

Berlin, den 18.03.2025

Empfehlungen an die neue Bundesregierung für ein unabhängiges und wirksames Desinformationsmonitoring im digitalen Raum

*Erkenntnisse aus der Bundestagswahl 2025 und darüber hinaus – Bedeutung für
Online-Diskursforschung und resiliente Demokratie*

Es gab keine Wahlen im Superwahljahr 2024 ohne Desinformationskampagnen – auch die Bundestagswahl 2025 war von gezielten Angriffen auf die Öffentlichkeit betroffen. In einer Zeit, die ohnehin von multiplen Krisen geprägt ist, verschärft Desinformation die Spaltung bereits polarisierter Gesellschaften weiter.

Dies stellt eine ernste Herausforderung für liberale Demokratien dar: Desinformation untergräbt das Vertrauen in Institutionen, verzerrt öffentliche Debatten und beeinflusst die demokratische Meinungsbildung der Bürger:innen. Dabei ist Desinformation kein vorübergehendes Phänomen, sondern längst eine Konstante unseres Informations-ökosystems.

Warum Desinformationsmonitoring jetzt gestärkt werden muss

Die aktuelle geopolitische Gesamtlage mit erstarkenden und zunehmend koordiniert agierenden autoritäreren Kräften, die gezielt den rationalen und faktenbasierten Diskurs angreifen, macht den Kampf gegen Desinformation zu einer integralen Aufgabe einer Sicherheitsarchitektur, die gegen hybride Bedrohungen gewappnet sein muss. Nicht nur die Demokratie steht unter Druck, auch Sicherheit und wirtschaftliche Stabilität sind bedroht.

Akteure, die Desinformation generieren und verbreiten, testen fortlaufend neue Taktiken und setzen verstärkt Künstliche Intelligenz ein, um irreführende Inhalte kostengünstig, in großem Umfang und passgenau auf ihre Zielgruppen zugeschnitten zu produzieren.

Ein kontinuierliches Desinformationsmonitoring ist daher essenziell, um fortlaufend verlässliche Daten zu gewinnen, manipulative Dynamiken frühzeitig zu erkennen und deren Auswirkungen systematisch zu analysieren. Nur so lassen sich belastbare Evidenzen generieren – **als Grundlage für faktenbasierte Regulierung, wirksame Gegenmaßnahmen und eine stärkere Rechenschaftspflicht von Plattformen.**

Wachsende Bedrohungslage – klare Herausforderungslage

Diejenigen, die sich besonders für die Wahrung offener digitaler Diskursräume einsetzen – **unabhängige Forschende und zivilgesellschaftliche Organisationen** – stehen vor **erheblichen Herausforderungen**:

1. **Mangelnder Datenzugang und Plattformtransparenz:**

Forschende und zivilgesellschaftliche Akteure haben nur begrenzten Zugang zu relevanten Daten großer Plattformen. Trotz Digital Services Act (DSA) hakt dessen nationale Implementierung, Datenzugänge müssen bei Plattformen beantragt werden und werden oft willkürlich abgelehnt – wie das Verfahren von Democracy Reporting International gegen X [zeigt](#). Selbst bewilligte Datenzugänge sind durch lange Bearbeitungszeiten oft kaum praktikabel für zeitkritische Recherche.

2. **Fragmentierte Zuständigkeiten und unzureichende Ressourcen:**

Es fehlt weiterhin an einer koordinierten Gesamtstrategie zwischen staatlichen Institutionen, Wissenschaft und Zivilgesellschaft. Die Zusammenarbeit ist bislang zu wenig strukturiert und systematisch, was zu erheblichen Wissenslücken führt. Darüber hinaus mangelt es an tragfähigen Strukturen und Ressourcen für ein kontinuierliches, plattformübergreifendes Monitoring von Desinformation. Insbesondere die notwendige Forschungsinfrastruktur – etwa Serverkapazitäten, spezialisierte Sprachmodelle oder datenintensive Analysemethoden – ist mit hohen Kosten und erheblichem Ressourcenaufwand verbunden.

