

HERBST DER FÄLSCHER

Russische Desinformation und die Landtagswahlen im Osten

Drei Landtagswahlen im Osten Deutschlands, bei denen der Kreml mit gefälschten Medienberichten, KI-Videos und Bot-Netzwerken versucht, Wahlkämpfe zu beeinflussen, rücken eine drängende Frage erneut auf die Tagesordnung. Wie lassen sich Desinformation und ausländische Einflussnahme wirksam bekämpfen? Dieses Spotlight zeigt, mit welchen Themen und Mitteln Moskau operiert, wie sich der Staat und die Gesellschaft gegen die Angriffe zur Wehr setzen können und wo weiterhin Lücken bestehen.



Foto: © Bradley Davis via flickr; Lizenz: CC BY-ND 2.0.

VON MIKHAIL POLIANSKII

Am 6. September wählt Sachsen-Anhalt einen neuen Landtag, zwei Wochen später folgen Mecklenburg-Vorpommern, die Berliner Abgeordnetenhauswahl und Kommunalwahlen in Niedersachsen. Seit Juni kursieren im Netz Kurzvideos, die Logos von ARD, ZDF, FAZ und anderen etablierten Medien kopieren und mit ihnen erfundene Skandale über Kandidatinnen und Kandidaten verbreiten.¹ Nach Angaben von DW-Faktencheck sind seit dem 24. Juni *mehr als 180 solcher Fake-Posts* auf X, Bluesky und TikTok erschienen, dokumentiert vom anonymen Recherchekollektiv Antibot4Navalny.² Die meisten Beobach-

ter ordnen die Kampagne der russischen Einflussoperation Matryoschka (auch unter dem Namen Overload bekannt) zu. Nach Einschätzung des Bundesamts für Verfassungsschutz und internationaler Analysen handelt es sich dabei um ein GRU-nahes Netzwerk, das mit Storm-1516 (siehe Infobox) verflochten ist und gezielt deutsche Wahlkämpfe ins Visier nimmt.³ Das ist keine neue Bedrohung, doch sie hat sich in den vergangenen Jahren (nicht zuletzt dank generativer KI) deutlich fortentwickelt und schafft neue Risiken.⁴ Neu dabei ist unter anderem die Ausweitung der Ziele. Erstmals rücken nicht mehr nur Spitzenpolitiker auf Bundesebene ins Visier, sondern auch weniger bekannte Kandidaten auf Landeslisten. Ein Beispiel ist der Linke Kandidat Eric Stehr aus Sachsen-Anhalt, Listenplatz zwei, dem in gefälschten Videos Mord, Sexpartys an einer Uni und Notenbetrug unterstellt wurden.⁵ Diese Verschiebung zeigt, wie tief russische Einflussnahme inzwischen in den deutschen Wahlprozess hineinreicht und wie ernst sie hierzulande genommen werden muss.⁶

DREI WIEDERKEHRENDE THEMENFELDER

Die Kampagne folgt einem inhaltlich erkennbaren Muster. Ein erster Fokus ist die *Vertiefung des Ost-West-Gegensatzes*.⁷ Ein gefälschtes Eurostat-Video behauptet, eine Mehrheit der Westdeutschen halte die Wiedervereinigung für einen „historischen Fehler“. Eurostat bestätigte DW, das Video nicht produziert und keine entsprechende Umfrage durchgeführt zu haben.⁸ Weitere Fälschungen behaupten eine geplante Teilung Deutschlands bis 2030, eine neue Berliner Mauer oder eine strukturelle Benachteiligung Ostdeutschlands bei Sicherheit und Infrastruk-

tur, teils unter dem Hashtag #TimeToDivideGermany. Damit sollen Menschen aus Ost- und Westdeutschland gegeneinander aufgebracht werden, unter anderem durch die Behauptung, Ostdeutsche würden von Westdeutschen verachtet oder diskriminiert.⁹ Gerade vor den Landtagswahlen in Sachsen-Anhalt und Mecklenburg-Vorpommern ist diese Linie brisant. Sie knüpft an Gefühle der Benachteiligung und „Ostalgie“ an, die von der AfD bereits mit der DDR-Symbolik und einem starken Fokus auf „ostdeutsche Identität“ politisch bespielt wird. Russische Kampagnen verstärken damit Narrative, die in vielen ostdeutschen Wahlkreisen ohnehin präsent sind. Sie erfinden also kein Problem, sondern versuchen, vorhandene Risse zu vertiefen.

