APuZ
Aus Politik und Zeitgeschichte

Schild, Schwert – und Social Media

Strategien und Erscheinungsformen russischer Desinformation

Julia Smirnova
19.09.2025 / 15 Minuten zu lesen

Russlands moderne Propaganda knüpft an sowjetische „aktive Maßnahmen“ an: Ziel ist die Destabilisierung westlicher Demokratien, das Untergraben von Vertrauen in Institutionen und das Schüren gesellschaftlicher Konflikte.

Unmittelbar vor der Bundestagswahl 2025 wurden auf mehreren Social-Media-Plattformen Videos verbreitet, die Zweifel an der Rechtmäßigkeit der Wahl säen sollten. In einigen dieser Videos wurden angebliche Wahlzettel aus Leipzig gezeigt, auf denen die Partei Alternative für Deutschland (AfD) nicht aufgeführt war. In einem anderen Video wurden Briefwahlzettel mit Stimmen für die AfD geschreddert. Trotz rascher Dementis der regionalen Wahlleitungsbüros wurden die Videos weiterhin online verbreitet – unter anderem von einer AfD-Politikerin aus Hamburg. Diese Videos waren inszeniert, und die gezeigten „Wahlzettel“ waren möglicherweise speziell für die Videos angefertigt worden. Hinter der Kampagne stand mutmaßlich der russische Desinformationsakteur Storm-1516.[1]

Dies ist nur ein Beispiel für die Manipulationskampagnen, mit denen Russland vor der Bundestagswahl im Februar 2025 versuchte, die öffentliche Meinung in Deutschland zu beeinflussen, etablierte Parteien und Politiker:innen zu diskreditieren, die AfD zu unterstützen und polarisierende Themen zu verstärken.[2] Die Aktivitäten russischer Desinformationsakteure in Europa beschränken sich jedoch nicht nur auf Wahlen: Seit Beginn der groß angelegten russischen Invasion in die Ukraine im Februar 2022 richtet sich russische Desinformation konstant gegen ukrainische Geflüchtete in Europa, die ukrainische Regierung, die NATO sowie gegen demokratische Parteien und Institutionen. Die Falschbehauptungen variieren je nach Zielgruppe und Anlass und bilden einen kontinuierlichen „Feuerwehrschlauch der Lügen“.[3]

Russland setzt Informationsmanipulation strategisch ein, um seine Kriegsziele in der Ukraine zu unterstützen, westliche Gesellschaften langfristig zu destabilisieren, Demokratieskepsis zu verstärken und prorussische Kräfte zu stärken. In einem Informationsumfeld, in dem neue Technologien es einfach machen, täuschende Inhalte schnell und massenhaft zu erstellen und zu verbreiten, und in dem die Gatekeeper-Funktion journalistischer Medien zunehmend durch Empfehlungsalgorithmen sozialer Medien ersetzt wird, sind solche organisierten und koordinierten Kampagnen aus dem Ausland ein erhebliches Risiko für Demokratien. Sie zielen darauf ab, den Meinungsbildungsprozess nachhaltig zu beeinflussen, die gemeinsame Faktengrundlage für politische Debatten zu zerstören und demokratische Institutionen zu schwächen. Dabei bildet Russland Allianzen mit anderen autoritären Staaten und inländischen antidemokratischen Akteuren, bedient sich ihrer Ideen und Taktiken und schneidet eigene Propagandabotschaften so zurecht, dass diese von ihnen übernommen und weiterverbreitet werden.

Die Entwicklung der russischen Propaganda über die Jahre zeigt, wie sowjetische geheimdienstliche Ansätze wiederbelebt und durch digitale Technologien und marktwirtschaftliche Bedingungen weiterentwickelt und befeuert wurden

