CeMAS

Fortsetzung folgt: Die prorussische Desinformations-kampagne Doppelgänger in Deutschland

Gefördert durch:
ALFRED LANDECKER FOUNDATION

Herausgeber

CeMAS – Center für Monitoring,
Analyse und Strategie gGmbH
Konstanzer Straße 15A, D-10707 Berlin
E-Mail: info@cemas.io
www.cemas.io
Berlin, November 2024

ISBN: 978-3-9825777-2-2

V.i.S.d.P. sind Miro Dittrich und
Gregor Bauer für CeMAS gGmbH.
Konzept und Redaktion: Lea Frühwirth
Text: Lea Frühwirth und Julia Smirnova
Mitarbeit: Anna Meyer

Design: PARAT.cc
Lektorat: Benjamin Triebe
Druck: Offizin Scheufele,
Tränkestraße 17, 70597 Stuttgart

Bildnachweis:

CeMAS/Eigene Screenshots. Die Bildrechte verbleiben bei CeMAS gGmbH.

Coverbild, Seite 1:
Getty Images / Bloomberg / Kontributor;
IMAGO / ZUMA Press Wire
Seite 6: IMAGO / photothek
Seite 11: IMAGO / SNA; Pexels /
Max Avans

Infografiken: PARAT.cc, Carolin Wabra

Ermöglicht wurde diese Veröffentlichung durch die Alfred Landecker Foundation.

Die Veröffentlichung stellt keine Meinungsäußerung der Alfred Landecker Foundation dar.

Fortsetzung folgt:
Die prorussische Desinformations-kampagne Doppelgänger in Deutschland

Gefördert durch:
ALFRED LANDECKER FOUNDATION


Bild
SZ
ODR

Inhaltsverzeichnis

4 Executive Summary

- Die verdeckte Einflussoperation Doppelgänger wird seit dem Beginn der vollumfänglichen russischen Invasion der Ukraine im Februar 2022 eingesetzt, um russische Kriegsziele zu unterstützen und die öffentliche Meinung in der Ukraine, der EU, den USA und weiteren Ländern zu manipulieren. Die im Sommer 2022 aufgedeckte Operation wird von russischen Unternehmen im Auftrag der russischen Präsidialverwaltung ausgeführt und konzentriert sich auf die Verbreitung von prorussischen und polarisierenden Inhalten online.
- Die russische Desinformationskampagne Doppelgänger ist auch 2024 weiterhin im deutschsprachigen Raum aktiv. Nach wie vor veröffentlicht sie irreführende prorussische Inhalte über kopierte oder eigene digitale Medienportale, deren Inhalte in erster Linie über Facebook und X (ehemals Twitter) verbreitet werden.
- Die Websites präsentieren sich als detailliertes Plagiat deutscher Medienmarken oder eigenständige Nachrichtenportale mit thematischen Schwerpunkten. Eingebettet in diesen Rahmen werden prorussische Artikel platziert. Technische Mechanismen dienen dem Schutz und Fortbestehen der Kampagne, auf Gegenmaßnahmen erfolgt eine Adaption der entsprechenden Websites.
- Für die Verbreitung auf Facebook kamen 2024 bezahlte Werbeanzeigen zum Einsatz, deren typische Erscheinungsform bereits mehrfach dokumentiert wurde – auch von der Plattform selbst. Dennoch konnten irreführende politische Werbeanzeigen mit prorussischem Inhalt weiterhin verbreitet werden, indem sie schlicht nicht als politische Werbeanzeigen gekennzeichnet werden.
- Für die Verbreitung auf X werden viele unterschiedliche Accounts eingesetzt, welche die Inhalte in Arbeitsteilung den Nutzer:innen zuführen. Typischerweise veröffentlicht eine Gruppe von Accounts neue Beiträge, die von einer anderen Gruppe amplifiziert werden. Die Plattform reagiert trotz an X gemeldeter Kampagnen und bereits eröffnetem Prüfverfahren nach dem Digital Services Act (DSA) nicht ausreichend konsequent, sodass Inhalte dieser Art bis Redaktionsschluss verfügbar waren.

- Ein Leak von internen Dokumenten der für Doppelgänger verantwortlichen Social Design Agency (SDA) gibt Einblick in die Kampagnenziele für Deutschland: Die Zustimmungswerte zur AfD sollen steigen, jene für die Grünen sinken. Gefördert werden sollen Zukunftsängste sowie die Haltung, „den eigenen Wohlstand“ nicht für den „Sieg über Russland“ opfern zu wollen.
- Die Konstanten im Vorgehen der Kampagne bieten eine Angriffsfläche, die zur Aufdeckung neuer Aktivitäten und ihrer Eindämmung herangezogen werden könnte.
- Den Aufwand verstärken, um die Kampagne wirksam einzudämmen: Die zur Verfügung stehenden Hebel wie wiederholte Muster zur Erkennung oder Plattformregulierung zur Eindämmung müssen konsequent und koordiniert genutzt werden. Gefragt sind hierbei staatliche Akteure, die betroffenen Plattformen sowie Forscher:innen im Bereich Desinformation.
- In diesem Report zeigt CeMAS, dass die Doppelgänger-Kampagne trotz Gegenmaßnahmen weiterhin Bestand hat und erörtert mögliche Gründe für die trotz vielfältiger Handlungsmöglichkeiten beständige Diskrepanz zwischen dem Ist- und Sollzustand der Kampagneneindämmung im digitalen Diskurs.


Frankfurter Allgemeine
ZEITUNG
FAZ.NET
Ampelkratie ist bereit, Deutschland zu spalten
BRD
DDR
Süddeuts
Volksdiplomatie

Einleitung

Die erstmals 2022 aufgedeckte Doppelgänger-Kampagne verbreitet prorussische Artikel gefälschter oder erfundener Nachrichtenseiten über Netzwerke von nicht-authentischen Social-Media-Accounts. Die russische Desinformationskampagne gilt als fortlaufend und wandlungsfähig, ihr typisches Vorgehen ist inzwischen gut dokumentiert. Als illegitimer Einflussversuch auf digitale westliche Diskursräume ist sie ein Teil der russischen hybriden Kriegsführung und stellt aufgrund ihrer vertrauenszersetzenden Impulse ein Risiko für die deutsche Gesellschaft dar. Umso wichtiger ist ihre effektive und effiziente Eindämmung. Angesichts des wiederholt offengelegten Vorgehens und strukturellen Aufbaus der Kampagne gibt es dafür eigentlich viele mögliche Ansatzpunkte. Dennoch kann sie auch im Jahr 2024 noch fortbestehen und ein internationales Publikum mit prorussischen Inhalten ansprechen, darunter auch Deutschland.

Der vorliegende CeMAS-Report trägt die Erkenntnisse zum vergangenen und aktuellen Erscheinungsbild der prorussischen Doppelgänger-Kampagne in Deutschland zusammen, überprüft das Fortbestehen der daraus abgeleiteten Verbreitungsmuster und stellt die verschiedenen Leerstellen in der Bewältigung dieser illegitimen russischen Einflussversuche heraus.

⑧ Doppelgänger: Bisher beobachtetes Vorgehen

Erst im Sommer 2022 deckten Journalist:innen und Desinformationsforschende die sogenannte Doppelgänger-Kampagne öffentlich auf und analysierten sie (Wienand et al., 2022; Alaphilippe et al., 2022; Aleksejeva et al., 2022; Nimmo & Agranovich, 2022; Institute for Strategic Dialogue [ISD], 2022a). Die verdeckte prorussische Einflussoperation begann bereits im Februar 2022, kurz nach dem Beginn der vollumfänglichen Invasion der Ukraine durch Russland. Sie verfolgt zum einen das Ziel, die Ukraine zu destabilisieren und die Unterstützung für den osteuropäischen Staat im Westen zu untergraben. Zum anderen versuchen die Akteur:innen hinter der Operation, westliche Verbündete der Ukraine zu schwächen, polarisierende Themen zu verbreiten, prorussische Stimmen zu unterstützen und für die Aufhebung der Sanktionen gegen Russland zu werben. Zu den Zielländern der Kampagne gehören insbesondere Deutschland, Frankreich, Italien, Polen, die USA, Israel und die Ukraine.

Doppelgänger wird der russischen Firma Social Design Agency/SDA (Rus. „Агентство Социального Проектирования“, Deu. „Agentur für soziales Design“) sowie der Structura National Technology (Rus. „ГК Структура“, Deu. „GK Struktura“), beide mit Sitz in Moskau, zugeordnet (U.S. Department of Justice, 2024; VIGINUM, 2023; Nimmo & Agranovich, 2022; Blum et al., 2024). Das US-Justizministerium und Viginum brachten zudem die russische Organisation ANO Dialog, die Desinformations- und Propagandaaktivitäten in Russland intern betreibt (Zholobova et al., 2023), mit der Kampagne in Verbindung. Die involvierten Firmen agieren laut internen SDA-Dokumenten (U.S. Department of Justice, 2024) mutmaßlich im Auftrag und in Abstimmung mit der russischen Präsidialverwaltung. Die Betreiber:innen installierten ein Monitoring der klassischen sowie der sozialen Medien und führten politische Analysen und Meinungsumfragen in den Zielländern durch, um zielgruppenspezifische Narrative zu entwickeln.