Ein zweites Thema zielt auf die *Delegitimierung staatlicher Institutionen*. Nach dem Berliner Stromausfall im Dezember 2025 verbreiteten zum Beispiel TikTok-Accounts Videos, die eine Essensverteilung durch die AfD sowie ein angebliches staatliches Verbot dieser Hilfsaktion behaupteten. In der laufenden TikTok-Auswertung vom Center for Monitoring, Analysis and Strategy (CeMAS) werden solche Inhalte durchgängig mit einem Muster kombiniert, in dem die Bundesregierung, insbesondere Bundeskanzler Friedrich Merz, als bürgerfern und regelungswütig dargestellt wird, während die AfD positiv erscheint. Der Eindruck, der Staat sei unfähig, Krisen zu bewältigen, und „Volksparteien“ und etablierte Medien seien Teil eines korrupten Kartells, gehört zu den Kernbotschaften vieler dieser Clips.¹⁰

Der dritte Themenbereich betrifft die *Ukraine*. Da Deutschland zu den größten Gebern von Hilfen für Kiew zählt, versuchen pro-russische Akteure, die Ukraine als korrupt und die deutsche Solidarität als Überbelastung darzustellen. Ein konkretes Beispiel ist ein vielfach geteiltes TikTok-Video, das sich auf ein angebliches CIA-Dossier beruft und behauptet, Präsident Wolodymyr Selenskyj habe 400 Millionen Dollar aus westlichen Hilfsgeldern in Luxusvillen in der Ukraine, Italien und England investiert.¹¹ Faktenchecker haben diesen und viele andere ähnliche Vorwürfe als unbelegt und irreführend zurückgewiesen.¹² Nichtsdestotrotz finden solche Geschichten in Deutschland immer wieder einen politischen Widerhall. Häufig werden reale Korruptionsfälle in der Ukraine mit stark überzogenen oder frei erfundenen Vorwürfen vermischt, um den Eindruck zu erwecken, die Unterstützung Deutschlands sei grundsätzlich fehlgeleitet. In ostdeutschen Wahlkreisen, in denen Skepsis gegenüber Waffenlieferungen und die Angst vor steigenden Lebenshaltungskosten besonders ausgeprägt ist, können solche Kampagnen eine ohnehin kritische Stimmung weiter emotionalisieren und werden von Parteien wie der AfD gezielt aufgegriffen, etwa in Anträgen, die ein sofortiges Ende der Unterstützung für Kiew fordern.¹³

MOSKAUS TECHNISCHER WERKZEUGKASTEN: MEDIA-SPOOFING UND CONTENT-FARMEN

Technisch beruht ein wesentlicher Teil der Kampagne auf sogenanntem Media-Spoofing, also dem Nachbau von

Design, Schriftart und Logo etablierter Medienmarken. Die OSINT¹⁴-Gruppe Gnida Project konnte nachweisen, dass die Matroschka-Operation seit November 2024 für diese Zwecke mehr als 100 deutschsprachige Domains registriert hat, viele davon zunächst inaktiv und für spätere Aktivierung vorbereitet.¹⁵ Zu den dokumentierten Fällen zählen eine angebliche Affäre der damaligen Außenministerin Annalena Baerbock sowie eine gefälschte Anschuldigung gegen den FDP-Verteidigungspolitiker Marcus Faber, ein russischer Agent zu sein.¹⁶ Nach US-Angaben wurde eine vergleichbare Infrastruktur in den USA „im Auftrag und mit finanzieller Unterstützung der GRU“ betrieben, um rasch Falschinformationen zu erstellen und über ein Netzwerk imitierten Nachrichtenseiten zu verbreiten.¹⁷

