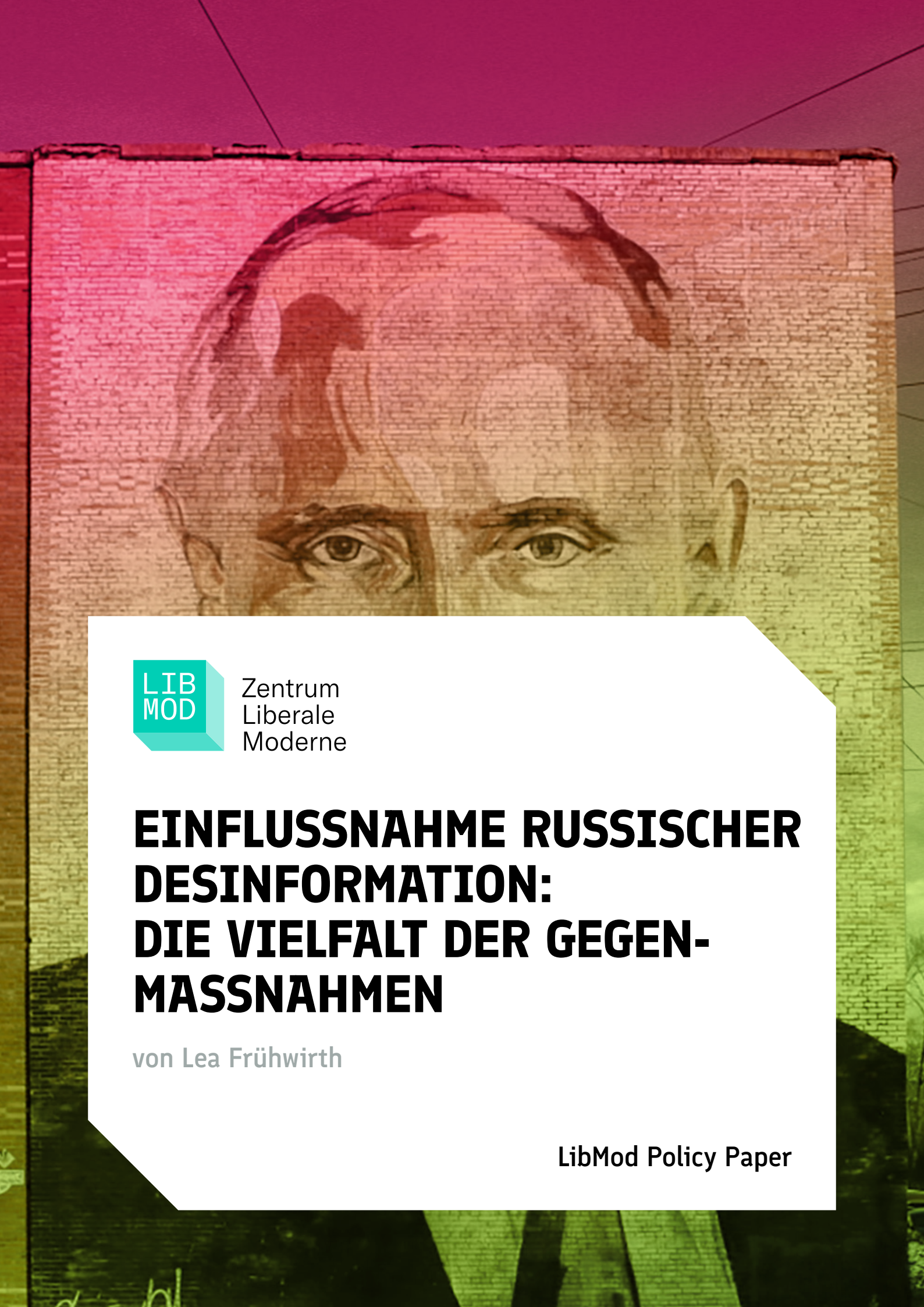

LIB MOD
Zentrum Liberale Moderne

EINFLUSSNAHME RUSSISCHER DESINFORMATION: DIE VIELFALT DER GEGEN-MASSNAHMEN

von Lea Frühwirth

LibMod Policy Paper

INHALT

Über die Autorin

Lea Frühwirth ist eine deutsche Psychologin und seit 2023 Senior Researcherin für Desinformation bei CeMAS, dem gemeinnützigen Center für Monitoring, Analyse und Strategie. Sie beschäftigt sich mit dem Aufdecken von Desinformationskampagnen im digitalen Raum und der Entwicklung systemischer Ansätze zur Bewältigung illegitimer ausländischer Einflussversuche.