Die Akteur:innen hinter Doppelgänger verwendeten dabei eine Reihe von Taktiken, um prorussische Inhalte zu erstellen und zu verbreiten, die Reichweite der Kampagne zu messen und Gegenmaßnahmen der Social-Media-Plattformen zu umgehen:

1. Das zentrale Element der Doppelgänger-Kampagne ist die Erstellung von geklonten Websites, die die digitalen Auftritte etablierter Medien, Regierungsstellen und internationaler Organisationen optisch fast identisch replizierten. Dazu wurden Domains registriert, die sich von den echten Domainnamen nur durch wenige Buchstaben oder durch Domainendungen unterscheiden (z. B. *spiegel(.)ltd* oder *spiegeli(.)life* statt spiegel.de). Auf den gefälschten Nachrichtenseiten werden Artikel mit prorussischen oder spaltenden Narrativen veröffentlicht.
2. Ähnliche Artikel werden auch auf eigenen, speziell für die Kampagne erstellten Webportalen veröffentlicht, die wie authentische unabhängige Medienorganisationen oder Blogs wirken können. Dazu gehören Websites mit mehreren Sprachversionen wie RRN („Recent Reliable News") sowie länderspezifische Websites wie „Grenzezank", „Kaputte Ampel" oder „Meister Urian" (Bayrisches Landesamt für Verfassungsschutz [BayLfV], 2024).
3. Die Kampagne verwendet außerdem graphische und audiovisuelle Inhalte wie Videos, Memes, Bilder, Karikaturen und gefälschte Screenshots mit erfundenen Social-Media-Beiträgen von Politiker:innen (Auswärtiges Amt [AA], 2024). Vor allem zu Beginn der Kampagne enthielten solche Videos häufig Logos von etablierten Medien, um den Eindruck zu erwecken, dass sie von bekannten Medienorganisationen stammen (ISD, 2022a).
4. Um Links zu gefälschten und eigenen Medien zu verbreiten, sowie direkt prorussische Kommentare und audiovisuelle Inhalte zu posten und die Originalposts zu amplifizieren, verwendet die Kampagne von Anfang an eine Vielzahl von nicht-authentischen Accounts auf Social-Media-Plattformen. Der Einsatz von solchen Accounts wurde etwa für Facebook, Instagram (Nimmo & Agranovich, 2022), X (ISD, 2022a) und Telegram (ISD, 2022b) dokumentiert. Die Accounts sollen dabei wie authentische Nutzer:innen aus den Zielländern wirken. Zu diesem Zweck wurden auf Facebook beispielsweise Profilbilder verwendet, die von Social-Media-Auftritten echter Menschen gestohlen wurden (Wienand et al., 2022). Auf X posteten die Accounts Texte, die in

der Ich-Form geschrieben wurden, als würden sie von besorgten Bürger:innen stammen (ISD, 2022a).

5. Um Einschränkungen der Social-Media-Plattformen zu umgehen und die Reichweite der Kampagne zu messen, kamen mehrere Weiterleitungen und Webtrackingsoftware (Recorded Future, 2023; Nimmo et al., 2023) zum Einsatz. Die Social-Media-Posts enthielten Links zu sogenannten „Front-Domains", von denen Nutzer:innen unwissentlich über mehrere Weiterleitungsstufen zu den gefälschten oder eigenen Websites geführt wurden.
6. Auf Facebook wurden Links zu gefälschten Websites sowie anderen Inhalten zudem seit Beginn der Kampagne mithilfe bezahlter Werbung verbreitet (Nimmo & Agranovich, 2022).
7. Nicht-authentische Accounts verbreiteten 2022 außerdem Petitionen für den Stopp der Waffenlieferungen an die Ukraine, Kürzungen der Ausgaben für Geflüchtete und die Einführung einer staatlichen Kontrolle der Lebensmittelpreise (Aleksejeva et al., 2022, ISD, 2022a).

Doppelgänger ist lediglich ein Teil der umfassenden Bemühungen des Kremls, die öffentliche Meinung im Ausland zu manipulieren und Russlands Kriegsziele in der Ukraine mit Einflusskampagnen zu unterstützen. Die Implementierung durch private Firmen beeinflusst augenscheinlich einzelne Merkmale der Kampagne: etwa die Verwendung von Online-Marketing-Strategien oder Verhaltensweisen, die darauf ausgerichtet sind, Inhalte möglichst lange und großflächig auf Social-Media-Plattformen zu verbreiten und dabei hohe Verbreitungs- und Reichweitenzahlen zu erzeugen, um den Output der Kampagne gegenüber den Auftraggeber:innen zu demonstrieren. Obwohl der tatsächliche Einfluss der Kampagne auf die öffentliche Meinung in den Zielländern aufgrund der teilweise niedrigen inhaltlichen Qualität beschränkt zu sein scheint, erscheint die Operation aggressiv, beständig und insbesondere wandlungsfähig.


Selenskyjs neue Gegenoffensive
Deutschland am härtesten treffe
Tretz der Spekulationen über die Möglichkeit von Verhandlungen
ukrainische Präsident eine neue Gegenoffensive starten, die die
Verbündeten teuer zu stehen kommen wird.
21.07.2023, 14.53 Uhr

12 Aktueller Auftritt der Doppelgänger-Kampagne in Deutschland

Auch 2024 behielt die Doppelgänger-Kampagne ihren Fokus auf der Verbreitung prorussischer Inhalte in Form von vermeintlichen Nachrichtenseiten. Hierfür kamen sowohl Kopien großer deutschsprachiger Medienwebsites zum Einsatz als auch Eigenkreationen. Die verbreiteten Seiten existieren mitunter seit der ersten Jahreshälfte 2023 (AA, 2024).

Die Platzierung: Prorussische Artikel auf vermeintlichen Nachrichtenseiten

Für den Zeitraum 2023 bis 2024 wurden Plagiate der Medien Der Spiegel, Die WELT, FAZ, Süddeutsche Zeitung, BILD, ND-Aktuell, Morgenpost, Tagesspiegel, T-Online, Spektrum und Psychologie-heute dokumentiert, wobei jeweils alternative Domainendungen wie .ltd oder .pm genutzt wurden (AA, 2024; BayLfV, 2024; Chavane et al., 2024; Qurium, 2024; Milenkoski, 2024). Für manche der Kopien wurden gleich mehrere Alternativdomains angelegt. Die Detailtreue der imitierten Medienseiten ist laut eines Reports des Auswärtigen Amts auf ein fast vollständiges Plagiat des Quellcodes der Vorlagenseiten zurückzuführen. Mit bloßem Auge sei die Fälschung für Nutzer:innen so kaum noch erkennbar (AA, 2024).

Die Kampagne nutzt darüber hinaus eigens erstellte Portale mit thematischen Schwerpunkten, die die Platzierung prorussischer Inhalte auf den ersten Blick unauffällig verpacken sollen. Für den Zeitraum zwischen 2023 und 2024 wurden 17 solcher Portale dokumentiert, die vordergründig ihre jeweiligen Schwerpunktthemen wie Klimawandel, Migration, Streiks, Finanz- und Wirtschaftsthemen, Astrologie oder Verschwörungserzählungen bedienten (AA, 2024; BayLfV, 2024; Chavane et al., 2024; ClearSky Cyber Security, 2024; Milenkoski, 2024). In diesen Rahmen eingebettet wurden dann im Sinne der Desinformationskampagne die zentralen prorussischen Artikel platziert, die sich in ihrer inhaltlichen Ausrichtung zum Beispiel gegen die deutsche Regierung oder die Ukraine wenden.

Für den Zeitraum März 2023 bis Ende Mai 2024 dokumentierte das Auswärtige Amt 12.970 deutschsprachige Artikel auf den Seiten, die der Doppelgänger-Kampagne zugeordnet werden. Das Auswärtige Amt geht davon aus, dass generative künstliche Intelligenz genutzt wurde, um diese Menge herstellen zu können – etwa zur Textgenese oder zur Übersetzung aus anderen Sprachen (AA, 2024).

Abbildung 1
Screenshots von Doppelgänger-Artikeln aus dem Sommer 2024. Imitiert werden Spiegel und FAZ.

Seit ihrer erstmaligen Dokumentation 2022 ist die Doppelgänger-Kampagne mit wiederholter Exposition und Eindämmungsmaßnahmen konfrontiert (Alaphilippe et al., 2022; VIGINUM, 2023). Wie das beständige Auftreten von Doppelgänger-Aktivitäten demonstriert, sind diese Gegenmaßnahmen bisher allerdings nicht ausreichend. Seitdem sind immer wieder Anpassungen im Vorgehen beobachtet worden, die als Maßnahme zur Aufrechterhaltung des Kampagnenbetriebs interpretiert werden (Franklin et al., 2024a). Während beispielsweise zu Beginn die Zielseiten direkt verbreitet wurden, veröffentlicht die Kampagne jetzt variierende Links, die klickende Nutzer:innen über mehrere Instanzen zu den Inhalten weiterleiten. Dabei wird geprüft, ob ein:e Nutzer:in zur Zielgruppe für den jeweiligen Artikel zählt. Beim Klick auf einen deutschen Artikel wird ein:e französische:r Nutzer:in typischerweise

Aktueller Auftritt der Doppelgänger-Kampagne

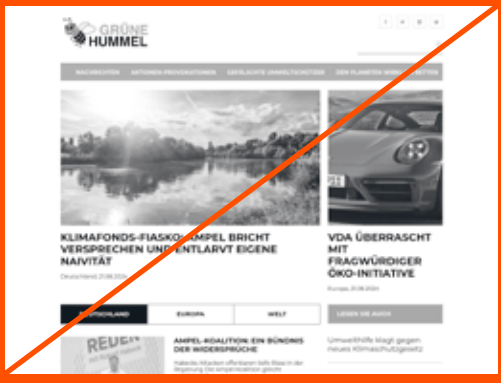


Abbildung 2
Screenshots verschiedener eigenständiger Doppelgängerportale von August 2024

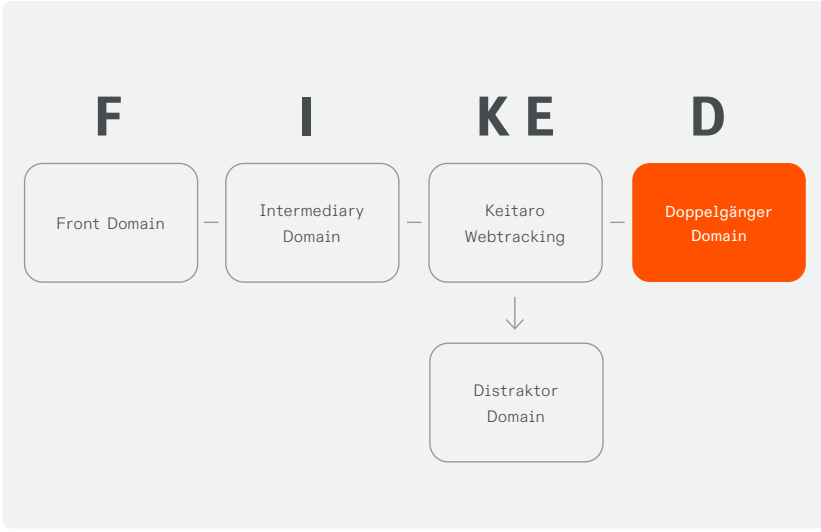


Abbildung 3
Weiterleitungsschema der Doppelgängerlinks (Qurium, 2024)

auf eine Distraktor-Domain geleitet, während ein:e deutsche:r Nutzer:in zum deutschen Artikel gelangt (Qurium, 2024). Auf Facebook verzichtete die Kampagne laut Plattformbetreiber Meta ab April 2024 auf die Verbreitung von URLs, und vermittelte ihre Inhalte stattdessen direkt im Beitrag. Meta führt diese Vorgehensweise auf Sperrungen der Ziel-Domains auf Facebook zurück (Franklin et al., 2024a). Im August berichtete der Plattformbetreiber wieder von verbreiteten Links (Franklin et al., 2024b).