Parallel dazu hat sich in den letzten Jahren ein zweites, technisch aufwendigeres Feld von KI-gestützten Content-Farmen etabliert, was in dieser Kampagne zunehmend eingesetzt wird. In der oben aufgegriffenen CeMAS Studie von Julia Smirnova identifiziert sie mindestens 72 deutschsprachige Accounts mit zusammen rund 1,1 Millionen Followern allein auf TikTok. Zwischen dem 15. November 2024 und dem 27. Januar 2026 veröffentlichten diese Accounts mindestens 5.265 Videos, die zusammen 162 Millionen Aufrufe, 2,7 Millionen Likes und rund 386.000 Kommentare erhielten. Die meistgesehenen Videos kamen auf rund 38 Millionen Wiedergaben.¹⁸ Inhaltlich behaupten die Videos erfundene neue Vorschriften (wie eine Hundesteuer, ein Verbot privater Gärten oder ein Wochenend-Staubsaugverbot) und stellen diese als Entscheidungen des Bundeskanzlers dar, ohne dass eine öffentliche Debatte stattgefunden hätte. Sprachliche Fehler in KI-generierten Vertonungen und Untertiteln sowie zeitlich eng beieinanderliegende Account-Registrierungen deuten laut CeMAS auf ein koordiniertes, Kreml-nahes Netzwerk hin.¹⁹ Ein Account veröffentlichte, zum Beispiel, am Anfang Videos mit russischer Tonspur, bevor er auf deutschsprachige Inhalte umstellte.²⁰

WIE WIRKSAM SIND DIE KAMPAGNEN?

Trotz dieser Zahlen bleibt die Frage nach der tatsächlichen Wirkung offen.²¹ Pablo Maristany de las Casas vom Institute for Strategic Dialogue (ISD) analysiert die aktuelle Kampagne und kommt zu dem Befund, dass „die Auswirkungen ... nicht signifikant sind. Das sehen wir auch an der künstlichen Amplifizierung der Inhalte“.²² Gemeint ist, dass viele Beiträge zunächst vor allem von Bot-Netzwerken und vernetzten Aktivistengruppen verstärkt werden und nur begrenzt Interaktionen oder Kommentare von echten Menschen auslösen.²³ CeMAS kommt für die Bundestagswahl 2025 zu einem ähnlichen Ergebnis. Selbst millionenfach ausgespielte Kampagnen ließen sich kaum mit messbaren Verschiebungen in der Wählerentscheidung verknüpfen.²⁴

Empirische Studien aus anderen Ländern stützen diesen Befund.²⁵ Untersuchungen zur Wirkung von Wahlkampf-Desinformation zeigen, dass Fake-Botschaften vor allem dann greifen, wenn sie an bestehende Identitäten und Überzeugun-

Media-Spoofing ist die täuschend echte Nachahmung von Design, Schrift und Logo etablierter Medienmarken, um Falschinformationen als vermeintliche Beiträge seriöser Redaktionen auszugeben.

Storm 1516 ist die von der Bundesregierung öffentlich attribuierte Bezeichnung für eine vom russischen Militärgedienste GRU unterstützte Einheit, die mit Fake-Webseiten, Deepfake Sequenzen und pseudo-investigativen Inhalten Wahlen und politische Debatten in Deutschland und Europa zu beeinflussen versucht. Dieser Einheit wurde unter anderem auch eine Einmischung in die Bundestagswahl 2025 nachgewiesen.

gen anknüpfen, und selbst dann meist eher Einstellungen in kleinen Teilgruppen als das gesamte Wahlergebnis beeinflussen. Gleichzeitig belegen Experimente zum „Illusory Truth Effect“, dass wiederholte Falschbehauptungen mit der Zeit glaubwürdiger erscheinen und damit die epistemische Grundlage demokratischer Entscheidungen untergraben können.²⁶ Eine Studie zu den tschechischen Parlamentswahlen 2021 kommt zu dem Schluss, dass Desinformation vor allem dort wirksam ist, wo sie auf bereits polarisierte Milieus trifft und durch lokale Akteure verstärkt wird.²⁷

