrachtungen aus sechs wissenschaftlichen Perspektiven, 06.03.2020, WasIstDesinformation_Paper_LFMNRW.pdf (medienanstalt-nrw.de), Letzter Aufruf: 05.12.2023.

11 EEAS, 1st EEAS Report on Foreign Information Manipulation and Interference Threats Towards a framework for networked defence, 07.02.2023, EEAS-DataTeam-ThreatReport-February2023-02.pdf (europa.eu), Letzter Aufruf: 05.12.2023.

12 i.A.a. Wardle, C., Derakhshan, H., Information Disorder: Toward an interdisciplinary framework for research and policy making, Council of Europe report DGI(2017)09, 27.09.2017, 168076277c (coe.int), Letzter Aufruf: 05.12.2023.

13 Smirnova, J., Winter, H., Ein Virus des Misstrauens: Der russische Staatssender RT DE und die deutsche Corona-Leugner-Szene, 05.11.2021, https://www.isdglobal.org/isd-publications/ein-virus-des-misstrauens-der-russische-staatssender-rt-de-und-die-deutsche-corona-leugner-szene1/, Letzter Aufruf: 05.12.2023.

14 Gensing, P., Russland und das Impfen. Widersprüchliche Propaganda, ARD Faktenfinder, 26.08.2021, https://www.tagesschau.de/faktenfinder/russland-staatssender-impfungen-101.html, Letzter Aufruf: 05.12.2023

15 WHO, Neue Studie der WHO verdeutlicht negative Auswirkungen von Infodemien und Fehlinformationen auf das Gesundheitsverhalten, 01.09.2022, Neue Studie der WHO verdeutlicht negative Auswirkungen von Infodemien und Fehlinformationen auf das Gesundheitsverhalten, Letzter Aufruf: 05.12.2023.

16 Smirnova, J., Arcostanzo, F., German-Language Disinformation about the Russian Invasion of Ukraine on Facebook, 01.03.2022, https://www.isdglobal.org/digital_dispatches/german-language-disinformation-about-the-russian-invasion-of-ukraine-on-facebook/, Letzter Aufruf: 05.12.2023.

17 IPCC, 2022: Climate Change 2022: Impacts, Adaptation and Vulnerability. Contribution of Working Group II to the Sixth Assessment Report of the Intergovernmental Panel on Climate Change. Cambridge University Press. Cambridge University Press, Cambridge, UK and New York, NY, USA, 3056 pp., doi:10.1017/9781009325844.

18 CAAD, Deny, Deceive, Delay (Vol 3): Climate Information Integrity Ahead of COP28, 29.11.2023, https://caad.info/analysis/reports/deny-deceive-delay-vol-3-climate-information-integrity-ahead-of-cop28/, Letzter Aufruf: 05.12.2023.

19 Best, V., Decker, F., Fischer, S., Küppers, A., Demokratievertrauen in Krisenzeiten: Wie blicken die Menschen in Deutschland auf Politik, Institutionen und Gesellschaft?, 26.04.2023, Studie Vertrauen in Demokratie in Krisenzeiten (fes.de), Letzter Aufruf: 05.12.2023.

20 Bundesamt für Verfassungsschutz, Desinformation als Mittel gezielter Einflussnahme fremder Staaten, Bundesamt für Verfassungsschutz - Spionage- und Proliferationsabwehr - Desinformation als Mittel gezielter Einflussnahme fremder Staaten, Letzter Aufruf: 05.12.2023.

21 Bradshaw, S., Bailey, H., Howard P. N., Industrialized Disinformation. 2020 Global Inventory of Organized Social Media Manipulation, https://demtech.oii.ox.ac.uk/wp-content/uploads/sites/12/2021/02/CyberTroop-Report20-Draft9.pdf, Letzter Aufruf: 05.12.2023.

22 Guerin, C. , Maharasingam-Shah, E., Public Figures, Public Rage: Candidate abuse on social media, 05.10.2020, https://www.isdglobal.org/isd-publications/public-figures-public-rage-candidate-abuse-on-social-media/, Letzter Aufruf: 05.12.2023.

23 Smirnova, J., Winter, H., Mathelemuse, N., Dorn, M., Schwertheim, H., Digitale Gewalt und Desinformation gegen Spitzenkandidat:innen vor der Bundestagswahl 2021, 16.09.2021, Digitale-Gewalt-und-Desinformation_v5.pdf (isdgermany.org), Letzter Aufruf: 05.12.2023.

24 Reveland, C., Debatte um Baerbock-Äußerung. Eine pro-russische Kampagne?, ARD Faktenfinder, https://www.tagesschau.de/faktenfinder/baerbock-zitat-101.html , Letzter Aufruf: 05.12.2023.

25 Klimpel, L., Geschlechtsspezifische Desinformation. Wie Politikerinnen im Netz diskreditiert werden, ARD Faktenfinder, 01.05.2021, https://www.tagesschau.de/faktenfinder/geschlechtsspezifische-desinformation-101.html, Letzter Aufruf: 05.12.2023

26 Berliner Staatskanzlei, https://twitter.com/RegBerlin/status/1540402071551332358, Letzter Aufruf: 05.12.2023.

27 Deutscher Bundestag, Sachstand. Die rechtliche Qualität medialer Auftritte der Bundesregierung mit Blick auf den Rundfunkstaatsvertrag, 14.06.2019, https://www.bundestag.de/resource/blob/656502/b61bab8c0d6c5e3f3e451537cd3012d5/WD-10-035-19-pdf-data.pdf, Letzter Aufruf: 05.12.2023.