Die Kampagne scheint außerdem zusätzliche Mechanismen einzusetzen, um die Wahrscheinlichkeit einer Exposition zu verringern. Verbreitet werden in der Regel Links, die über Weiterleitung zu einem Zielartikel führen. Wer von dort aus die Seite erkunden will, wird unauffällig zur authentischen Vorlagenseite weitergeleitet. Auch das direkte Ansteuern der Landing Page einer gefälschten Seite – etwa spiegel(.)ltd – führt über eine Weiterleitung unauffällig zur echten Seite. Anders verhält es sich bei den eigens erstellten Portalen der Kampagne. Diese präsentieren beim direkten Ansteuern der Domain eine übliche Landing Page mit Artikel- und Themenauswahl.

Mitte Juli 2024 veröffentlichten Qurium (2024) und Correctiv Faktencheck (Bernhard et al., 2024a) umfangreiche Recherchen zur Infrastruktur hinter der Kampagne. Am selben Tag beobachtete der Bayerische Verfassungsschutz ungewöhnliche Aktivitäten in

einem Werbetracking-System der Kampagne: Nach mehreren fehlerhaften, ungewöhnlichen Login-Versuchen sei schließlich das Gesamtsystem gesichert worden. Der Bayerische Verfassungsschutz interpretierte dies als Reaktion auf die Recherchen und führt sie auf Befürchtungen zu möglichen Abschaltungen zurück (BayLfV, 2024). Dienstleister, die für die Kampagne genutzt worden waren, gaben im Nachgang der Veröffentlichungen Serverkündigungen und Kontosperren sowie weitere präventive Maßnahmen bekannt, die sowohl den Weiterleitungsmechanismus als auch die Zielseiten betreffen sollten.

Im Rahmen der Recherchen war mitunter öffentlich geworden, dass die Kampagne auch auf Infrastruktur aus Deutschland zurückgegriffen hat, um ihre prorussischen Inhalte zu verbreiten. Der Bericht mit entsprechenden Details kursierte laut Correctiv bereits im Frühjahr 2024 „unter Regierungsstellen zweier EU-Staaten“ (Bernhard et al. 2024b, Abschnitt 5). In Deutschland habe er dem Auswärtigen Amt und dem Bundesinnenministerium vorgelegen. Rückfragen in Bezug auf mögliche Sanktionsverstöße im Kontext der Kampagne führten laut Correctiv zu Verweisen auf andere verantwortliche Stellen und schließlich beim Zoll zur Absage, „keine Auskünfte zu Einzelfällen zu erteilen“ (Bernhard et al., 2024b, Abschnitt 8).

Obwohl die oben genannten deutschsprachigen Doppelgänger-Websites über Monate hinweg wiederholt dokumentiert wurden und davon ausgegangen werden kann, dass durch die Veröffentlichungen zur technischen Infrastruktur eine Disruption im Betrieb ausgelöst wurde, konnten auch im August 2024 wieder Kampagnenaktivitäten beobachtet werden. Die Verbreitung der Inhalte findet weiterhin nach den bekannten Mustern über Facebook und X statt. Dort sollen die prorussischen Inhalte offenkundig ihr Zielpublikum erreichen: die deutschsprachige Bevölkerung.

Die Verbreitung: Soziale Medien als Amplifikatoren

Zur Verbreitung der prorussischen Doppelgänger-Websites kommen soziale Medien zum Einsatz, wo nicht-authentische Accounts oder Seiten genutzt werden, um die irreführenden Inhalte dem Zielpublikum zuzuführen. Doppelgängeraktivitäten mit deutschsprachiger Zielgruppe konnten 2024 insbesondere auf den Plattformen Facebook und X festgestellt werden. Die Form der Kampagne passt sich dabei den Plattformgegebenheiten und Kommunikationsmöglichkeiten an.

Facebook: Bezahlte Werbung für prorussische Einflussversuche

Die Verbreitung der Inhalte auf Facebook erfolgte 2024 vor allem über bezahlte Werbeanzeigen. Hierfür werden Facebook-Seiten mit generischen Namen angelegt, die dann Anzeigen schalten (Châtelet & Osadchuk, 2024). Von August 2023 bis Ende März 2024 beobachtete die zu Algorithmen arbeitende Nonprofit-Organisation AI Forensics eine prorussische Einflusskampagne mit deutsch- und französischsprachiger Zielgruppe (Bouchaud et al., 2024). In insgesamt 3.826 Anzeigen ging es um die Diskreditierung von Hilfsleistungen gegenüber der Ukraine, die Abwertung der bestehenden Regierungen oder aktuelle Reizthemen. Diese Inhalte sollen pro Tag durchschnittlich über 37.000 deutschsprachige Nutzer:innen erreicht haben. Ende April 2024 eröffnete die EU-Kommission ein formelles Verfahren zur Prüfung der Einhaltung des Digital Services Acts (DSA) gegen Meta.[1] Die irreführende Nutzung von Werbeanzeigen und die Verbreitung von Desinformationskampagnen wurden dabei explizit angeführt (Europäische Kommission, 2024a).

Trotz der Eröffnung dieses Verfahrens konnten auch in den letzten Wochen vor der Wahl zum Europäischen Parlament 2024 weiterhin Anzeigen nach ähnlichem Doppelgänger-Muster beobachtet werden. Das ISD dokumentierte für den Zeitraum vom 26. April bis zum 26. Mai 2024 insgesamt 34 prorussische Anzeigen in deutscher Sprache mit einer Gesamtreichweite von 160.000 Aufrufen (ISD, 2024b). AI Forensics und CheckFirst ergänzten ihren ersten Bericht um weitere 275 prorussische Werbeanzeigen für Mai 2024, davon 75 deutschsprachige Anzeigen mit insgesamt über 400.000 erreichten Nutzer:innen (Bouchaud & Amaury, 2024; Amaury, 2024). Für Juni dokumentierte das internationale Forschungsnetzwerk Counter Disinformation Network (CDN) weitere 98 prorussische Anzeigen (Frühwirth & Nazari, 2024).

1 Der Digital Services Act (DSA) ermöglicht die Regulierung von digitalen Diensten, darunter auch Social Media Plattformen. Wo die EU-Kommission einen Verstoß vermutet, kann sie ein Prüfverfahren eröffnen. Wird eine Verfehlung der Vorgaben festgestellt, können Anpassungen eingefordert werden. Auch hohe Geldbußen sind möglich.

Verschärfte Regelungen zur Schaltung politischer Werbeanzeigen, etwa das Vorlegen eines Ausweisdokuments, die Kennzeichnung der Finanzierungsquelle sowie eine Sperre für Anzeigen in jeweils anderen Ländern, sollen den Missbrauch von Facebook-Werbeanzeigen zur Verbreitung irreführender Inhalte, die der illegitimen ausländischen Einflussnahme dienen, unterbinden (Meta, o. D. b). Allerdings scheint die Umgehung dieser Maßnahmen für Betreiber:innen von Desinformationskampagnen kein Problem darzustellen: AI Forensics und CheckFirst hatten im Januar und Februar 2024 ebenfalls festgestellt, dass knapp 2/3 der EU-weit erfassten Facebook-Werbeanzeigen mit politischen Inhalten initial nicht als solche deklariert worden waren. Eine nachträgliche Einordnung als politisch durch Meta sei nur in 5 % dieser Fälle geschehen. Die erfolgten Entscheidungen werden außerdem als inkonsistent kritisiert, etwa seien ursprünglich nicht als politisch markierte Anzeigen im Rahmen der Moderation als politisch gekennzeichnet worden, ohne dass sie Metas Kategorie dafür erfüllen würden (Bouchaud et al., 2024). Verschärfte Regeln für politische Anzeigen greifen natürlich nicht, wenn die Kennzeichnung als politische Anzeige einfach umgangen werden kann. Auch nach Veröffentlichung dieser Ergebnisse im April 2024 scheint dieses Vorgehen weiterhin funktioniert zu haben. So war von den 98 vom CDN berichteten prorussischen Anzeigen aus dem Monat Juni keine einzige als politische Werbeanzeige gekennzeichnet worden (Frühwirth & Nazari, 2024).

Die aktuell typische Gestaltung der Anzeigen weist außerdem Merkmale auf, die Meta selbst im Mai 2024 als aktuelle Erscheinungsform von Doppelgänger-Content auf Facebook beschrieben hatte: Der Verzicht auf das Teilen von Links sowie die Formulierung der Texte in Algospeak[2] (Franklin et al., 2024a). Meta interpretierte dieses angepasste Vorgehen der Kampagne als Hinweis auf die Wirksamkeit der eigenen Gegenmaßnahmen. Nichtsdestotrotz konnten prorussische Anzeigen weiterhin in dieser Form auf Facebook verbreitet werden.