Über das Projekt „Sicher durch die Transformation“

Die wachsende Verunsicherung und der Vertrauensverlust sind weit verbreitete Phänomene in allen westlichen Demokratien. Sicherheit während der Transformation zu gewährleisten, ist daher eine zentrale Aufgabe einer veränderungsbereiten und lernfähigen Politik. Das gemeinsame Projekt „Sicher durch die Transformation“ der Landesregierung Nordrhein-Westfalens und des Zentrums Liberale Moderne verfolgt das Ziel, konzeptionelle Ideen und Impulse zu diesem Thema zu liefern.

Im Rahmen von fünf Veranstaltungen, die in der Landesvertretung Nordrhein-Westfalens in Berlin stattfinden, werden zentrale Herausforderungen für Nordrhein-Westfalen diskutiert. Jede Veranstaltung wird von einem Impulspapier begleitet, das nicht nur die Politik in Nordrhein-Westfalen adressiert, sondern auch Entscheidungsträger auf Landes-, Bundes- und europäischer Ebene anspricht. Diese Impulse sollen einen Beitrag zur Bewältigung der anstehenden Transformationsprozesse leisten.

Das Projekt wird gefördert durch

Die Landesregierung
Nordrhein-Westfalen

1. Einleitung: Die Bedrohung durch Desinformation erkennen

Desinformationskampagnen stellen als illegitime Einflussversuche auf den öffentlichen Diskurs ein Risiko für die Gesellschaft dar. Wo die gemeinsame Faktengrundlage bedroht wird, braucht es wirksame Schutz- und Gegenmaßnahmen. Im vorliegenden Policy Paper soll die aktuelle Bedrohungslage abgebildet und die Vielfalt möglicher Gegenmaßnahmen vorgestellt werden.

2. Was sind Desinformationen und warum sind sie gefährlich?

Desinformation beschreibt bewusst verbreitete Unwahrheiten mit Manipulations- oder Schadensabsicht. Das Gefahrenpotenzial entsteht nicht allein durch das Vermitteln falscher Fakten zu einem Sachverhalt. Autoritäre Staaten wie Russland nutzen sie gezielt über Jahre hinweg zum Untergraben des Vertrauens in Qualitätsmedien, Politiker:innen und demokratische sowie staatliche Institutionen, um Gesellschaften zu destabilisieren. Auch werden bestimmte gesellschaftliche Gruppen gezielt stigmatisiert bzw. deren Stigmatisierung verschärft, was zu einem steigenden Gefahrenpotential für etwa Geflüchtete oder die muslimische und jüdische Bevölkerung führen kann. Das Phänomen hat also zahlreiche Facetten, die in ihrer Komplexität betrachtet und bearbeitet werden müssen, um eine effektive gesamtgesellschaftliche Bewältigung und Eindämmung zu erreichen.

Autoritäre Staaten wie Russland nutzen Desinformation gezielt und über Jahre hinweg, um Vertrauen zu untergraben und Gesellschaften zu destabilisieren.

3. Rückblick: Bundestagswahl 2025

Während Desinformation als beständiges Grundrauschen ein konstantes Risiko für demokratische Gesellschaften darstellt, werden Aktivitäten zu bestimmten Anlässen wie etwa Wahlen zusätzlich verstärkt. Während des Wahlkampfs zur vorgezogenen Bundestagswahl im Februar 2025 konnte CeMAS beispielsweise Aktivitäten der bekannten russischen Desinformationskampagne Doppelgänger dokumentieren. Diese verbreitet prorussische Inhalte in Form von gefälschten Nachrichtenartikeln und über soziale Netzwerke. Dabei wird anhand gefälschter Webseiten bekannter Medien eine vermeintliche Mehrheitsmeinung simuliert, beispielsweise gegen die Unterstützung der Ukraine gegen den russischen Angriffskrieg. Während des Wahlkampfs lagen weitere Schwerpunkte auf dem Schüren von Ängsten in der deutschen Bevölkerung und der Verbreitung diskreditierender Aussagen zu deutschen Parteien wie den Grünen oder der CDU, sowie zu den Kanzlerkandidaten Olaf Scholz, Robert Habeck und Friedrich Merz (Frühwirth, 2025e). Merz wurde dabei insbesondere Ende Januar in den Fokus genommen und diskreditiert (Frühwirth, 2025a). Die AfD wurde vom Doppelgänger-Netzwerk selten, aber positiv erwähnt. Ein weiteres prorussisches Netzwerk kommunizierte öfter zu AfD und BSW, ebenfalls stets positiv (Frühwirth, 2025c). Auch typische Falschbehauptungen zu angeblichem Wahlbetrug waren wieder im Umlauf (Smirnova, 2025; Frühwirth, 2025d). Eine mögliche Auswirkung von Desinformation auf Bevölkerung und Wahlergebnis ist nicht direkt messbar, da Menschen täglich vielen verschiedenen Reizen ausgesetzt sind und eine Meinungs- oder Verhaltensänderung nicht auf einen Einflussfaktor zurückgeführt werden kann.