„Aktive Maßnahmen“ der Sowjetunion

Im Bereich der Desinformation und Propaganda im Ausland kann der Kreml auf umfassende Erfahrungen aus dem Kalten Krieg zurückgreifen. Jahrzehntelang setzte die Sowjetunion Propaganda und sogenannte aktive Maßnahmen der Geheimdienste ein, um ihre geopolitischen Interessen durchzusetzen und die als ideologische Gegner wahrgenommenen kapitalistischen Länder zu schwächen sowie deren Gesellschaften zu destabilisieren. Gegenpropaganda, also die Bekämpfung westlicher Narrative, war ein weiteres Ziel. Als „aktive Maßnahmen“ wurden diverse offene und verdeckte Taktiken bezeichnet, mit denen versucht wurde, Entscheidungen und die öffentliche Meinung im Ausland zu beeinflussen. Der sowjetische Geheimdienst KGB setzte eine Reihe solcher Taktiken ein, die von der Anwerbung von Agent:innen und der Erstellung gefälschter Dokumente bis zur verdeckten Unterstützung von Frontorganisationen wie dem World Peace Council oder der International Organisation of Journalists reichten. Diese Organisationen stellten sich nach außen als unabhängig dar, verbreiteten jedoch sowjetische Propaganda.[4] Die Streuung von Halbwahrheiten und Falschinformationen erfolgte gezielt auch durch persönliche Kontakte und Gespräche auf Konferenzen oder während der Besuche ausländischer Delegationen in der Sowjetunion. Darüber hinaus wurde Propagandamaterial gedruckt und verbreitet und wurden Pressekonferenzen organisiert sowie False-Flag-Angriffe inszeniert. Die Maßnahmen wurden akribisch und sorgfältig geplant, um erfundene Behauptungen möglichst glaubwürdig erscheinen zu lassen und die wichtige Zielgruppe der Entscheidungsträger:innen und Journalist:innen in die Irre zu führen.

Zu den bekanntesten Beispielen sowjetischer Desinformation gehört die Verbreitung der Behauptung, das HI-Virus sei in einem US-amerikanischen Labor entstanden. Diese Falschbehauptung wurde 1983 in der indischen Zeitung „Patriot“ platziert, die von der Sowjetunion finanziell unterstützt wurde. Später wurde diese Behauptung von sowjetischen Medien aufgegriffen und von einem ostdeutschen Wissenschaftlerpaar, wissentlich oder unwissentlich, verbreitet. So gelangte sie schließlich in westliche Massenmedien. Sowjetische Geheimdienste schreckten auch nicht davor zurück, rechtsextreme Angriffe und Drohungen zu inszenieren: So organisierten sie Ende der 1950er Jahre eine Kampagne, bei der antisemitische Graffiti im Namen deutscher Nazis hinterlassen wurden, um Westdeutschland zu diskreditieren. Vor den Olympischen Spielen 1984 in Los Angeles verschickten sie gefälschte Ku-Klux-Klan-Drohbriefe an Mitglieder des Internationalen Olympischen Komitees aus afrikanischen Ländern.[5]

Die moderne russische Desinformation weist auf strategischer und taktischer Ebene eine Reihe von Ähnlichkeiten mit dem sowjetischen Ansatz auf.[6] Die Schwächung und Destabilisierung geopolitischer Gegner sowie die Unterstützung der russischen Außen- und Sicherheitspolitik sind nach wie vor die zentralen Ziele russischer Einflussversuche im Ausland. Taktiken wie die Fälschung von Dokumenten, die Inszenierung von Aktionen unter falscher Flagge oder die Anwerbung von Einflussagent:innen aus den Reihen prorussischer Aktivist:innen und Politiker:innen werden auch heute von russischen Desinformationsakteuren eingesetzt. Die Gründung vermeintlich unabhängiger Organisationen wie des Global Fact-Checking Network – ein angeblich unabhängiges Netzwerk von Faktenchecker:innen, das in Wirklichkeit von einer kremlnahen Organisation betrieben wird – erinnert stark an die Taktik der Sowjetunion.[7]

Das moderne Informationsumfeld unterscheidet sich jedoch deutlich von dem zur Zeit des Kalten Krieges. Über soziale Medien wie Facebook, X, YouTube, Telegram oder TikTok können heutige Desinformationsakteure Zielgruppen im Ausland direkt ansprechen. Die in den vergangenen Jahren aufgedeckten russischen Kampagnen setzen eher auf die massenhafte, teilweise spam-artige Verbreitung von Desinformation niedriger Qualität als auf sorgfältig vorbereitete Aktionen, die Medien und Entscheidungsträger:innen täuschen sollen. Die moderne russische Desinformation wird nicht zentral geplant und ausgeführt. Daran sind mehrere staatliche und nichtstaatliche Akteure beteiligt, die nicht selten miteinander konkurrieren.[8]