2 Algospeak bezeichnet eine gezielte Schreibweise bestimmter Begriffe, die in sozialen Medien genutzt wird, um Sperren von Beiträgen mit unerlaubten Themen zu vermeiden (Lorenz, 2022).

X: Veröffentlichung und Amplifikation im großen Stil

Die Verbreitung von Doppelgänger-Inhalten auf X nahm verschiedene Formen an, zeigte sich jedoch wiederholt als arbeitsteiliges Muster mit zwei Accountgruppen: Eine Gruppe veröffentlicht jeweils ein neues Posting, während eine zweite dieses in Form von Antworten unter den Beiträgen Dritter im großen Stil weiterverbreitet. So erreichen die Beiträge trotz weniger Likes und niedriger Follower:innen-Anzahl der Urheber:innen hohe Share-Zahlen im drei-, meist vierstelligen Bereich. Es ist davon auszugehen, dass dieses Vorgehen der Verschleierung der künstlichen Verbreitung dient, da zwar die unter dem Beitrag angezeigte Share-Zahl sichtbar steigt, die dafür verantwortlichen Beiträge aber in der zum Posting gehörenden Share-Übersicht nicht abrufbar sind (InfoEpi Lab., 2024b). Während die veröffentlichenden Accounts nach dem Posten eines Beitrags üblicherweise pausieren, verbreiten die Amplifikationsaccounts mehrere der Originale jeweils mehrfach. Die Beiträge kommen durch dieses Vorgehen auf hohe Viewzahlen, deren Aussagekraft allerdings vorsichtig eingeordnet werden muss.[3]

3 Views spiegeln nicht zwingend die Menge der exponierten Nutzer:innen wider: Sieht ein:e Nutzer:in zwei Beiträge, würde er:sie als zwei Views erfasst. Auch ist anzunehmen, dass die amplifizierenden Accounts ebenfalls in die Views eingehen.

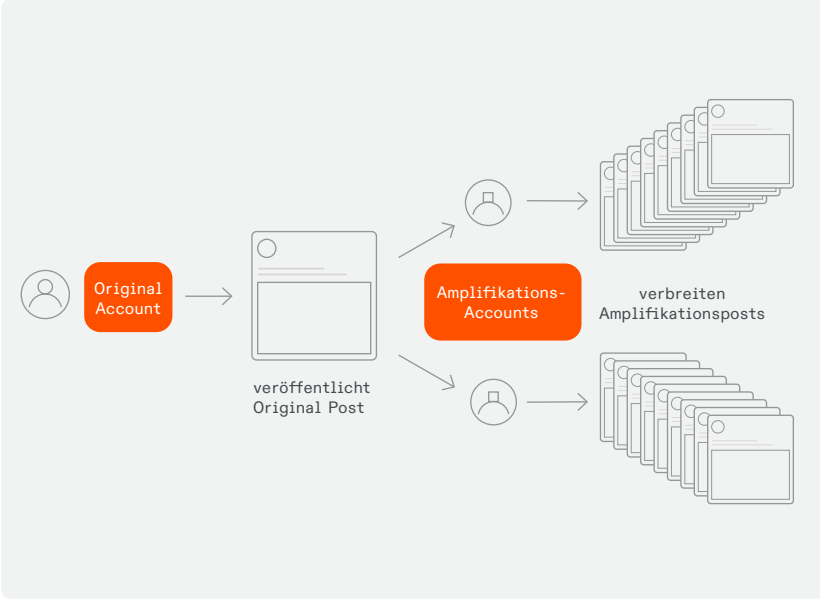


Abbildung 4
Typisches Verbreitungsmuster von Doppelgänger-Postings auf X

Die Beiträge des beschriebenen Musters beinhalteten typischerweise prorussische Aussagen zu aktuellen (gesellschafts-)politischen

Themen, ein Bild sowie einen Link. Letzterer führt entweder über das Doppelgänger-typische Weiterleitungsmuster FIKED[4] (Qurium, 2024) per Umweg zu einer gefälschten oder erfundenen Nachrichtenseite mit prorussischem Inhalt oder zu einem echten Nachrichtenartikel bestehender Medien, der in die gewünschte Erzählung passt (Milenkoski, 2024; BayLfV, 2024). Aktivitäten dieser Art wurden für die erste Jahreshälfte 2024 immer wieder dokumentiert (AA, 2024; Frühwirth & Nazari, 2024; Milenkoski, 2024).

Insgesamt zeigt sich auf X ein umfangreiches Volumen an eingesetzten Ressourcen und Aktivitäten. Über den Jahreswechsel 2023/24 dokumentierte das Auswärtige Amt insgesamt 50.000 aktive Accounts, die für über 1,8 Millionen prorussische Beiträge verantwortlich gewesen sein sollen. Die Frequenz der Beiträge zeigte dabei Hinweise auf eine automatisierte Veröffentlichung (Rosenbach & Schult, 2024). Ein späterer technischer Bericht des Auswärtigen Amts sprach Anfang Juni 2024 von einem Netzwerk „aus hunderttausenden inauthentischen Accounts“ und „Millionen von Posts“. Hier sind augenscheinlich veröffentlichende und amplifizierende Accounts eingerechnet. Auch scheinen Weiterleitungen der Originalbeiträge als eigenständiger Beitrag gewertet zu werden. Den Amplifikationsaccounts, die Originalbeiträge als Antworten weiterverbreiten, attestiert auch dieser Bericht aufgrund eines accountübergreifenden Postingmusters eine automatisierte Vorgehensweise. Weitere beschriebene Kampagnenmuster stützen sich auf die Nutzung von Hashtags sowie die Verbreitung gefälschter Screenshots von Politiker:innen oder Nachrichtenseiten direkt auf X (AA, 2024).

Globale Kampagne im Juni 2024

Die Verbreitung prorussischer Inhalte nach dem oben beschriebenen Muster konnte auch im Juni 2024 auf X beobachtet werden. Wie CeMAS in Kooperation mit dem internationalen Counter Disinformation Network (CDN) zeigen konnte, waren zwischen dem 4. und 28. Juni mindestens 1.366 Accounts zur Veröffentlichung von prorussischen Originalbeiträgen aktiv, die dann von vielen weiteren Amplifikationsaccounts durchschnittlich über eintausendmal weiterverbreitet wurden. Während ebenfalls Inhalte auf französisch, englisch, italienisch, polnisch und ukrainisch dokumentiert werden konnten, stellten die deutschsprachigen Originalbeiträge mit 495 Postings den größten Anteil dar (Frühwirth & Nazari, 2024).

4 Das Akronym steht für „Front Intermediary KEitaro Doppelgänger“ und beschreibt eine Weiterleitung von Nutzer:innen von einer Front-URL über Intermediary URLs und eine URL des Tracking-Dienstes Keitaro zur Doppelgänger-URL (siehe Abbildung 3, Seite 15). Das Vorgehen ermöglicht die Verbreitung der Doppelgängerseiten, ohne diese direkt zu posten und damit Sperren zu riskieren.

Inhaltlich widmeten sich die deutschen Beiträge überwiegend der Kritik an der deutschen Regierung, der Instrumentalisierung aktueller Reizthemen und der Diskreditierung von Unterstützungsleistungen gegenüber der Ukraine. Laut X-Metriken erreichten die deutschsprachigen Beiträge durchschnittlich jeweils 2.284 Views und kamen so insgesamt auf 1.130.918 Views. Antworten Dritter auf die Beiträge legen außerdem nahe, dass die Inhalte nicht im Kreis der Kampagnenaccounts blieben, sondern durchaus ein Mindestmaß an authentischer Aufmerksamkeit erlangen konnten. Unter den 495 Beiträgen konnten 95 entsprechende Antworten dokumentiert werden. Die Untersuchung stützte sich auf das mehrfach dokumentierte Posting-Muster der Kampagne auf X. Wie CeMAS zeigen konnte, war dieser Ansatz so distinkt, dass die Kampagne allein anhand struktureller Beitragsaspekte wie Interaktionszahlen und Inhaltsarten aufgedeckt werden konnte, ohne auf das üblichere Vorgehen über Schlagworte und Schwerpunktthemen angewiesen zu sein.

Neben dem verbreiteten Muster aus Veröffentlichung und Amplifikation zeigten sich weitere abweichende Erscheinungsformen der Kampagne. Spontanere Aktivitäten waren etwa im Nachgang zu salienten Ereignissen von russischem Interesse zu beobachten, beispielsweise nach dem Terroranschlag in Moskau im März (ISD, 2024a; The Insider, 2024a), als Reaktion auf eine russlandkritische Recherche zum Havanna-Syndrom im April/Mai 2024 (The Insider, 2024b) oder in Bezug auf den Ukraine-Friedensgipfel in der Schweiz Mitte Juni 2024, zu dem Russland nicht eingeladen war (Frühwirth & Nazari, 2024). Des Weiteren wurde der Einsatz kostenpflichtig verifizierter Accounts (Reset Tech, 2024), die Verbreitung gefälschter Prominenten-Testimonials sowie das systematische Nutzen von Hashtags beobachtet (Antoniuk, 2024; Bernhard, 2024; InfoEpi Lab., 2024a). Ein französischer Beitrag mit vermutetem Doppelgänger-Bezug fiel durch bezahlte Bewerbung auf X auf (Lehn, 2024). Hinweise zum Entstehungshintergrund der Texte lieferte OpenAI im Mai 2024: Der Betreiber von ChatGPT hatte laut Eigenaussage Doppelgänger-Aktivitäten zur Erstellung von anti-ukrainischem Content im eigenen System bemerkt und daraufhin den entsprechenden Zugriff gesperrt (OpenAI, 2024).