Es gilt jedoch zu beachten, dass Desinformationskampagnen ihre Kernaussagen in vielen Einzelimpulsen beständig über Jahre hinweg streuen. Dies birgt die Gefahr, dass irreführende Behauptungen und diskreditierende Erzählungen schleichend Fuß fassen, da Inhalte, die öfter wahrgenommen werden, als glaubwürdiger eingestuft werden (Universität Marburg, o. D.). Auch haben repräsentative Erhebungen zu den Zustimmungswerten zu russischen Propagandaaussagen in der deutschen Bevölkerung gezeigt, dass diese seit Beginn des russischen Angriffskriegs auf die Ukraine signifikant angestiegen sind (Lamberty, 2024). Das Risiko entfaltet sich über die Langzeitperspektive. Es empfiehlt sich ein abgewogener Umgang, der das Phänomen weder bagatellisiert, noch vorauseilend katastrophisiert.

Am wirkungsvollsten ist der koordinierte und kooperative, anlassbezogene Einsatz von Gegenmaßnahmen, die an jeweils unterschiedlichen Schritten im Prozess ansetzen.

4. Desinformation als komplexe Herausforderung

Die Notwendigkeit wirksamer Eindämmungsmaßnahmen von Desinformation ist in der aktuellen weltpolitischen Lage evident. Das integrative Modell zum Umgang mit Desinformation betrachtet diese in all ihren Facetten, und eröffnet so vielversprechende Handlungsräume zur Problemeinordnung und -eindämmung (Lamberty & Frühwirth, 2023). Dadurch wird eine größere Bandbreite von Gegenmaßnahmen sichtbar, als dies bei einer reinen Fokussierung auf die Informationsperspektive möglich wäre. Das vorliegende Policy Paper gibt Einblick in die Vielfalt dieser Handlungsmöglichkeiten und zeigt exemplarisch auf, welche Werkzeuge zur Eindämmung von Desinformation zur Verfügung stehen.

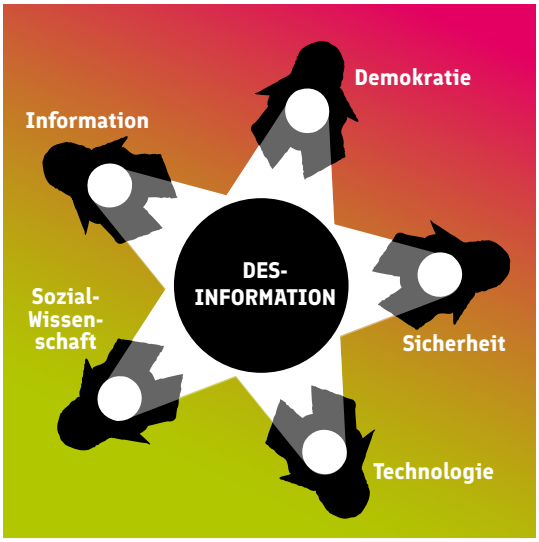

Abbildung 1: Das integrative Modell zum Umgang mit Desinformation soll die Komplexität des Phänomens sichtbar machen. (Lamberty & Frühwirth, 2023).