Desinformationskampagnen wirken daher häufig kumulativ und indirekt. Sie verstärken bereits vorhandenes Misstrauen, polarisieren Diskurse und verschieben das „Overton-Fenster“, also den Bereich dessen, was öffentlich sagbar scheint. In Regionen mit ohnehin hohen AfD-Ergebnissen und angespannten sozialen Lagen können solche Operationen den Schritt von Skepsis zu aktiver Unterstützung radikaler Parteien erleichtern. Zugleich zeigen Vergleichsstudien zur digitalen Öffentlichkeit, dass ein Mangel an „digital Agency“ (der Fähigkeit, Quellen einzuordnen, Inhalte zu hinterfragen und sich aktiv zu informieren) mit einer höheren Neigung zu rechtspopulistischen Einstellungen und Far-Right-Voting korreliert.²⁸

WAS SCHON GETAN WURDE UND WELCHE SCHRITTE NOCH Vorgenommen werden müssen

Die Reaktion der deutschen Sicherheitsbehörden ist inzwischen deutlicher und koordinierter, bleibt aber im Kern überwiegend reaktiv. Das Bundesamt für Verfassungsschutz bestätigt öffentlich „unzulässige ausländische Einflussnahme und Informationsmanipulation“ und ordnet die Aktivitäten der Matrjoschka-Kampagne klar Russland zu.²⁹ In Sachsen-Anhalt und Berlin ermittelt der Staatsschutz wegen Verleumdung, nachdem betroffene Kandidaten wie Eric Stehr Anzeige erstattet haben.³⁰ Gleichzeitig hat die Bundesregierung auf wiederholte hybride Angriffe und Wahlbeeinflussung mit diplomatischen Schritten wie der Einbestellung des russischen Botschafters reagiert.

Im Juni hat die Bundesregierung mit dem „Gemeinsamen Zentrum zur Abwehr hybrider Bedrohungen“ (GAZ Hyb-

rid) eine neue Koordinationsstelle geschaffen, in der unter anderem Verfassungsschutz, Bundesamt für Sicherheit in der Informationstechnik und Generalbundesanwaltschaft zusammenarbeiten. Eine der fünf Arbeitsgruppen des Zentrums widmet sich explizit „Desinformation und Einflussnahme“ fremder Mächte und soll Erkenntnisse über hybride Angriffe (einschließlich Wahlbeeinflussung) bündeln.³¹ Zugleich führen Polizei und Landeskriminalämter in mehreren Bundesländern Pilotprojekte zur Beobachtung politischer Deepfakes und zur Kooperation mit Faktencheck-Organisationen durch.

Nichtdestotrotz bleiben noch einige kritische Punkte offen. Eine der wichtigsten Schwachstellen bleibt, dass die Plattformen nach wie vor zögerlich handeln, obwohl Bot-Netzwerke und Desinformationskampagnen inzwischen gut dokumentiert sind. Instrumente wie der EU Digital Services Act (DSA)³², der großen Plattformen Transparenzpflichten, Risikobewertungen und Maßnahmen gegen systemische Desinformation auferlegt, werden ebenfalls in der Praxis noch nicht konsequent durchgesetzt.³³

Vor diesem Hintergrund lassen sich drei notwendige Maßnahmen skizzieren. Erstens brauchen Deutschland und die EU *mehr digitale Souveränität* bei den Plattformen und KI-Systemen. Wenn zentrale Nachrichtenströme über nicht-europäische, kaum regulierte Infrastrukturen laufen, bleibt die Bekämpfung von Desinformationskampagnen dauerhaft erschwert. Wer politische Inhalte algorithmisch ausspielt, sollte nachvollziehbar dokumentieren, nach welchen Kriterien dies geschieht und welche Netzwerke hinter auffälligen Mustern stehen. Diversifizierte Quellenanforderungen und klare Kennzeichnungspflichten für KI-Agenten müssen verpflichtend sein.³⁴ Für die kommende Wahl wären hier etwa verpflichtende Medien-Verifikationssysteme sinnvoll, die sicherstellen, dass Nutzerinnen und Nutzer sofort erkennen können, ob ein Video wirklich von ARD oder ZDF stammt, sichtbare Wasserzeichen oder plattformweite „Verified Media“-Labels.