Anfänge der digitalen Propaganda in Russland

Die Existenz der wohl bekanntesten russischen Trollfabrik, der Internet Research Agency (IRA), wurde 2013 in einem Enthüllungsbericht der regierungskritischen Zeitung „Nowaja Gaseta“ aufgedeckt.[9] Zu dieser Zeit erhielten die Angestellten der IRA den Auftrag, unabhängige russische Medien zu diskreditieren und unter falschen Identitäten Beiträge in sozialen Medien sowie Kommentare unter Onlineartikeln zu verfassen. Diese Kommentare sollten die russischen Machthaber und ihre Politik loben oder die USA und den Oppositionellen Alexej Nawalny kritisieren. Bereits 2011 und 2012 wurden Internettrolle eingesetzt, die aus der kremlnahen Jugendbewegung Naschi rekrutiert wurden. Sie sollten negative Kommentare zu Artikeln regierungskritischer russischer Medien und Blogger:innen verfassen und kremlfreundliche Narrative auf der russischen Plattform „VK“ verbreiten. Dies ging aus den 2012 geleakten E-Mails der Naschi-Pressesprecherin Kristina Potuptschik und des Leiters der staatlichen Jugendagentur Rosmolodjosch, Wassilij Jakemenko, hervor.[10] In den Folgejahren avancierte Potuptschik, die inzwischen auf der EU-Sanktionsliste steht, zu einer der Hauptauftragnehmerinnen des Kremls für digitale Propaganda. Sie war verantwortlich für das

Monitoring sozialer Medien, den Betrieb ganzer Netzwerke von Telegram-Kanälen sowie die Beauftragung von Blogger:innen, die gegen Bezahlung kremlfreundliche Beiträge veröffentlichten.

In den 2010er Jahren wurde digitale Propaganda im Inland für den Kreml immer wichtiger. Während Fernseh- und Radiosender sowie Printmedien in der ersten und zweiten Amtszeit von Präsident Wladimir Putin nahezu vollständig auf Regierungslinie gebracht wurden, war das Internet in Russland zu dieser Zeit noch frei von Zensur. Es wurde so zu einem Raum, in dem regierungskritische Medien, Blogger:innen und einfache Bürger:innen unabhängig agieren und ihre Meinung äußern konnten. Je bedeutender die digitale Öffentlichkeit in Russland wurde, desto eifriger versuchte der Kreml, diesen Informationsraum zu kontrollieren. Eine Taktik dabei war, den Raum zunächst mit kremlfreundlichen Inhalten zu überfluten, bevor restriktivere Maßnahmen wie Sperrungen, Repressionen gegen unabhängige Online-Redaktionen und Strafen für kritische Beiträge eingeführt wurden.[11]

Die Methoden der digitalen Propaganda, die später im Ausland eingesetzt wurden, wurden Anfang der 2010er Jahre im Inland erprobt: die Einrichtung einer Vielzahl eigener Online-Medien, Blogs, Telegram-Kanäle und Gruppen in sozialen Medien, der Aufbau von Kontakten zu bestehenden Telegram-Kanälen und Blogger:innen, die gegen Bezahlung Regierungspropaganda veröffentlichten, das sogenannte „Hack & Leak“, also die Veröffentlichung gestohlener E-Mails und Daten von Oppositionellen, sowie das Verfassen anonymer Beiträge in sozialen Medien und die koordinierte Verbreitung dieser Inhalte durch Fake-Profile und Bots.

Die Marktwirtschaft bot dabei günstige Bedingungen für digitale Desinformation und Propaganda: Propagandist:innen griffen auf Methoden zurück, die in einem florierenden Markt für Suchmaschinenoptimierung und digitales Marketing entwickelt wurden.[12] Die Aufträge wurden häufig von privaten Firmen ausgeführt. Die weitverbreitete Käuflichkeit von Content Creators in den sozialen Medien, die bereit waren, jegliche Inhalte gegen Bezahlung zu veröffentlichen, spielte dem Kreml in die Hände.

Staatsmedien

Die Einflusskampagnen im Ausland sind im Kontext der russischen, revisionistischen Außen- und Sicherheitspolitik zu verstehen. Sie nahmen vor allem in der zweiten Hälfte der 2010er Jahre deutlich zu, als die Konfrontation mit den USA, der EU und der NATO sowie die Aggression gegen die Ukraine zunahmen. Bezeichnend hierfür ist die Entwicklung des staatlichen Auslandssenders Russia Today (RT). Der Sender wurde 2005 als Instrument der Soft Power mit dem erklärten Ziel gegründet, ein positives Bild Russlands im Ausland zu verbreiten und der russischen Perspektive im internationalen Diskurs Gehör zu verschaffen. Mit der zunehmenden Aggressivität der russischen Außenpolitik gewann der Sender an Bedeutung, und seine Rolle wurde zunehmend sicherheitspolitisch aufgeladen. Bereits 2012 verglich die Chefredakteurin Margarita Simonjan ihren Sender in einem Interview mit dem Verteidigungsministerium. Während Russland 2008 Krieg gegen Georgien geführt habe, habe RT einen Informationskrieg gegen die ganze Welt geführt.[13]