Veränderungen auf X seit Übernahme durch Elon Musk

Ein Grund für den intensiven Einsatz von X zur Verbreitung der Doppelgänger-Inhalte könnte in der reduzierten Resilienz der Plattform gegenüber digitalen Problemphänomenen liegen (Lyndell, 2024). Seit der Übernahme und Umgestaltung durch Elon Musk im Herbst 2022 wurde u.a. Personal in den Bereichen Trust and Safety sowie Contentmoderation abgebaut (Brewster, 2024). Verifikationshaken wurden zum Bezahlprodukt gemacht (Neutsch, 2023), die Sichtbarkeit von Titeln und Quellen aus Vorschaukacheln von Links deutlich reduziert (Herbig, 2023). Beides führt zu einer schlechteren Orientierungsfähigkeit bezüglich der Einschätzung von Authentizität und Vertrauenswürdigkeit von Accounts bzw. Links. Auch die Reaktion der Plattform auf die direkte Meldung von Desinformationskampagnen bleibt hinter den Erwartungen zurück. Über die im Juni 2024 beobachtete prorussische Kampagne mit deutlichen Doppelgänger-Mustern hatten CeMAS und das CDN die Plattform Mitte Juli 2024 unterrichtet. Zu diesem Zeitpunkt waren noch 623 Beiträge online. Über einen Monat nach der Meldung waren davon 622 weiterhin auf der Plattform abrufbar (Frühwirth & Nazari, 2024). Bei einer erneuten Überprüfung am 11. Oktober 2024 waren diese 622 Beiträge weiterhin abrufbar.

Die EU-Kommission hatte gegen X bereits im Dezember 2023 ein Verfahren nach DSA eingeleitet (Europäische Kommission, 2023). Zur Begründung wurden mögliche Verstöße bezüglich der Verbreitung illegaler Inhalte, der Bekämpfung von Informationsmanipulation sowie zum Datenzugriff für Forschende genannt. Die möglicherweise irreführende Praxis der bezahlten Verifikationshäkchen wird ebenfalls angeführt. Während Elon Musk sich angesichts des verstärkten Drucks aus Brüssel unbeeindruckt präsentierte und immer wieder öffentlich mit dem ehemalig zuständigen EU-Kommissar Thierry Bréton stritt (Walsh, 2024), scheint sich an der DSA-Compliance der Plattform seit Eröffnung des Verfahrens wenig getan zu haben. Mitte Juli 2024 konstatierte eine vorläufige Feststellung der EU-Kommission, dass durch die irreführende Praxis der bezahlten Verifikationshäkchen, die verfehlte Transparenz bezüglich der Nachverfolgungsmöglichkeiten von geschalteten Werbeanzeigen auf der Plattform sowie durch das Verfehlen der Vorgaben zum Datenzugang für Forschende die Vorschriften des DSA nicht eingehalten würden. Die Kommission stellte vorläufig fest, dass „das Unternehmen gegen das Gesetz über digitale

Dienste verstößt“ (Europäische Kommission, 2024b, Abschnitt 6). Sollte diese noch vorläufige Einschätzung Bestand haben, sind u.a. empfindliche Bußgelder möglich.

Bekanntes Muster im August weiterhin im Einsatz

Zur Überprüfung des Status Quo auf X untersuchte CeMAS im August 2024, inwiefern die oben beschriebenen Muster auch nach mehrfacher Dokumentation noch genutzt wurden. Zur möglichst breiten Aufdeckung vermuteter latenter Aktivitäten kam dabei wieder der von CeMAS entwickelte, strukturbasierte Suchwinkel ohne Einschränkung auf Schlagwörter oder Narrative zum Einsatz. Trotz der mehrfachen Dokumentation und laufenden Untersuchung durch die EU-Kommission konnte CeMAS auf X weiterhin typische Doppelgänger-Muster feststellen: Zwischen dem 1. und 16. August 2024 konnten 104 deutsche Postings dokumentiert werden, die im ähnlichen Stil prorussische Inhalte verbreiteten. Während die Vorgehensweise bezüglich prorussischer Aussagen und hoher Sharezahlen dem bisher gesehenen Muster entsprach, zeigten sich im Einsatz von Links drei verschiedene Strategien:

Abbildung 5
Unterschiede der Postingmuster im August 2024

28 Beiträge verbreiteten Bilder mit Links nach einem adaptierten FIKED-Schema

19 Beiträge verbreiteten Bilder oder Videos ohne Link

57 Beiträge verbreiteten Links zu echten Artikeln existenter Medienhäuser

Für die Verbreitung echter Nachrichtenartikel wurden Inhalte ausgewählt, die sich mit den Kommunikationszielen Russlands decken. So ging es wiederholt um kritisch lesbare Berichte zur deutschen Bundesregierung, der deutschen Wirtschaft oder der Unterstützung der Ukraine.

Postings ohne Links waren inhaltlich wie handwerklich von niedriger Qualität: Die Grafiken wirken stilistisch wie der Versuch, eine Meme-affine Zielgruppe anzusprechen. Oft gibt es eine Text-Bild-Schere, die Postings wirken daher eher beliebig:

Abbildung 6
Beispiele der Beiträge ohne Links

Abbildung 7
Veränderung des Front-URL Musters Mitte Juli 2024

2024-07-01	[redacted].click/zrz2os
2024-07-01	[redacted].click/897zd7
2024-07-01	[redacted]20.click/h75b77
2024-07-01	[redacted]get31.click/lo5xkb
2024-07-01	[redacted].click/sgz2zg
2024-07-02	[redacted].online/cbbagt
2024-07-05	[redacted]r-oficial.site/sowvz1
2024-07-05	[redacted]hostings.link/el39is
2024-07-05	[redacted]r-oficial.site/fg8nuy
2024-07-05	[redacted].com/m46g48
2024-07-05	[redacted]onyahaber.site/e2wx0u
2024-07-05	[redacted]aswamy.gop/qarzv0
2024-07-05	[redacted]om/if9g4m
2024-07-05	[redacted]om/fqd8w3
2024-07-05	[redacted]nuss.ch/uhdbei
2024-07-05	[redacted]le.group/npb59j
2024-07-05	[redacted]onyahaber.site/5crhhn
2024-07-05	[redacted]onyahaber.site/6zvdk2
2024-07-05	[redacted]online.site/kz4wjb
2024-07-05	[redacted]or-oficial.site/gaw889
2024-07-05	[redacted]rendsus.link/pon27p
2024-07-05	[redacted]maswamy.gop/kzqap3
2024-07-05	[redacted]hostings.link/noi403
2024-07-05	[redacted].com/hqpfk3
2024-07-05	[redacted]le.group/nhvgg1
2024-07-05	[redacted]maswamy.gop/kbl424
2024-07-05	[redacted]rendsus.link/nhmoig
2024-07-05	[redacted]aswamy.gop/4az3wj
2024-07-05	[redacted]onyahaber.site/yw87dd
2024-07-05	[redacted]nuss.ch/g6y5z1
2024-07-05	[redacted]om/r6falh
2024-07-08	[redacted]bosio433.click/38la55
2024-07-08	[redacted]bosio433.click/g7mnie
2024-07-08	[redacted]e115.click/vuitok
2024-07-08	[redacted]ng3.click/uft8qz
2024-07-11	Qurium und Correctiv veröffentlichen Recherchen. Am selben Tag beobachtet der Bayerische Verfassungsschutz Unregelmäßigkeiten auf einem Keitaro-Tracking-Server

Aus Sicherheitsgründen wurden Teile der URLs unkenntlich gemacht.

2024-07-21	[redacted]/0e2a9g
2024-07-21	[redacted]/217vlr
2024-07-21	[redacted]/7jm0gd
2024-07-21	[redacted]/r34c38
2024-07-21	[redacted]/tauamv
2024-07-21	[redacted]/u0ieny
2024-07-21	[redacted]/vfnicn
2024-07-21	[redacted]/w9atu6
2024-07-24	[redacted]Der-Krieg-hat-eine-neue-Frist-erhalten-DER-SPIEGEL
2024-07-27	[redacted]/Harris-ist-gefhrlich-fr-die-deutsche-Industrie-DER-SPIEGEL
2024-07-27	[redacted]/Harris-ist-gefhrlich-fr-die-deutsche-Industrie-DER-SPIEGEL
2024-07-27	[redacted]/Harris-ist-gefhrlich-fr-die-deutsche-Industrie-DER-SPIEGEL
2024-07-27	[redacted]/Harris-ist-gefhrlich-fr-die-deutsche-Industrie-DER-SPIEGEL
2024-07-27	[redacted]/Harris-ist-gefhrlich-fr-die-deutsche-Industrie-DER-SPIEGEL
2024-07-27	[redacted]/Harris-ist-gefhrlich-fr-die-deutsche-Industrie-DER-SPIEGEL
2024-07-27	[redacted]/Harris-ist-gefhrlich-fr-die-deutsche-Industrie-DER-SPIEGEL
2024-07-27	[redacted]/Harris-ist-gefhrlich-fr-die-deutsche-Industrie-DER-SPIEGEL

Beiträge mit Doppelgänger-Links zeigten Hinweise auf eine Veränderung im Verbreitungsmodus. Während zuvor beständig Links im Format *„abcde.domainname.com/abcde“* verbreitet wurden, wurde dieses Muster im Juli 2024 verändert. Bis zum Montag, 8. Juli 2024 zeigten die erfassten Beiträge das alte Muster, am Sonntag, 21. Juli 2024 war eine leichte Variation zu beobachten. Ab Mittwoch, dem 24. Juli wurde augenscheinlich das neue Muster genutzt, die vorherigen kamen danach bis zum Ende des dokumentierten Zeitraums am 16. August 2024 nicht mehr vor. Vor dem Hintergrund der auf Beständigkeit und Wandlungsfähigkeit ausgelegten Doppelgänger-Kampagne ist davon auszugehen, dass es sich hierbei um eine weitere Adaption zur Aufrechterhaltung des Betriebs handelt. Der Zeitpunkt dieser Anpassung legt nahe, dass die Umstellung mit den Recherche-Veröffentlichungen von Qurium und Correctiv Faktencheck am 11. Juli 2024 zusammenhängt. Technische Dienstleister, deren Dienste die Kampagne für ihre Infrastruktur genutzt hatte, hatten nach der Veröffentlichung bekannt gegeben, Server bzw. Konten gesperrt zu haben. Das von CeMAS dokumentierte neue Linkmuster erscheint vor diesem Hintergrund als Kompensationsmaßnahme in Reaktion auf den gestörten technischen Betrieb. Während die vorherigen Front-URLs keine offensichtlichen Hinweise auf die letztlichen Ziel-URLs beinhalteten, bildet das neue Muster nun den Artikeltitel der Zielseite ab.