Zweitens sollte die *Kooperation mit der Zivilgesellschaft und der Forschung* ausgebaut werden. Da staatliche Stellen oft erst einschreiten, nachdem Medien, Faktenchecker und zivil-

Mikhail Polianskii ist Postdoctoral Researcher am PRIF. Er forscht zur Außenpolitik Russlands sowie den Russland-EU/NATO-Beziehungen im Rahmen der Europäischen Sicherheit.



KONTAKT

polianskii@prif.org

PRIF, Darmstädter Landstr. 110–114, 60598 Frankfurt/M.
PVst, DPAG 43853, Entgelt bezahlt, ISSN-2512-627X

gesellschaftliche Organisationen Kampagnen öffentlich gemacht haben, sollten diese verlässlicher finanziert und unterstützt werden. Gerade mit Blick auf die anstehenden Wahlen im Osten wäre eine engere Verzahnung zwischen GAZ Hybrid, Landeswahlleitungen, lokalen Medienhäusern und Forschungsprojekten sinnvoll.

Drittens ist eine *offensive politische Kommunikationsstrategie* erforderlich, die nicht nur reaktiv „Fakten checkt“, sondern proaktiv kommuniziert, wie Desinformation funktioniert und welche Akteure dahinterstehen. Dazu gehört, offen zu benennen, dass Russland eine langfristige Strategie verfolgt, die deutsche Demokratie zu schwächen, ohne dabei den innerdeutschen Charakter politischer Konflikte zu negieren oder den Erfolg der AfD pauschal als „Produkt Moskaus“ zu rahmen. Bürger:innen in besonders betroffenen Regionen brauchen mehr Angebote politischer Bildung, lokale Medienförderung und sichtbare Ansprechpersonen, damit das Gefühl der Vernachlässigung nicht allein extremistischen Akteuren

überlassen bleibt. Der Staat kann und sollte hier mehr tun, gerade weil Abgeordnete und kommunale Mandatsträgerinnen besonders häufig Ziele solcher Kampagnen sind. Wichtige Maßnahmen wären Schutzprogramme gegen digitale Hetze, zentrale Hotlines für Desinformationsvorfälle im Wahlkampf und klare Protokolle, wie Behörden innerhalb weniger Stunden auf größere Kampagnen reagieren.

Viele dieser Maßnahmen wären nicht nur ein Schutz gegen Russland, sondern würden demokratische Gesellschaften generell gegen Desinformation robuster machen, von wem auch immer sie ausgeht. Denn am Ende entscheidet nicht, wer die Fälschungen in die Welt setzt, sondern ob eine Gesellschaft lernt, sich dagegen zu wappnen, bevor die nächste Wahl vor der Tür steht.

Der Text entstand im Rahmen des „Projekts PATTERN: How Does the Past Matter? Der russische Aggressionskrieg gegen die Ukraine und der Kalte Krieg“, das 2025 einen Fokus auf hybride Bedrohungen legte.

PRIF SPOTLIGHT: Das Peace Research Institute Frankfurt (PRIF) ist das größte Friedensforschungsinstitut in Deutschland. PRIF analysiert die Ursachen gewaltsamer internationaler und innerer Konflikte, erforscht die Bedingungen des Friedens und arbeitet daran, den Friedensgedanken zu verbreiten.

V.i.S.d.P.: Karin Hammer, Öffentlichkeitsarbeit (PRIF), Darmstädter Landstr. 112, Frankfurt am Main, Telefon (069) 959104-0, info@prif.org, www.prif.org. Design: Anja Feix · Layout: PRIF · Druck: Druckerei Spiegler

Textlizenz: Creative Commons (Namensnennung/Keine Bearbeitungen/4.0 International).

Die verwendeten Bilder unterliegen eigenen Lizenzbedingungen.



Fußnoten und weiterführende Links:
prif.org/spotlight1326-fn
DOI 10.48809/prifspot2613