3. **Zunehmende politische Diskreditierung:**

Initiativen zur Bekämpfung von Desinformation und Stärkung gesellschaftlicher Resilienz geraten zunehmend unter politischen Druck - sowohl durch ausländische staatliche als auch durch inländische Akteure, die entsprechende Maßnahmen gezielt delegitimieren.

Fünf Empfehlungen für eine starke Monitoring-Infrastruktur

1. **Nachhaltige Forschungsfinanzierung über Wahlzyklen hinaus.**

Es braucht langfristige, strukturelle Förderung für Plattformforschung – losgelöst von projektbasierten Förderlogiken – um ein kontinuierliches Monitoring von Plattformen unabhängig von Legislaturperioden zu ermöglichen.

2. **Stärkung der Bundesnetzagentur als Digital Services Coordinator (DSC)**

mit ausreichend Planstellen und Forschungsbudget, um unabhängige Forschungsorganisationen zu unterstützen und ihrer Plattformaufsicht im Rahmen der Um- und Durchsetzung des DSA nachzukommen.

3. **Aufbau staatlicher Kapazitäten zur Erkennung ausländischer Einflussnahme.**

Die interministerielle Projektgruppe „Zentrale Stelle zur Erkennung ausländischer

Informationsmanipulation" (PG ZEAM) sollte als eine zentrale Stelle zur frühzeitigen Erkennung und Bekämpfung ausländischer Desinformationskampagnen weiter ausgebaut und dauerhaft mit ausreichenden Mitteln ausgestattet werden. Diese sollte in enger Kooperation mit Zivilgesellschaft und Wissenschaft agieren.

4. **Verständnis von Desinformationsmonitoring als Teil einer erweiterten Sicherheitspolitik, die hybride Bedrohungen ganzheitlich begreift und ihnen entgegentritt.** Sicherheitspolitische und gesellschaftspolitische Dimensionen müssen dabei nicht nur in einer gemeinsamen Problemdefinition zusammenlaufen, sondern auch in entsprechenden Lösungsstrategien gemeinsam gedacht und entsprechend finanziert und implementiert werden.

5. **Aufbau und Förderung eines unabhängigen Forschungsgremiums,** in dem zivilgesellschaftliche Forschende und Wissenschaftler:innen ihr Wissen bündeln, Ressourcen teilen und einen Dialog zu ethischen Standards in Desinformationsmonitoring organisieren können.

Unterzeichnet von (Stand: 21.03.2025):

Bertelsmann Stiftung

CeMAS - Center für Monitoring, Analyse und Strategie

Center for Advanced Internet Studies (CAIS)

Democracy Reporting International (DRI)

Institute for Strategic Dialogue Germany (ISD Germany)

Leibniz-Institut für Wissensmedien (IWM)

Dr. Johannes Breuer | Digital Society Observatory, GESIS – Leibniz-Institut für Sozialwissenschaften

Univ.-Prof. Dr. phil. André Calero Valdez | Institut für Multimediale und Interaktive Systeme, Universität zu Lübeck

Dr. Philipp Darius | Centre for Digital Governance, Hertie School of Governance

Dr. Wiebke Drews | Forschungsprojekt SPARTA, Universität der Bundeswehr München

Prof. Dr. Jasmin Riedl | Forschungsprojekt SPARTA, Universität der Bundeswehr München

Prof. Dr. Daniela Stockmann | Centre for Digital Governance, Hertie School of Governance

Ansprechpartner:innen:

Charlotte Freihse | Bertelsmann Stiftung

E-Mail: charlotte.freihse@bertelsmann-stiftung.de

Clara Ruthardt | Bertelsmann Stiftung

E-Mail: clara.ruthardt@bertelsmann-stiftung.de

Prof. Dr. Hendrik Heuer | CAIS

E-Mail: hendrik.heuer@cais-research.de

Josef Holnburger | CeMAS

E-Mail: josef.holnburger@cemas.io

Dr. Pia Lamberty | CeMAS

E-Mail: pia.lamberty@cemas.io