5. Die Vielfalt der Gegenmaßnahmen

Vereinfacht lässt sich die Verbreitung von Desinformation als Kommunikationsprozess darstellen, bei dem ein Akteur versucht, Inhalte in Umlauf zu bringen und damit eine Gesellschaft zu beeinflussen. Damit das funktioniert, muss die Message viele Individuen erreichen:

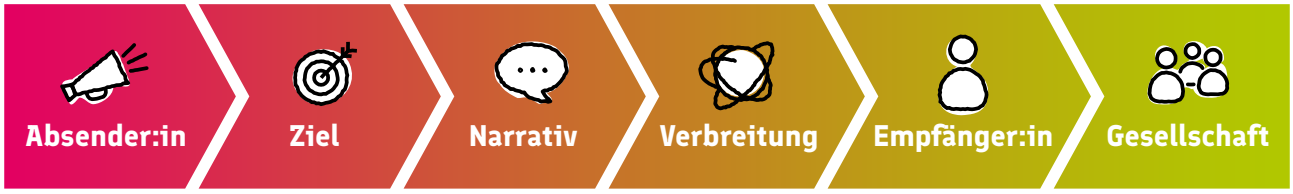

Abbildung 2: Die Verbreitung von Desinformation als Kommunikationsprozess (Lamberty & Frühwirth, 2023).

Gegenmaßnahmen sollen Fluss und Wirkung dieser Manipulationsversuche stören. Dafür kommen verschiedene Maßnahmen in Frage, die an jeweils unterschiedlichen Schritten im Prozess ansetzen und in das Expertisefeld unterschiedlicher Akteur:innen fallen. Am wirkungsvollsten ist der koordinierte und kooperative, anlassbezogene Einsatz dieser Gegenmaßnahmen. Im Folgenden soll eine Auswahl innovativer und inspirierender Maßnahmen vorgestellt werden, die exemplarisch zeigen, was möglich ist.

5.1. Beim Akteur ansetzen

Eine möglichst tiefgreifende Kenntnis des Akteurs, seiner Motive, Ressourcen und Vorgehensweisen hilft, möglichst passgenaue Gegenmaßnahmen zu ergreifen. Diese können auch am Akteur selbst ansetzen, wie im Bereich Deterrence ("Abschreckung"). Dabei soll die Kosten-Nutzen-Rechnung von Desinformation so verändert werden, dass sich der Einsatz für den Akteur nicht mehr rechnet und er seine Handlungen reduziert oder einstellt. Deterrence kann verschiedene Formen annehmen, wie beispielsweise das Signalisieren von Wachsamkeit oder das Verhängen von Sanktionen. Zwei offensivere Beispiele sollen die USA laut Medienberichten zum Schutz der Zwischenwahlen 2018 gegen russische „Trollfabriken" angewandt haben. Demnach blockierte das US-Militär den Internet zugang der russischen Internet Research Agency (IRA) am Wahltag, um ihre Einflussversuche zu unterbinden (Nakashima, 2019). Außerdem habe das US-Militär operative Kräfte aus der Kampagnenausführung der IRA direkt kontaktiert, um sie von illegitimen Einflussversuchen abzubringen (Barnes, 2018).

5.2. Die Verbreitung stören

Das proaktive Eingreifen in die Verbreitung von Desinformation hat sich ebenso als vielversprechender Eindämmungswinkel bewiesen. So haben investigative Recherchen der schwedischen IT-Forensik-Organisation Qurium und CORRECTIV Faktencheck zur oben erwähnten russischen Desinformationskampagne Doppelgänger in zwei Fällen zu spürbaren Störungen geführt (Bernhard et al., 2024d; Bernhard et al., 2024a). Nachdem von der Kampagne genutzte Webhosting-Dienstleister kontaktiert wurden, hatten diese Zugänge der Kampagnenbetreiber:innen gesperrt. Der Doppelgängerkampagne wurde damit zentrale Infrastruktur entzogen. Das führte zu wochenlangen Störungen in der Verbreitung ihrer gefälschten Nachrichtenseiten und zwang deren Betreiber zu einer Umstellung des Betriebs (Bernhard et al., 2024c; Frühwirth & Smirnova, 2024). Auch auf staatlicher Ebene wurden Gegenmaßnahmen gegen Doppelgänger-Webseiten gesetzt. Das amerikanische Justizministerium gab im September 2024 die Beschlagnahmung von 32 Doppelgänger-Webseiten bekannt (Bernhard et al., 2024b).