Die Beiträge wurden jeweils binnen weniger Minuten von verschiedenen Accounts gepostet, was für eine koordinierte und mögliche automatisierte Veröffentlichung spricht. Dabei fällt auf, dass die Muster FIKED-neu und Direktlinks wiederholt zeitgleich genutzt werden, Beiträge ohne Link jedoch nicht zeitgleich mit den anderen Kategorien auftreten. Die parallel auftretenden Muster können dabei Ausdruck von Variationsexperimenten zur Reichweitenmaximierung, der Versuch eines besonders resilienten Vorgehens im Falle von Gegenmaßnahmen oder ein Hinweis auf unterschiedliche beteiligte Akteure sein. Von außen betrachtet ist dies nicht abschließend feststellbar.

Laut X-Metriken erreichten die 104 Beiträge insgesamt 716.126 Views, wobei die verschiedenen Vorgehensweisen unterschiedlich abschnitten. Beiträge ohne Link wiesen durchschnittlich mehr Views auf als die beiden linkbasierten Kategorien, was allerdings erwartbaren Metriken bei X entspricht. CeMAS löste am 9. September 2024 eine Meldung der 104 dokumentierten Beiträge an X aus. Bei einer

erneuten Prüfung am 24. September 2024 konnten 47 Postings weiterhin abgerufen werden. Die übrigen Beiträge waren gelöscht worden, wobei die meisten dazugehörigen Accounts gesperrt (26) oder „vorrübergehend eingeschränkt“ (22) worden waren. In neun Fällen wurden Beiträge gelöscht, ohne sichtbare Konsequenzen für die verantwortlichen Accounts zu veranlassen. Diese verbreiteten im September weiterhin prorussische Inhalte in verschiedenen Sprachen. Bei einer weiteren Überprüfung am 1. Oktober 2024 waren alle Accounts des August-Datensatzes gesperrt.

Kategorie	Anzahl	Views Durchschnitt	Views Summe
Ohne Link	19	9.657	183.482
Echte Artikel	57	6.636	378.272
DG-Artikel	28	5.513	154.372
Gesamt	104	6.886	716.126

Abbildung 8
Überblick der Views nach Beitragskategorie

Nachdem sich die musterbasierte Recherche zur Aufdeckung aktueller Doppelgängerbeiträge auf X wiederholt als wirksam herausgestellt hatte, nutzte CeMAS diesen Ansatz außerdem, um potenzielle ältere Beiträge aufzudecken. Mit dieser retrospektiven Untersuchung konnte CeMAS zeigen, dass entsprechende Inhalte mitunter monatelang auf X stehen geblieben waren. So konnten Anfang Oktober 2024 noch 581 deutschsprachige Beiträge im Doppelgängermuster abgerufen werden, die zwischen Dezember 2023 und April 2024 veröffentlicht worden waren.

Obwohl die beschriebenen Muster von externen Forschenden wiederholt erfasst und an X gemeldet wurden, sodass von einer Kenntnis durch die Plattform ausgegangen werden muss, konnten entsprechende Desinformationsinhalte bis Redaktionsschluss auf der Plattform beobachtet werden. Auch weiter zurückliegende Beiträge bleiben mitunter monatelang online. Während die Sperre der August-Accounts zu begrüßen ist, zeigt die weitere Abrufbarkeit von deutlich früher gemeldeten Juni-Beiträgen und -Accounts die inkonsistenten Eindämmungsbemühungen der Plattform. Auch wird durch zwischenzeitliche Aktivitäten erst später gesperrter

Accounts sichtbar, dass die durch verzögerte Eindämmungsmaßnahmen entstehenden zeitlichen Freiräume die Verbreitung weiterer problematischer Inhalte begünstigen.

Die Strategie: Erkenntnisse aus SDA-Dokumenten

Der Datensatz „Factory of Fakes" – mehrere Tausend geleakte interne Dokumente der für die Doppelgänger-Kampagne verantwortlichen russischen Firma Social Design Agency (SDA), die die Süddeutsche Zeitung und das Online-Nachrichtenmagazin Delfi Estonia erhalten und über die sie als erste berichtet haben (Erb et al., 2024; Laine et al., 2024) – liefert zusätzliche Erkenntnisse über Ziele und Ausführung der Kampagne. CeMAS konnte einen Teil der Dokumente einsehen und unabhängig auswerten.

Der Datensatz bestätigt auf Basis interner Dokumente die bestehende Annahme, dass die Schwächung der Unterstützung für die Ukraine und die Destabilisierung der ukrainischen Verbündeten, insbesondere Deutschlands und Frankreichs, zu den zentralen Zielen der Kampagne gehören. Zu den konkreten Zielvorgaben für Deutschland zählten die Steigerung der Werte der AfD in monatlichen Wahlumfragen auf 20 % und die Förderung von Zukunftsängsten sowie bestimmten Haltungen in der Bevölkerung. So sollten 55 % der Deutschen die Meinung annehmen, den eigenen Wohlstand nicht für den Sieg über Russland aufopfern zu wollen. Auch wurden Werte von 40 % für eine Wahlentscheidung gegen die Grünen angestrebt. Vor der Europawahl 2024 wurde in einem der Dokumente eine Kampagne gegen Parteien der Mitte in Deutschland, Frankreich, Italien, Spanien und Polen vorgeschlagen. Die Stärkung der Fraktion „Identität und Demokratie" von rechtsextremen und rechtspopulistischen Parteien wurde als Möglichkeit dafür gesehen, die Entscheidungen des Europäischen Parlaments in eine prorussische Richtung zu bewegen. Ein weiteres, nach der Europawahl verfasstes Dokument erwähnte, dass die ausgeführte Kampagne rechtsextreme europäische Parteien als „Parteien des Friedens" darstellte und die Vorsitzende der Europäischen Kommission Ursula von der Leyen diskreditierte.

Zugleich veranschaulichen die Dokumente, dass die SDA die Erfolge der Einflusskampagnen gegenüber den Auftraggeber:innen in der russischen Präsidialverwaltung deutlich übertrieb. Die Wahlergebnisse der rechtsextremen Parteien bei der Europawahl wurden in den Dokumenten beispielsweise als direkter Erfolg der

russischen Kampagnen in den sozialen Medien gewertet. Diese irreführende Einschätzung über den Einfluss der Kampagne wurde mit aus dem Kontext gerissenen Zitaten aus einem Medienbericht und Aussagen eines europäischen Politikers über russische Desinformationskampagnen belegt.

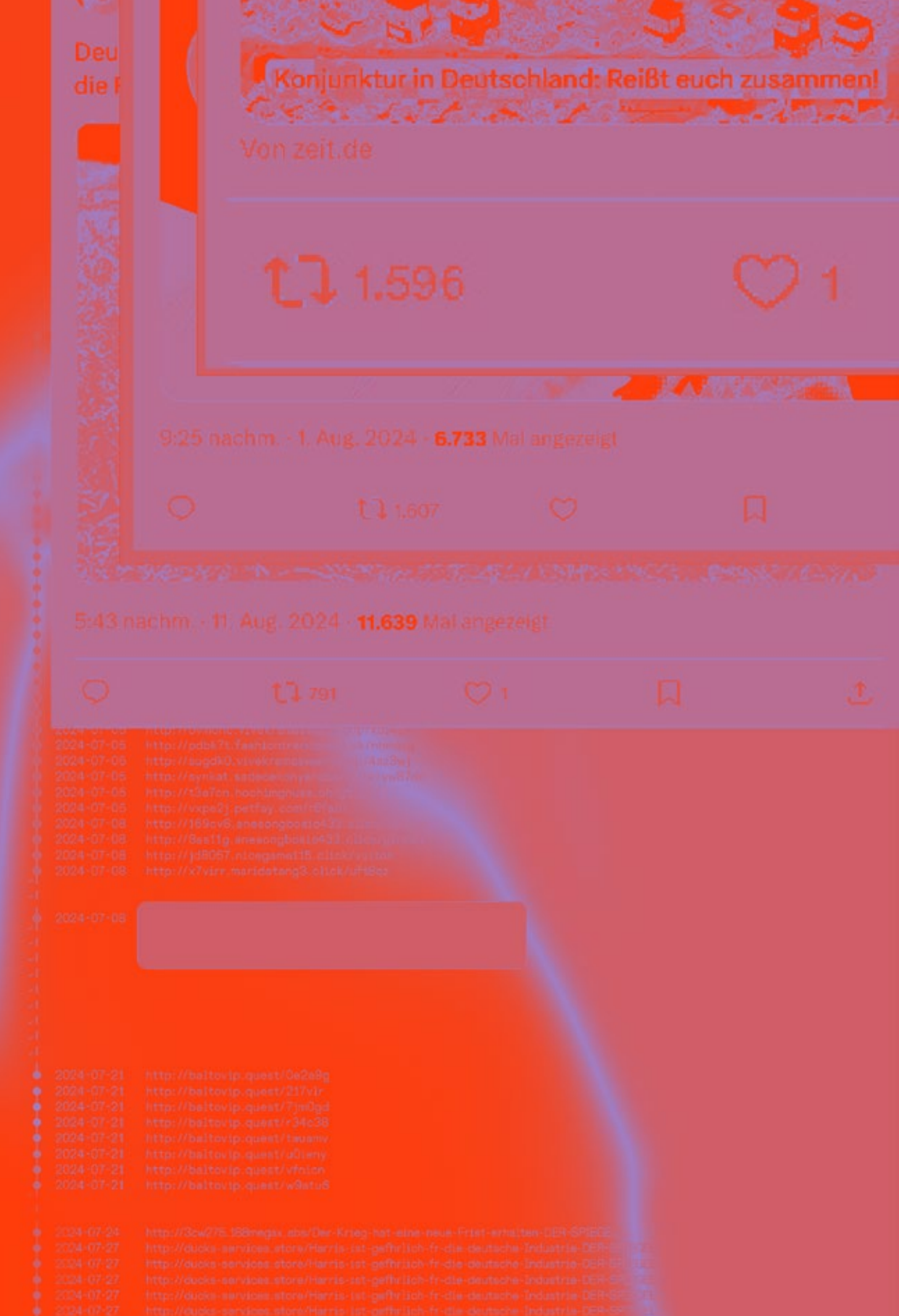
Excel-Tabellen zur Aktivität in Deutschland enthielten Links zu veröffentlichten Posts, Videos und Kommentaren auf Facebook, Instagram, Telegram, TikTok und YouTube sowie Statistiken für Reichweite und Engagement. Eine der Tabellen führte beispielsweise 11.009 Kommentare auf Facebook, Instagram und Telegram für den Zeitraum vom 15. Mai bis zum 2. August 2022 an. Als Reichweite dieser Kommentare wurde eine sehr hohe Zahl von über 165 Millionen Views angegeben, die jedoch offensichtlich irreführend ist. Die Zahl wird als ein Prozent der Gesamtanzahl der Follower:innen von Facebook- und Instagram-Seiten sowie Telegram-Kanälen angegeben, in denen propagandistische Kommentare hinterlassen wurden – als würde jede:r 100. Follower:in automatisch den jeweiligen Kommentar sehen.