28 Deutscher Bundestag, Sachstand. Die rechtliche Qualität medialer Auftritte der Bundesregierung mit Blick auf den Rundfunkstaatsvertrag, 14.06.2019, https://www.bundestag.de/resource/blob/656502/b61bab8c0d6c5e3f3e451537cd3012d5/WD-10-035-19-pdf-data.pdf, Letzter Aufruf: 05.12.2023.

29 Teetz, A., Ein Social-Media-Post ist kein Projektil: Konzeptionelle Herausforderungen durch Desinformation, 02.02.2023, s12399-023-00937-9.pdf (springer.com), Letzter Aufruf: 05.12.2023.

30 Unzicker, K., Desinformation: Herausforderung für die Demokratie, Einstellungen und Wahrnehmungen in Europa, 10.08.2023, ST-DZ_Desinformation_Herausforderung_fuer_die_Demokratie_Europa_2023.pdf (bertelsmann-stiftung.de), Letzter Aufruf: 05.12.2023.

31 Deutscher Bundestag, Beobachtung von Parteien durch den Verfassungsschutz, 09.03.2016, https://www.bundestag.de/resource/blob/425104/e0375fd93b9d020677398bc1ed1edf9e/wd-3-072-16-pdf-data.pdf, Letzter Aufruf: 05.12.2023.

32 Pamment, J., Nothhaft, H., Agardh-Twetman, H., Fjällhed, A., Countering Information Influence Activities: The State of the Art, 01.07.2018, Countering Information Influence Activities : The State of the Art, research report (msb.se), Letzter Aufruf: 05.12.2023.

33 Pamment, J., Nothhaft, H., Agardh-Twetman, H., Fjällhed, A., Countering Information Influence Activities: The State of the Art, 01.07.2018, Countering Information Influence Activities : The State of the Art, research report (msb.se), Letzter Aufruf: 05.12.2023.

34 Campaign Watch, Leitfaden für Digitale Demokratie, Startseite - Campaign-Watch, Letzter Aufruf: 05.12.2023.

35 Landesanstalt für Medien NRW, Eine Regulierung von Desinformation ist möglich, 10.11.2021, Eine Regulierung von Desinformation ist möglich - Pressemitteilungen - die medienanstalten (die-medienanstalten.de), Letzter Aufruf: 05.12.2023.

36 Amtsblatt der Europäischen Union, Verordnung (EU) 2022/350 des Rates, 01.03.2022, https://eur-lex.europa.eu/legal-content/DE/TXT/HTML/?uri=OJ:L:2022:065:FULL, Letzter Aufruf: 05.12.2023.

37 Hagey, K., Horwitz, J., Facebook Tried to Make Its Platform a Healthier Place. It Got Angrier Instead, The Wall Street Journal, 15.09.2021, Facebook Tried to Make Its Platform a Healthier Place. It Got Angrier Instead. - WSJ, Letzter Aufruf: 05.12.2023.

38 Zuckerberg, M., A Blueprint for Content Governance and Enforcement, https://www.facebook.com/notes/mark-zuckerberg/a-blueprint-for-content-governance-and-enforcement/10156443129621634/, Letzter Aufruf: 05.12.2023.

39 DISARM Foundation, Home Page, DISARM Foundation, Letzter Aufruf: 05.12.2023.

40 DISARM Foundation, DISARM Framework Explorer, Welcome to DISARM - Disarm Framework Explorer, Letzter Aufruf: 05.12.2023.

41 RND, Joseph Mercola – der Arzt, dem die Querdenker vertrauen, 24.01.2021, Joseph Mercola – der Arzt, dem die Querdenker vertrauen (rnd.de), Letzter Aufruf: 05.12.2023.

42 i.A.a. Pamment, J., RESIST 2 Counter-disinformation toolkit, January 2021, RESIST 2 Counter-disinformation toolkit (civilservice.gov.uk), Letzter Aufruf: 05.12.2023.

43 Pamment, J., The EU's Role in Fighting Disinformation: Crafting A Disinformation Framework, 24.09.2020, Pamment_-_Crafting_Disinformation_1.pdf (carnegieendowment.org), Letzter Aufruf: 05.12.2023.

44 Pamment, J., RESIST 2 Counter-disinformation toolkit, January 2021, RESIST 2 Counter-disinformation toolkit (civilservice.gov.uk), Letzter Aufruf: 05.12.2023.

45 i.A.a. Pamment, J., RESIST 2 Counter-disinformation toolkit, January 2021, RESIST 2 Counter-disinformation toolkit (civilservice.gov.uk), Letzter Aufruf: 05.12.2023.

46 i.A.a. Pamment, J., RESIST 2 Counter-disinformation toolkit, January 2021, RESIST 2 Counter-disinformation toolkit (civilservice.gov.uk), Letzter Aufruf: 05.12.2023.

ISD | Institute for Strategic Dialogue

Amman | Berlin | London | Paris | Washington DC

www.isdgermany.org