Auf europäischer Ebene hat der Digital Services Act (DSA) zum Ziel die Verbreitung von Desinformation über soziale Medien in der EU zu reduzieren. Das Plattformregulierungsgesetz nimmt insbesondere weit verbreitete digitale

Dienste („sehr große Online-Plattformen", sogenannte VLOPs) in die Pflicht, ihren Einfluss auf potenzielle systemische Risiken für die Gesellschaft zu analysieren und einzudämmen (Europäische Kommission, 2024). Aus Sicht der EU-Kommission verstoßen mehrere Plattformen gegen diese Vorgaben. Entsprechend sind aktuell (Stand Juni 2025) mehrere Verfahren anhängig, beispielsweise gegen X (ehemals Twitter), Meta oder TikTok (Europäische Kommission, 2025). Als Positivbeispiel im Bereich Contentmoderation kann die Plattform Bluesky gelten, die von vielen Nutzer:innen als Nachfolgeplattform von X verwendet wird. Als die russische Doppelgängerkampagne im Vorfeld der deutschen Bundestagswahl 2025 versuchte, auf Bluesky Fuß zu fassen, reagierte die Plattform schnell mit konsequenten Moderationsmaßnahmen und entfernte entsprechende Inhalte und Accounts (Nazari & Schwarz, 2025). Damit demonstrierte das verhältnismäßig kleine Bluesky: konsequentes Durchgreifen ist möglich und wirksam.

5.3. Individuen stärken

Maßnahmen, um Individuen für die manipulative Wirkung von Desinformation zu sensibilisieren, stehen nicht selten vor der Herausforderung, beim Publikum Gehör zu finden. Wie dies gelingen kann, zeigt beispielhaft die die schwedische Awareness-Kampagne „Don't be fooled" (Psychological Defence Agency, o. D.). In Broschüren, auf Plakaten und einer Webseite wird nicht nur vor Desinformation gewarnt. Es werden auch kompakt Kernpunkte zum Selbstschutz vermittelt und deren Bedeutung für Schwedens Sicherheit hervorgehoben. Schließlich wird die Rolle jedes Einzelnen bei der Abwehr von Desinformation betont, um die persönliche Relevanz aufzuzeigen. Durch die Betonung einer drohenden Manipulation („Don't be fooled") spricht die Kampagne bereits im Titel das menschliche Bedürfnis an, die eigene Entscheidungsfreiheit nicht durch externe Einflüsse beschränken zu lassen und positioniert die Kampagneninhalte damit als willkommene Unterstützung. In anderen Fällen wird auf gamifizierte Ansätze gesetzt, um Nutzer:innen in Spielform an das Thema Desinformation heranzuführen. In Online-Spielen wie Bad News, Go Viral! oder Harmony Square schlüpfen User:innen in die Rolle des Antagonisten, um typische Desinformationsstrategien kennen und verstehen zu lernen (Cambridge Social Decision-Making Lab, o. D.).

Auch Medienkompetenzschulungen stellen eine häufig besprochene Maßnahme zur Stärkung gegen manipulative Inhalte dar. Sie wenden sich typischerweise an junge Zielgruppen, die über das Bildungssystem erreicht werden können. Risiken durch Desinformation betreffen aber Menschen allen Alters. Ältere Zielgruppen sind jedoch schwieriger zu erreichen und es existieren bisher zu wenige Konzepte, um sie anzusprechen. Ein Beispiel, wie dies gelingen kann, ist das gemeinsam ausgerichtete Projekt „Business Council for Democracy" des Institute for Strategic Dialogue, der gemeinnützigen Hertie Stiftung und der Robert Bosch Stiftung. Es wählt den Zugang über den Arbeitsplatz. In freiwilligen Kursen bearbeiten Teilnehmende über mehrere Wochen hinweg in kurzen Sessions Themen wie Desinformation und Verschwörungserzählungen. Neben Hintergründen zu den Phänomenen werden auch konkrete Handgriffe vermittelt, wie auffällige digitale Inhalte auf ihre Authentizität überprüft werden können (Shiferaw & Laubenstein, 2022).

Wo irreführende Inhalte bereits im Umlauf sind, kommt es hingegen auf zeitnahe und anschlussfähige korrigierende Kommunikation an. Eine Richtigstellung muss einerseits schnell vielen Menschen bereitgestellt werden, und dabei andererseits so gestaltet sein, dass diese sie tatsächlich lesen. Ein Beispiel hierfür ist das taiwanesische 2-2-2-Prinzip: Demnach sollen Ministerien bei Bedarf binnen zwei Stunden mit einer Richtigstellung reagieren, die 200 Wörter beinhaltet und um 2 Grafiken ergänzt ist (Doublethink Lab, 2024). Die Kommunikation erfolgt also zeitnah, kompakt und anschaulich.