Laut den Dokumenten betreibt die SDA ein Monitoring von Medien sowie Umfrageergebnissen in den Zielländern, um Themen für prorussische Inhalte zu identifizieren. Typische Pressespiegel für Deutschland enthielten pro Tag rund 20 Artikel aus überregionalen und regionalen Medien zu Themen wie wirtschaftlichen Sorgen, Protesten gegen Waffenlieferungen an die Ukraine, Sanktionen gegen Russland und anderen Themen, die potenziell für prorussische Propaganda instrumentalisiert werden könnten. Die Dokumente machten außerdem deutlich, dass die SDA westliche Medienberichte und Analysen über die Doppelgänger-Kampagne verfolgte, ins Russische übersetzte und sie instrumentalisierte, um den vermeintlichen Erfolg der Kampagne gegenüber den Auftraggeber:innen zu demonstrieren.

Als Output-Formate werden in den SDA-Dokumenten längere Texte, Social-Media-Posts, Social-Media-Kommentare, Videos, Karikaturen, Memes, Graffiti sowie gefälschte Dokumente und gefälschte Screenshots genannt. Eines der Dokumente enthielt quantitative Vorgaben für die Erstellung der propagandistischen Inhalte für Deutschland und Frankreich: So sollten pro Tag und Land je drei längere Artikel erstellt und mit jeweils zehn Kommentaren versehen werden. Außerdem wurden je zwei Karikaturen, sechs Memes und 20 weitere Social-Media-Kommentare pro Tag und ein

"Fake" pro Woche gefordert. Die Dokumente erwähnen außerdem die Nutzung von bezahlter Werbung auf Facebook als Verbreitungstaktik sowie den Einsatz von Bots und KI-Tools wie ChatGPT und Midjourney.

Insgesamt zeichnen die SDA-Dokumente das Bild einer Kampagne, die unterschiedliche Taktiken erprobt, um Gegenmaßnahmen der Social-Media-Plattformen zu umgehen, die eigene Reichweite zu erhöhen und Desinformations- und Propagandabeiträge in diversen Formaten zu produzieren. Der durch das Leak ermöglichte Einblick in die interne Gestaltung und Ausrichtung der Doppelgänger-Kampagne bestätigt dabei bestehende Annahmen zu ihrer Zielsetzung. Die systematische Auswertung und teils Instrumentalisierung von Forschungsergebnissen stellt dabei einen wichtigen Debattenimpuls zum produktiven und abwägenden Umgang mit der Berichterstattung zu aufgedeckten Desinformationsaktivitäten dar.


Konjunktur in Deutschland: Reißt euch zusammen!
Von zeit.de
1.596
1
9:25 nachm. · 1. Aug. 2024 · 6.733 Mal angezeigt
1.607
5:43 nachm. · 11. Aug. 2024 · 11.639 Mal angezeigt
791
1

33 Trotz bekannter Muster nur begrenzte Eindämmung

Betrachtet man die bisherige Dokumentation zu Doppelgänger, so fallen drei Dinge auf:

- Die Kampagne weist über Monate und Jahre hinweg Konstanten in ihrem Vorgehen auf, die von außen beobachtbar sind.
- Diese Merkmale können sowohl zur Aufdeckung von weiterem Kampagnenmaterial herangezogen werden als auch Ansatzpunkte für Gegenmaßnahmen sein.
- Trotzdem wurde die Kampagne noch nicht effektiv unterbunden.

Von beständigen illegitimen Einflussversuchen autoritärer Staaten auf den gesellschaftlichen Diskurs gehen kurz- und langfristige Risiken für die Gesellschaft aus. Die deutsche Außenministerin Annalena Baerbock nannte im Frühjahr 2024 „Fake-News, Manipulation und gezielte[r] Einflussnahme“ als Mittel, mit denen Wladimir Putin die deutsche Demokratie zersetzen wolle (ZEIT ONLINE, 2024). Das Risikopotenzial des Phänomens ist also deutlich, eine wirksame Eindämmung notwendig. Es sollte ein Zustand angestrebt werden, bei dem die deutsche Bevölkerung nicht mehr von Doppelgänger-Inhalten erreicht wird. Betrachtet man die Kampagne vereinfacht als Kommunikationsprozess, sind für dieses Ziel mehrere Ansatzpunkte denkbar, die für eine Wirkungsmaximierung zusammen gedacht werden sollten. Die Einflussoperation stützt sich auf eine Kombination aus verschiedenen Prozessschritten und bietet in ihrem strukturellen Aufbau vielfältige neuralgische Punkte, wo sie beobachtet, empfindlich gestört und bestenfalls sogar wirkungslos gemacht werden könnte. Die bisher gezeigte Adaptionsbereitschaft ist dabei weniger als Argument gegen Eindämmungsbemühungen zu betrachten, sondern sollte als einzukalkulierender Faktor in der Entwicklungsprognose Eingang finden. Mit Adaptionsbemühungen ist zu rechnen, doch stellen sie jeweils eine temporäre Störung des Kampagnenbetriebs sowie eine Erhöhung ihres Ressourcenbedarfs dar, die das Kosten-Nutzen-Verhältnis des Einflussversuchs schrittweise zu Ungunsten der Betreiber:innen verschieben.

34 Der Weg vom Social-Media-Beitrag zur Doppelgängerseite

Abbildung 9
Exemplarischer Weg von User:innen vom Social-Media-Beitrag zur Doppelgängerseite

Wiederkehrende Muster im Kampagnenverhalten

Die Kampagne erstellt Inhalte auf Websites, die der Zielgruppe zugeführt werden sollen. Aus Nutzer:innensicht begegnet man beispielsweise auf X einem Post, der als Antwort unter einem anderen Beitrag geteilt wurde. Dieser enthält prorussische Inhalte und einen Link, der über eine Weiterleitungskette zu einem Doppelgänger-Artikel auf einer eigenen Website führt. Sind all diese Schritte durchlaufen, wurde ein:e Nutzer:in erfolgreich erreicht. Damit das funktioniert, benötigt die Kampagne neben Personal und Budget aktuell Ressourcen in zwei Bereichen: Websites und Social Media. Zur Bereitstellung der Websites braucht es Hosting, Domains, Software zur Gestaltung und Verwaltung der Seiten sowie Strukturen zur Weiterleitung der Nutzer:innen dorthin. Im Bereich der Verbreitung braucht die Kampagne große Mengen an Accounts auf Facebook und X, die Beiträge posten, sie amplifizieren oder bezahlte Werbung schalten, die dann der Zielgruppe angezeigt werden. Wenn diese Faktoren erfüllt sind, ist die Kampagne grundsätzlich in der Lage, irreführende Inhalte zu veröffentlichen und zu verbreiten, und damit potenziell die deutsche Bevölkerung zu erreichen. Diese Kette gilt es zu unterbrechen.

Zur Identifikation von Aktivitäten können bekannte Konstanten genutzt werden:

Domains

- Die Anzahl der Zielportale erscheint überschaubar, wenn auch mit mehreren Domain-Endungen gerechnet werden muss.
- Dokumentationen von neu erstellten Domains zeigen eine Tendenz, mehrere Domains auf einmal zu registrieren sowie eine Fokussierung der Namen auf bestimmte semantische Räume. Typisch sind Namen bekannter Medien, Begriffe, die neue Nachrichten- oder Medienseiten suggerieren sollen, aber auch solche, die nach kritischen Kommentaren zum Zeitgeschehen klingen (Europäischer Auswärtiger Dienst, 2024; Nimmo & Agranovich, 2022; Nimmo et al., 2023).
- Technische Konstanten zeigen sich in Form von Mehrfachnutzung von IP-Adressen, Hostern und Servern oder Performance-Tracking-Diensten (Chavane et al., 2024; Harfanglab, 2024; Recorded Future, 2023; VIGINUM, 2023). Außerdem wurden bei Verschlüsselungs-Zertifikaten zeitliche Parallelen beobachtet (Harfanglab, 2024).
- Die Weiterleitung erfolgt nach einem systematischen Muster aus Front-URL, Intermediary-URL und Doppelgänger-URL (FIKED) (Qurium, 2024).
- Laut FBI wurden die Doppelgänger-Domains von US-Unternehmen Namecheap, NameSilo und GoDaddy gemietet, mit Hilfe von Online-Personen mit erfundenen Namen. Die Akteur:innen verwendeten VPS-Dienste (Virtual Private Servers) und zahlten in Kryptowährungen, um die Verbindungen zu Russland zu verschleiern. Die verwendeten VPS-Dienste und IP-Adressen stehen in Verbindung zu kriminellen Cyber-Akter:innen, die Zugang zu kompromittierten IP-Adressen verkaufen, um Anonymität zu ermöglichen (US Department of Justice, 2024).