Der Sender positionierte sich zunehmend nicht nur als die offizielle Stimme Russlands, sondern auch als Gegenpol zu den westlichen Mainstreammedien. Diese wurden als Teil der politischen Elite dargestellt, die angeblich vor allem im eigenen Interesse und gegen das Interesse der breiten Bevölkerung handele. RT versuchte, mit Verschwörungserzählungen gezielt demokratieskeptische Gruppen am linken und rechten Rand des politischen Spektrums im Westen anzusprechen.[14] Während der Covid-19-Pandemie verstärkte die deutsche Version des Senders beispielsweise systematisch die Stimmen von Corona-Skeptiker:innen und Impfgegner:innen und stellte die Regierungsmaßnahmen zur Pandemiebekämpfung als undemokratisch dar.[15] Die Verstärkung polarisierender Themen und demokratiefeindlicher Stimmen ist eine Strategie, die RT konsequent einsetzt. Damit verbreitet das Medium nicht nur prorussische Positionen, sondern versucht auch, Einfluss auf die Innenpolitik der Zielländer auszuüben, indem es destabilisierende politische Strömungen und spalterische Botschaften unterstützt. Politische Institutionen und etablierte Medien in den Zielländern werden von RT diskreditiert und als Teil eines undemokratischen Systems dargestellt.

Im Globalen Süden stellen sich die russischen Staatsmedien RT und Sputnik als Verbündete lokaler Regierungen dar. Sie schließen Partnerschaften mit Medien in Afrika und Lateinamerika, die ihre Inhalte kostenlos übernehmen und weiterverbreiten. So bilden sich autoritäre, antiwestliche Allianzen, wie am Beispiel des venezolanischen Senders Telesur deutlich wird: Dieser Sender verbreitet regelmäßig Inhalte russischer und chinesischer staatlicher sowie mit dem Staat verbundener Medien wie Xinhua, RT, Sputnik und TV BRICS.[16]

In der EU wurden russische Staatsmedien kurz nach Beginn des großangelegten Angriffs auf die Ukraine sanktioniert und Zugang zu ihren Websites gesperrt, sie versuchen jedoch kontinuierlich, mit verschiedenen Methoden das Verbot zu umgehen, um ihr Zielpublikum weiterhin zu erreichen. So richtet RT kontinuierlich neue alternative Domains ein, um Sperrungen zu umgehen. Russische Staatsmedien gründeten auch mehrere neue Marken für Medienprojekte, Websites oder Social-Media-Kanäle. Als Nachfolgeprojekt der staatlich finanzierten Videoplattform Redfish wurde beispielsweise das Medium RED ins Leben gerufen, das alle Verbindungen zum russischen Staat bestritt und vor allem ein junges, linkes Publikum ansprechen sollte. Das inzwischen auch von der EU sanktionierte Medium fokussierte sich stark auf den Krieg zwischen Israel und der Hamas sowie auf propalästinensische Proteste in Europa und verbreitete spalterische Botschaften und Narrative der Terrororganisation Hamas.[17]

Diplomatische und kulturpolitische Kanäle

Neben den Staatsmedien sind auch die diplomatischen Vertretungen im Ausland eine Säule des Ökosystems der russischen Propaganda.[18] Der diplomatische Status schützt Botschaften und ihre Social-Media-Kanäle vor Sanktionen oder Sperrungen. Nach Beginn der großangelegten Invasion in der Ukraine waren diese Kanäle aktiv daran beteiligt, russische Kriegsverbrechen zu leugnen und den Angriffskrieg zu rechtfertigen. Die Social-Media-Accounts der russischen Botschaften verbreiteten Falschinformationen über das Massaker von Butscha, das Verschwörungsnarrativ über angebliche Biowaffenlabore in der Ukraine und Desinformation über die „Entnazifizierung“ der Ukraine als Grund für die Invasion.[19]