5.4. Die Gesellschaft schützen

Damit Schutz- und Eindämmungsmaßnahmen wirksam werden können, braucht es ausreichende Priorisierung und adaptive Ressourcenausstattung. Ein wichtiger Schritt dahin ist die regierungsseitig betriebene Institutionalisierung (OECD, 2023). So hat Frankreich 2021 eine Beobachtungsstelle für illegitime Einflussnahme aus dem Ausland namens VIGINUM geschaffen, um die digitale Öffentlichkeit zu schützen. Neben dem Aufdecken von Kampagnen fördert VIGINUM die ministerienübergreifende Zusammenarbeit und vernetzt sich international zum Wissensaustausch (Ferriol, 2022). In Schweden fungiert seit 2022 die Psychological Defence Agency als Früherkennungs- und -warnsystem zu illegitimen ausländischen Einflussversuchen und fördert den Aufbau von Resilienz dagegen (Woollacott, 2022; Psychological Defence Agency, 2024). Beide Agenturen veröffentlichen Publikationen und bereichern so auch die internationale Forschung. Sie zeigen, wie die sensible Rolle staatlicher Desinformationsbewältigung gestaltet werden kann, um die Bevölkerung vor externer Manipulation zu schützen ohne Freiheiten zu beschneiden.

Da illegitime Einflussversuche nicht an Staatsgrenzen halt machen, entstehen internationale Kooperationsbemühungen, um Ressourcen zu bündeln und Prozesse zu beschleunigen. Wer den Blick über die eigene Organisation hinaus wagt, Informationen offen teilt und sich partnerschaftlich unterstützt, kann mehr erreichen als jeder für sich allein. Das EU-weite Faktenchecker-Netzwerk EFCSN etwa bot zur Europawahl 2024 Einblicke in länderübergreifende narrative Schwerpunkte (European Fact-Checking Standards Network, o. D.). Mit dem Counter Disinformation Network (CDN), wurde ein Vernetzungs- und Kooperationshub für Desinformations-Forscher:innen geschaffen, der Vernetzung und Wissensaustausch im Bereich der Kampagnenaufdeckung stärkt, Doppelarbeiten vermeidet und gemeinsame Recherchen fördert (Alliance4Europe, o. D.).[1] Kooperative Ansätze ermöglichen eine schnellere und effizientere Entwicklung des Forschungsbereichs und eröffnen betroffenen Gesellschaften bessere Bewältigungsmöglichkeiten. Wo Desinformation auf Destabilisierung und Spaltung abzielt, setzen ihr diese Kooperationen belastbare Netzwerke, Vertrauensbildung und Zusammenhalt entgegen.

6. Fazit: Komplexität als Stärke nutzen

Die Komplexität von Desinformationskampagnen stellt zwar eine Herausforderung dar, bietet aber zugleich zahlreiche Ansatzpunkte, um ihr entgegenzuwirken. Um die Bevölkerung bestmöglich vor illegitimer ausländischer Einflussnahme zu schützen, sollte das gesamte Feld der verfügbaren Schutz- und Gegenmaßnahmen von Prävention bis Reaktion akteursübergreifend erschlossen und strategisch kombiniert zum Einsatz gebracht werden (Frühwirth, 2025b). Dazu braucht es ein ganzheitliches Bewältigungskonzept aus einem Guss, das Bewältigungs-Akteur:innen zusammenführt und ihre Kräfte und Instrumente bündelt. Frühzeitig stärkende Maßnahmen wie Sensibilisierungskampagnen oder Projekte zur Stärkung der von Desinformation angegriffenen gesellschaftlichen Werte schaffen einen Schutzschild, bevor Manipulationsversuche auftreten.

Ein kontinuierliches Monitoring illegitimer Einflussversuche sorgt im Akutfall dafür, dass Aktivitäten zeitnah bemerkt und wirksam eingedämmt werden können. Zur Qualitätssicherung gehören effiziente organisatorische Strukturen, Checks and Balances zur Prävention einer missbräuchlichen Verwendung sowie die regelmäßige Evaluation und Weiterentwicklung des eigenen Handelns. Da sich Vorgehensweise und Erscheinungsform von Desinformationskampagnen dynamisch weiterentwickeln, muss ein geeignetes Bewältigungssystem auf Adaption und kontinuierliche Verbesserung ausgelegt sein.