Über die staatliche Agentur Rossotrudnitschestwo, die dem Außenministerium untersteht und laut Medienberichten auch Verbindungen zu Geheimdiensten unterhält, [20] betreibt Russland ein Netzwerk von Russischen Häusern im Ausland. Diese konzentrieren sich auf Einflussnahme durch Soft-Power-Instrumente wie Sprachkurse, kulturelle Veranstaltungen und Studienreisen nach Russland. In der Praxis beteiligen sich diese Einrichtungen jedoch nicht nur an kulturpolitischen, sondern auch an propagandistischen Aktivitäten. Dazu zählt beispielsweise die Diskursnormalisierung der Besetzung der Krim und weiterer ukrainischer Gebiete sowie die Verbreitung von Desinformation über die Ukraine. Im Russischen Haus in Berlin wurden beispielsweise Bücher und Filme präsentiert, die russische Propaganda-Narrative über die Ukraine und die Maidan-Revolution 2014 unterstützten. Zudem pflegte das Russische Haus in Berlin Verbindungen zu Aktivisten in Deutschland, die an der Organisation prorussischer Veranstaltungen und Propagandaaktivitäten beteiligt waren.[21]

Von Hackern und Doppelgängern

Bei verdeckten Einflussoperationen wird im Gegensatz zu offenen Propagandakanälen die Urheberschaft der Kampagnen verschleiert. Dabei werden Desinformation, Propaganda oder durch Hacks gestohlene Dokumente über Medien oder Accounts veröffentlicht, die ihre Verbindung zum Auftraggeberstaat verstecken und als unabhängige Medien oder besorgte Bürger:innen der Zielländer auftreten. Der digitale Raum bietet Desinformationsakteuren zahlreiche Möglichkeiten, ihre Identitäten zu tarnen oder fiktive Personen zu erstellen, und schafft besonders günstige Bedingungen für verdeckte Einflussnahme. Für russische digitale Einflusskampagnen werden regelmäßig erfundene Expert:innen, Journalist:innen, Whistleblower:innen und ganze Medien oder Organisationen geschaffen. Als der russische Geheimdienst GRU 2016 die E-Mails der Demokratischen Partei in den USA stahl und WikiLeaks zuspielte, geschah dies über die Figur des angeblich rumänischen Hackers Guccifer 2.0.[22] Der Desinformationsakteur Storm-1516 erfindet regelmäßig Augenzeug:innen, die in Videos entweder von Schauspieler:innen gespielt oder durch KI dargestellt werden.[23]

In Russland sind mehrere staatliche und nichtstaatliche Akteure für verdeckte Kampagnen tätig, die teilweise in Konkurrenz zueinander stehen. Mehrere russische Geheimdienste unterhalten spezielle Abteilungen für psychologische Kriegsführung. Die auf Einflussoperationen spezialisierte GRU-Einheit 54.777 betreibt beispielsweise Frontorganisationen wie Inforos.[24] Storm-1516 hat mutmaßlich Verbindungen zur GRU-Einheit 29155.[25] Die GRU-Einheiten 26165 und 74455 stehen hinter Hacker-Angriffen von Akteuren, die als „Cozy Bear“ und „Fancy Bear“ bekannt sind.[26] Auch die Geheimdienste SVR[27] und FSB[28] führen eigene Einflusskampagnen im Ausland durch. Pseudo-NGOs und Online-Medien wie Institute of the Russian Diaspora[29] oder Strategic Culture Foundation[30] dienen häufig als Cover für geheimdienstliche Operationen.

Eine weitere Gruppe relevanter Akteure sind private Unternehmen, die auf Einflusskampagnen spezialisiert sind. Sie arbeiten entweder direkt im Auftrag des Staates oder von privaten Personen, die sich – wie der inzwischen verstorbene Gründer der Wagner-Gruppe, Jewgeni Prigoschin, der die Trollfabrik Internet Research Agency betrieb – als „Einflussunternehmer“ etablieren wollen.[31] Nach dem misslungenen Aufstand Prigoschins gegen den Kreml wurden seine Medienunternehmen geschlossen.[32]

Die heutigen Desinformations-Auftragnehmer sind näher an den Staat angebunden und stärker von ihm abhängig. Ein Beispiel ist das Unternehmen Social Design Agency (SDA), das direkt vom Kreml mit verdeckten Einflusskampagnen im Ausland beauftragt wird. Gemeinsam mit der staatlich finanzierten Organisation ANO Dialog ist SDA für die sogenannte „Doppelgänger"-Kampagne verantwortlich, bei der prorussische Desinformation und Propaganda auf gefälschten Websites etablierter Medien veröffentlicht und von zahlreichen gefälschten Accounts in den sozialen Medien verbreitet wird. Die geleakten internen Dokumente der SDA belegen, dass das Unternehmen im Auftrag und unter Anweisungen der russischen Präsidialverwaltung arbeitet.[33]

Private Desinformations-Auftragnehmer sind einerseits agil und erfinderisch, was die Methoden angeht, mit denen sie die Gegenmaßnahmen der Social-Media-Plattformen umgehen und ihre Inhalte verbreiten können. Andererseits sind sie stark daran interessiert, die Wirkung ihrer Kampagnen gegenüber den Auftraggebern zu übertreiben. Dabei werden die priorisierten Reichweiten-Metriken nicht selten künstlich in die Höhe getrieben, was realistische Rückschlüsse auf die tatsächliche Effizienz der Kampagnen unmöglich macht. Eigenwerbung und Prahlerei gehören zum Geschäft: Prigoschin ließ einen Spielfilm über die Einflusskampagnen der IRA rund um die US-Wahl drehen, in dem deren Wirkung massiv übertrieben wurde. Bei der Bewertung solcher Kampagnen ist es daher wichtig, diesen Aspekt nicht außer Acht zu lassen und nicht unnötig zur Eigenwerbung der Akteure beizutragen.

Künstliche Intelligenz

Die sich rasant entwickelnden KI-Technologien verändern das Feld der Desinformation und werden dessen Zukunft prägen. KI-basierte Anwendungen für Übersetzungen und die Erstellung von Texten ermöglichen die einfache Produktion einer Vielzahl unterschiedlicher Texte in mehreren Sprachen und das Füllen ganzer Websites mit KI-generierten Inhalten. Auch audiovisuelle Inhalte können viel einfacher manipuliert und neu erstellt werden. Bereits jetzt nutzen staatliche und staatsnahe Desinformationsakteure generative KI, um Desinformationsinhalte massenhaft zu erstellen und zu verbreiten. Russische Desinformation gelangt auch in die Trainingsdaten für Large Language Models wie ChatGPT und Gemini und werden von Chatbots in ihren Antworten wiedergegeben.[34]

Die russische Einflusskampagne „Operation Overload" nutzt Deepfakes von Stimmen, erstellt KI-generierte Videos und Bilder und konnte laut einer Analyse der finnischen Plattform Checkfirst die Anzahl der erstellten Originalinhalte in diesem Jahr um 155 Prozent erhöhen.[35] Dabei wurde ein KI-Tool einer deutschen Firma benutzt, um Bilder zu generieren, die muslimische Männer beim Randalieren in Berlin und Paris zeigen und damit migrationsfeindliche Stimmungen schüren sollen. Eine andere Kampagne namens „CopyCop" verwendet KI, um gefälschte Nachrichtenseiten anzulegen, auf denen Desinformation platziert wird.[36]

Fazit

Die moderne russische Desinformation und Propaganda verbindet klassische Strategien aus der Zeit des Kalten Krieges mit neuen Informationstechnologien. Ein komplexes Netzwerk aus diversen staatlichen und nicht staatlichen Akteuren, Cover-Organisationen, Einflussagent:innen und Multiplikator:innen im Ausland ermöglicht es, unterschiedliche Zielgruppen mit speziell auf sie zugeschnittenen Botschaften anzusprechen. Das digitale Informationsumfeld schafft besonders günstige Bedingungen für Einflusskampagnen, während KI die massenhafte Produktion täuschender Inhalte beschleunigt und vereinfacht. Um sich vor diesen Angriffen zu schützen, müssen Politik, Wirtschaft und Zivilgesellschaft in Deutschland und der EU eine gemeinsame Bewältigungsstrategie entwickeln, die präventive und reaktive Maßnahmen umfasst.[37] Private Tech-Unternehmen – von Social-Media-Plattformen über Suchmaschinen bis hin zu KI-Entwicklern – müssen proaktiv die Verantwortung dafür übernehmen, dass ihre Tools und Plattformen nicht von autoritären Staaten missbraucht werden. Die Regulierungsmaßnahmen in diesem Bereich müssen verstärkt und konsequent umgesetzt werden. Vor allem ist jedoch ein politisches Verständnis dafür nötig, dass es sich bei russischen Einflusskampagnen um eine langfristige Strategie zur Destabilisierung handelt, auf die es eine umfassende strategische Antwort zu finden gilt.

Fußnoten

[1] Vgl. Max Hoppenstedt, Russische Trollgruppe verbreitet offenbar Fakevideos zur Briefwahl, 21.2.2025, ↗ https://www.spiegel.de/a-325b8c89-8dae-4adc-ada9-f8d9ab6dd9f2; Julia Smirnova, Videos mit Falschbehauptungen über Wahlbetrug – Hinweise auf einen russischen Akteur, 21.2.2025, ↗ https://btw2025.cemas.io/artikel/videos-mit-gefaelschten-wahlunterlagen.