Eine zeitgemäße Bewältigungsstrategie zum Schutz der Bevölkerung sollte also auf ein kooperatives Vorgehen setzen, das die gesamte Bandbreite verfügbarer Maßnahmen von Prävention bis Reaktion fallbezogen und akteursübergreifend einsetzt, das eigene Vorgehen kontinuierlich weiterentwickelt und sich bereits heute auf die Herausforderungen von morgen einstellt.

1 Anmerkung: Die Autorin ist Mitglied im Counter Disinformation Network (CDN).

Quellen:

1. Alliance4Europe (o. D.). A4E Counter Disinformation Network (CDN). https://alliance4europe.eu/cdn
2. Barnes, J. (2018, 23. Oktober). U.S. Begins First Cyberoperation Against Russia Aimed at Protecting Elections. The New York Times. https://www.nytimes.com/2018/10/23/us/politics/russian-hacking-usa-cyber-command.html
3. Bernhard, M., Hock, A. & Thust, S. (2024a, 13. November). Doppelgänger: CORRECTIV-Recherchen legen russische Propaganda-Kampagne lahm. https://correctiv.org/faktencheck/russische-desinformation/2024/11/13/propaganda-desinformation-russland-recherchen-legen-doppelgaenger-kampagne-lahm/
4. Bernhard, M., Hock, A. & Thust, S. (2024b, 3. September). Doppelgänger: USA beschlagnahmen Propaganda-Webseiten, die Deutschland im Visier hatten. https://correctiv.org/faktencheck/russische-desinformation/2024/09/05/doppelgaenger-usa-beschlagnahmen-propaganda-webseiten-die-deutschland-im-visier-hatten
5. Bernhard, M., Hock, A. & Thust, S. (2024c, 18. Juli). Nach CORRECTIV-Recherche: Russische Propaganda-Kampagne gerät ins Stocken. https://correctiv.org/aktuelles/russland-ukraine-2/2024/07/18/nach-correctiv-recherche-russische-propaganda-kampagne-geraet-ins-stocken
6. Bernhard, M., Hock, A. & Thust, S. (2024d, 11.Juli). Russische Propaganda und Fakes – dank Technik aus Europa. https://correctiv.org/faktencheck/russische-desinformation/2024/07/11/doppelgaenger-wie-russland-eu-unternehmen-fuer-desinformation-und-propaganda-nutzt
7. Cambridge Social Decision-Making Lab (o. D.). Prebunking conspiratorial, electoral, and medical disinformation through online games. https://inoculation.science/inoculation-games
8. Doublethink Lab (2024, 9. August). Taiwan POWER: A Model for Foreign Information Manipulation & Interference Resilience. https://medium.com/doublethinklab/taiwan-power-a-model-for-resilience-to-foreign-information-manipulation-interference-70ea81f859b7
9. Europäische Kommission (2024, 25. Juli). A Safer & Fairer Online Environment. https://digital-strategy.ec.europa.eu/en/factpages/safer-fairer-online-environment
10. Europäische Kommission (2025, 12. Februar). Supervision of the designated very large online platforms and search engines under DSA. https://digital-strategy.ec.europa.eu/en/policies/list-designated-vlops-and-vloses
11. European Fact-Checking Standards Network (o. D.). https://efcsn.com
12. Ferriol, G. (2022, 2. November). VIGINUM Year #1. https://www.sgdsn.gouv.fr/publications/viginum-annee1
13. Frühwirth, L. (2025a, 4. Februar). Doppelgänger gegen Merz: Desinformationskampagne verstärkt Stimmungsmache auf X. CeMAS Bundestagswahl 2025 Monitoring. https://btw2025.cemas.io/artikel/doppelgaenger-gegen-merz
14. Frühwirth, L. (2025b, 25. Juni). Geschlossen gegen Manipulation. Integriertes Modell zur Bewältigung ausländischer Einflussversuche (FIMI). https://cemas.io/publikationen/fimi-geschlossen-gegen-manipulation
15. Frühwirth, L. (2025c, 28. Januar). Koordiniert und verifiziert: Pro-russische Kampagne veröffentlicht Hunderte Beiträge auf X. CeMAS Bundestagswahl 2025 Monitoring. https://btw2025.cemas.io/artikel/koordiniert-und-verifiziert