[2] Vgl. Center für Monitoring, Analyse und Strategie (CeMAS), Autoritäre Strategien im Netz: Monitoring und Analyse digitaler Risiken rund um die Bundestagswahl 2025, 14.4.2025, ↗ https://cemas.io/publikationen/btw2025.

[3] Christopher Paul/Miriam Matthews, The Russian „Firehose of Falsehood" Propaganda Model, 11.6.2016, ↗ https://www.rand.org/pubs/perspectives/PE198.html.

[4] Vgl. Nicholas J. Cull et al., Soviet Subversion, Disinformation and Propaganda, Oktober 2017, ↗ https://www.lse.ac.uk/iga/assets/documents/arena/2018/Jigsaw-Soviet-Subversion-Disinformation-and-Propaganda-Final-Report.pdf.

[5] Vgl. Thomas Rid, Active Measures: The Secret History of Disinformation and Political Warfare, London 2020, S. 123–141.

[6] Vgl. Roman Horby et al., The Transformation of Propaganda: The Continuities and Discontinuities of Information Operations, From Soviet to Russian Active Measures, in: Nordic Journal of Media Studies 5/2023, S. 68–94.

[7] Vgl. Russia: Fact-Checking Is the Kremlin's Latest Propaganda Tool, 25.6.2025, ↗ https://rsf.org/en/russia-fact-checking-kremlins-latest-propaganda-tool.

[8] Dabei ist zu berücksichtigen, dass gerade geheimdienstliche Einflusskampagnen länger unentdeckt bleiben können. Ein vollständiger Vergleich wird erst möglich sein, wenn interne Dokumente und Anweisungen moderner Desinformationsakteure in der gleichen Qualität vorliegen wie von den sowjetischen Akteuren.

[9] Vgl. Alexandra Garmaschapowa, Gdje schiwut trolli i kto ih kormit, 9.9.2013, ↗ https://novayagazeta.ru/articles/2013/09/07/56253-gde-zhivut-trolli-i-kto-ih-kormit.

[10] Vgl. Anastasija Karimowa, Kremljowskaja Blogodel'nja, 13.2.2012, ↗ https://www.kommersant.ru/doc/1868022.

[11] Vgl. Ilya Kiriya, Control Strategies Over the Russian Internet, in: Media and Communication 4/2021, S. 16–26.

[12] Vgl. Sergey Sanovich, Computational Propaganda in Russia, Oxford 2017, ↗ https://demtech.oii.ox.ac.uk/wp-content/uploads/sites/12/2017/06/Comprop-Russia.pdf.

[13] Vgl. Alexander Gabujew, Njet nikakoj objektiwnosti, 7.4.2012, ↗ https://www.kommersant.ru/doc/1911336.

[14] Vgl. Ilya Yablokov/Precious N Chatterje-Doody, Russia Today and Conspiracy Theories: People, Power and Politics on RT, London 2021.

[15] Vgl. Julia Smirnova/Hannah Winter, Ein Virus des Misstrauens: Der russische Staatssender RT DE und die deutsche Corona-Leugner-Szene, Institute for Strategic Dialogue, November 2021, ↗ https://www.isdglobal.org/wp-content/uploads/2021/11/RT-DE_final-report.pdf.

[16] Vgl. Peter Benzoni, Media Vassalage: How Venezuela's TeleSUR Acts as Russia and China's Information-Laundering Front, 7.3.2015, ↗ https://securingdemocracy.gmfus.org/media-vassalage-how-venezuelas-telesur-acts-as-russia-and-chinas-information-laundering-front.

[17] Vgl. Europäische Union, Beschluss (GASP) 2024/2643 des Rates vom 8. Oktober 2024 über restriktive Maßnahmen angesichts der destabilisierenden Aktivitäten Russlands, ↗ https://eur-lex.europa.eu/eli/dec/2024/2643/2025-05-22.

[18] Vgl. US Department of State, GEC Special Report: Russia's Pillars of Disinformation and Propaganda, August 2020, ↗ https://2021-2025.state.gov/russias-pillars-of-disinformation-and-propaganda-report.

[19] Vgl. Vassilena Dotkova, Diplomacy by Disinformation: The Role of Russian Embassies in the Kremlin's Information War, 26.5.2025, ↗ https://factcheck.bg/en/diplomacy-by-disinformation-the-role-of-russian-embassies-in-the-kremlin-s-information-war.