16. Frühwirth, L. (2025d, 28. Februar). Nach der Wahl: Falschbehauptungen zu angeblichem Wahlbetrug wandern durch soziale Medien. CeMAS Bundestagswahl 2025 Monitoring. https://btw2025.cemas.io/artikel/falschbehauptungen-wahlbetrug
17. Frühwirth, L. (2025e, 20. Januar). Russische Desinformation vor der Bundestagswahl: Doppelgänger-Kampagne macht Stimmung gegen Parteien. CeMAS Bundestagswahl 2025 Monitoring. https://btw2025.cemas.io/artikel/update-doppelgaenger
18. Frühwirth, L. & Smirnova, J. (2024, 19. November). Fortsetzung folgt: Die prorussische Desinformationskampagne Doppelgänger in Deutschland. https://cemas.io/publikationen/fortsetzung-folgt-doppelgaenger/
19. Lamberty, P. (2024, 22. Februar). Jahrestag des russischen Angriffskriegs auf die Ukraine: Glaube an Propaganda- und Verschwörungserzählungen. https://cemas.io/blog/prorussische-verschwoerungserzaehlungen/
20. Lamberty, P. & Frühwirth, L. (2023, 19. Juni). Informationsmanipulation als komplexe Herausforderung. Integratives Modell zum Umgang mit Desinformation. https://cemas.io/publikationen/integratives-modell-desinformation/
21. Nakashima, E. (2019, 27. Februar). U.S. Cyber Command operation disrupted Internet access of Russian troll factory on day of 2018 midterms. The Washington Post. https://www.washingtonpost.com/world/national-security/us-cyber-command-operation-disrupted-internet-access-of-russian-troll-factory-on-day-of-2018-midterms/2019/02/26/1827fc9e-36d6-11e9-af5b-b51b7ff3-22e9_story.html
22. Nazari, S. & Schwarz, K. (2025, 27. Januar). Sky's the Limit? Russian Influence Operation Doppelgänger Expands to Bluesky. https://alliance4europe.eu/doppelganger-bluesky
23. OECD (2023). Good practice principles for public communication responses to mis- and disinformation. OECD Public Governance Policy Papers, No. 30, OECD Publishing, Paris, https://doi.org/10.1787/6d141b44-en
24. Psychological Defence Agency (2024, 3. April). Our mission. https://mpf.se/psychological-defence-agency/about-us/our-mission
25. Psychological Defence Agency (o. D.). Get the tools! https://bliintelurad.se/en
26. Shiferaw, S. & Laubenstein, S. (2022, April). Der Business Council for Democracy. Info-Paket via https://www.bc4d.org
27. Smirnova, J. (2025, 21. Februar). Videos mit Falschbehauptungen über Wahlbetrug – Hinweise auf einen russischen Akteur. CeMAS Bundestagswahl 2025 Monitoring. https://btw2025.cemas.io/artikel/videos-mit-gefaelschten-wahlunterlagen
28. Universität Marburg (o. D.). Der „Illusory Truth Effect". https://www.uni-marburg.de/de/fb04/team-heck/forschung/der-illusory-truth-effect
29. Woollacott, E. (2022, 5. Januar). Sweden Launches Psychological Defense Agency To Counter Disinformation. Forbes. https://www.forbes.com/sites/emmawoollacott/2022/01/05/sweden-launches-psychological-defense-agency-to-counter-disinformation

Zentrum
Liberale
Moderne

Desinformationskampagnen stellen als illegitime Einfluss-versuche auf den öffentlichen Diskurs ein Risiko für die Gesellschaft dar.

Wo die gemeinsame Faktengrundlage bedroht wird, braucht es wirksame Schutz- und Gegenmaßnahmen. Im vorliegenden Policy Paper soll die aktuelle Bedrohungslage abgebildet und die Vielfalt möglicher Gegenmaßnahmen vorgestellt werden.

Gefördert durch

Die Landesregierung
Nordrhein-Westfalen

Herausgegeben im Juli 2025
vom

Zentrum Liberale Moderne
Reinhardtstraße 15
10117 Berlin

+49 (0)30 - 13 89 36 33
info@libmod.de

www.libmod.de