[20] Vgl. Ivan U. Klyszcz, Rossotrudnichestvo in Africa: Propaganda and Soft Power, 22.10.2024, ↗ https://euvsdisinfo.eu/rossotrudnichestvo-in-africa-propaganda-and-soft-power.

[21] Vgl. Mariia Protsiuk et al., Russian Cultural Diplomacy in Germany, Kyjiw 2024, ↗ https://ui.org.ua/wp-content/uploads/2024/11/russian-cultural-diplomacy-in-germany.-ukrainian-institute.pdf.

[22] Vgl. United States of America v. Viktor Borisovich Netyksho et al., 31.7.2018, ↗ https://www.justice.gov/archives/sco/file/1080281/dl?inline.

[23] Vgl. Viginum, Analysis of the Russian Information Manipulation Set Storm-1516, Mai 2025, ↗ https://www.sgdsn.gouv.fr/files/files/Publications/20250507_TLP-CLEAR_NP_SGDSN_VIGINUM_Technical%20report_Storm-1516.pdf.

[24] Vgl. Anton Troianovski/Ellen Nakashima, How Russia's Military Intelligence Agency Became the Covert Muscle in Putin's Duels With the West, 28.12.2018, ↗ https://www.washingtonpost.com/world/europe/how-russias-military-intelligence-agency-became-the-covert-muscle-in-putins-duels-with-the-west/2018/12/27/2736bbe2-fb2d-11e8-8c9a-860ce2a8148f_story.html.

[25] Vgl. Viginum (Anm. 23)

[26] Vgl. United States of America v. Viktor Borisovich Netyksho et al. (Anm. 22)

[27] Vgl. Christo Grozev et al., Leaks Reveal How Russia's Foreign Intelligence Agency Runs Disinformation Campaigns in the West, 4.7.2024 ↗ https://theins.ru/en/politics/272870.

[28] Vgl. Dada Lyndell et al., Intercontinental Lies: FSB Launches Disinformation and Conspiracy Campaign in Africa, 8.2.2024, ↗ https://theins.ru/en/politics/268980.

[29] Vgl. Rat der Europäischen Union, Durchführungsverordnung des Rates zur Durchführung der Verordnung (EU) Nr. 269/2014 über restriktive Maßnahmen angesichts von Handlungen, die die territoriale Unversehrtheit, Souveränität und Unabhängigkeit der Ukraine untergraben oder bedrohen, 25.7.2023, ↗ https://data.consilium.europa.eu/doc/document/ST-11609-2023-INIT/de/pdf.

[30] Vgl. U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC), Treasury Escalates Sanctions Against the Russian Government's Attempts to Influence U.S. Elections, 15.4.2021, ↗ https://home.treasury.gov/news/press-releases/jy0126.

[31] Vgl. Marlene Laruelle/Kevin Limonier, Beyond „Hybrid Warfare": A Digital Exploration of Russia's Entrepreneurs of Influence, in: Post-Soviet Affairs 4/2021, S 318–335.

[32] Vgl. Serge Poliakoff, Trolls Behind the Mask of Journalists: How Yevgeny Prigozhin's Patriot Media Group Was Organized, in: Problems of Post-Communism 1/2025, S. 1–13.

[33] Vgl. Lea Frühwirth/Julia Smirnova, Fortsetzung folgt: Die prorussische Desinformationskampagne Doppelgänger in Deutschland, 19.11.2014, ↗ https://cemas.io/publikationen/fortsetzung-folgt-doppelgaenger.

[34] Vgl. A Well-Funded Moscow-Based Global „News" Network Has Infected Western Artificial Intelligence Tools Worldwide With Russian Propaganda, 6.3.2025, ↗ https://www.newsguardrealitycheck.com/p/a-well-funded-moscow-based-global.

[35] Vgl. Operation Overload: More Platforms, New Techniques, Powered by AI, Juni 2015, ↗ https://checkfirst.network/wp-content/uploads/2025/06/Overload%C2%A02_%20Main%20Draft%20Report_compressed.pdf.

[36] Vgl. Recorded Future, Russia-Linked CopyCop Uses LLMs to Weaponize Influence Content at Scale, 9.5.2024, ↗ https://go.recordedfuture.com/hubfs/reports/cta-2024-0509.pdf.

[37] Vgl. Lea Frühwirth, Geschlossen gegen Manipulation, 25.6.2025, ↗ https://cemas.io/publikationen/fimi-geschlossen-gegen-manipulation.