Social Media

- CeMAS konnte zeigen, dass das typische Beitragsmuster auf X so distinkt ist, dass es als strukturelle Recherchevorlage genutzt werden kann, ohne auf Keywords angewiesen zu sein (Frühwirth & Nazari, 2024).
- Aktuelle Muster zur Verwendung von Werbeanzeigen auf Facebook sind ebenfalls bekannt. Sie stammen in der Regel von eigens angelegten Facebook-Seiten mit generischen Namen (Châtelet & Osadchuk, 2024), werden trotz politischen Inhalts nicht als politische Werbeanzeigen deklariert (Bouchaud et al., 2024) und greifen auf Algospeak zurück (Franklin et al., 2024).
- Es gibt Grund zur Annahme, dass binnen weniger Tage nach einem Ereignis von russischem Interesse mit spontaneren Aktivitäten zu rechnen ist (Frühwirth & Nazari, 2024; ISD, 2024a; The Insider, 2024a; The Insider, 2024b). Die Akteur:innen hinter der Kampagne betreiben Monitoring von Medien in den Zielländern und entwickeln Inhalte, die auf echte Ereignisse Bezug nehmen (Blum et al, 2024).

Potenziale für Identifikation und Eindämmung

Diese Beobachtungen lassen sich für Recherchen zur Kampagne nutzen. Im Bereich Domains sollten die wiederholt beobachteten Server, Dienste, Domainnamen und Weiterleitungsketten als Ausgangspunkt für die kontinuierliche Aufdeckung von Aktivitäten herangezogen werden. Konkret könnte das neue Front-URL Muster genutzt werden, um ausgehend von bekannten Doppelgänger-Portalen nach Front-Domains mit passenden Artikeltiteln zu suchen. Auch die bekannte Weiterleitungsverkettung bietet Möglichkeiten, von einer bekannten URL vor- oder nachgeschaltete Internetadressen aufzudecken. Im Bereich der Kampagnenverbreitung in sozialen Medien hat CeMAS gezeigt, dass die bekannten Postingmuster themenunabhängig genutzt werden können, um die Kenntnis bisher erfolgter Aktivitäten zu vervollständigen und neu auftretende Beitragswellen in Echtzeit zu identifizieren. Die entdeckten Datenpunkte aus dem Bereich Verbreitung können verwendet werden, um weitere Aspekte des Domainbereichs aufzudecken und umgekehrt. Gegen gefälschte Domainnamen sind außerdem rechtliche Schritte möglich (Buchmann, 2023; Lothian, 2022; UDRP disputes, 2023).

Neben der Identifikation von Aktivitäten sind die dokumentierten Konstanten außerdem einsetzbar, um die Kampagne einzudämmen. Ansatzpunkte zur Störung der Infrastruktur im Domainbereich bietet der Sanktionsstatus der Firmen hinter der Kampagne (Council of the European Union, 2023; U.S. Department of The Treasury, 2024). Die Abhängigkeit der Operation von bestimmten Software-Dienstleistern könnte ein weiterer Ansatzpunkt sein. Diese über die Kampagnenaktivitäten in Kenntnis zu setzen, kann dazu führen, dass Zugänge und Konten gesperrt werden. Die potenzielle Wirksamkeit solcher Maßnahmen war im Juli 2024 beobachtbar (Bernhard et al., 2024c). Im Bereich der sozialen Medien sollten bekannte Muster sowohl retrospektiv als auch fortschreitend und in Echtzeit gemonitort werden, damit irreführende Inhalte gelöscht und verantwortliche Accounts gesperrt werden können.

Die Lücke zwischen Ist- und Sollzustand

Während die Doppelgänger-Aktivität vielfältige Ansatzpunkte zu ihrer kontinuierlichen Beobachtung und möglichen Eindämmung bietet, stellt sich die Frage, warum sie dennoch weiterhin aktiv sein kann. Sowohl staatliche Institutionen als auch Plattformbetreiber berichten immer wieder von den eigenen Maßnahmen gegen Desinformationskampagnen und andere Formen illegitimer Einflussnahme. Dass diese Maßnahmen unabhängig von ihrem Umfang bisher nicht ausreichend sind, um unerwünschte Aktivitäten einzudämmen, ist dabei evident. Ausschlaggebend ist letztlich nicht der investierte Aufwand, sondern das Gesamtergebnis. Bleibt zu viel manipulative Aktivität übrig, sind auch die daraus hervorgehenden gesellschaftlichen Risiken nicht gebannt.

Da die beteiligten Akteur:innen vielfältige Handlungsoptionen haben, stellt sich die Frage, inwieweit das Problem priorisiert wird. Werden kontinuierliche, proaktive und ausreichend ausgestattete Ermittlungen zur Identifikation von Doppelgänger-Aktivitäten durchgeführt? Werden diese und ähnliche Kampagnen als beständiger Bedrohungsfaktor verstanden, proaktiv untersucht und wird auch ihre konstante Adaptionstendenz einkalkuliert? Wie wird mit externen Hinweisen auf identifizierte Kampagnenaktivität umgegangen? Wird die Bewertung der eigenen Aktivitäten am Ressourceneinsatz bemessen oder am Problemstatus?


DSA

Fazit und Handlungsempfehlungen

Desinformation als komplexen Kommunikationsprozess verstehen und eindämmen

Um der Wirkungsfähigkeit der Doppelgänger-Kampagne umfassend begegnen zu können, braucht es einen integrierten Blick auf die Komplexität von Desinformationskampagnen. Relevant sind hierbei die Aspekte Information, Technologie, Sicherheit, Demokratie und Sozialwissenschaft. Desinformationskampagnen können dabei als Kommunikationsprozess verstanden werden, der zwischen Sender und Empfänger mehrere Schritte durchläuft, bei denen er beobachtet und gestört werden kann. Dafür werden jeweils die Ressourcen unterschiedlicher Akteur:innen benötigt. Für eine Wirkungsmaximierung sollten diese zeitnah, koordiniert und kombiniert eingesetzt werden (Lamberty & Frühwirth, 2023).

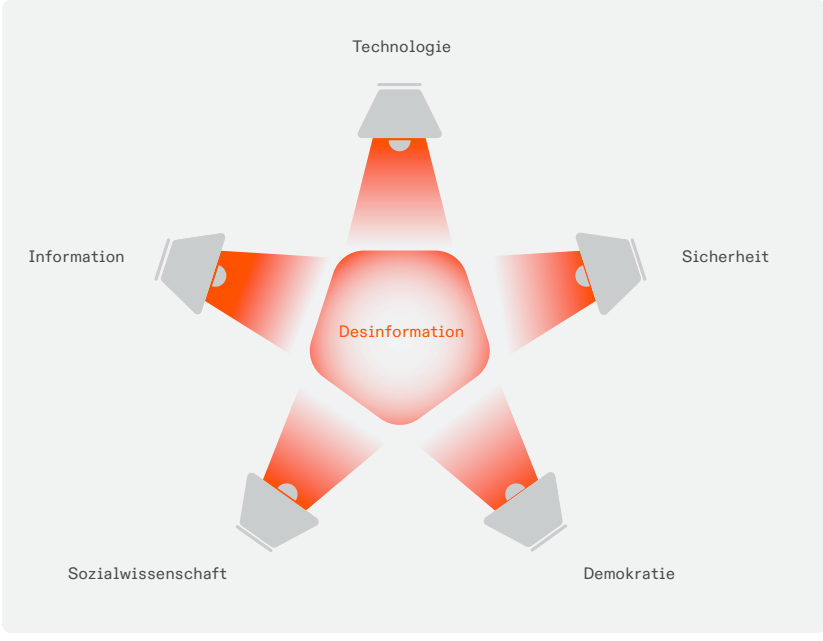


Abbildung 10
Integratives Modell zum Umgang mit Desinformation

Staatliche Akteure müssen bestehende Sanktionen konsequent durchsetzen

Staatliche Stellen sollten den Sanktionsstatus der Doppelgänger-Betreiber (Council of the European Union, 2023; U.S. Department of The Treasury, 2024) nutzen, um die erreichbare Infrastruktur zu

Abbildung 11
Desinformation als Kommunikationsprozess

entziehen. Wie wirksam das sein kann, zeigte sich Mitte Juli 2024: Die Kampagne musste sich wochenlang umstellen und wurde sichtbar gebremst (Bernhard et al., 2024c). Dass sich mithilfe der in Deutschland befindlichen Infrastruktur darüber hinaus wertvolle Erkenntnisse über die interne Funktionsweise der Kampagne generieren lassen, zeigte außerdem der Bayerische Verfassungsschutz (2024). Wo Infrastruktur aus Deutschland heraus nicht abgeschaltet werden kann, sollten zudem Maßnahmen zu deren Zugänglichkeit geprüft werden. Domains wie spiegel(.)ltd oder welt(.)pm verbreiten inzwischen seit Jahren irreführende Inhalte an die deutsche Bevölkerung, obwohl ihre Betreiber eigentlich unter Sanktionen stehen. Was die Verbreitung betrifft, so sollten staatliche Stellen die Betreiber der Social-Media-Plattformen in die Pflicht nehmen. Der DSA führt sowohl Facebook als auch X als sogenannte VLOPs, also sehr große Online-Plattformen, für die besondere Sorgfaltspflichten gelten – beispielsweise in Hinblick auf systemische Risiken, die durch die Beschaffenheit der Plattformen verschärft werden können (Europäische Kommission, o. D.). Gegen beide wurden bereits Verfahren zur Prüfung möglicher Verstöße eröffnet (Europäische Kommission, 2023; Europäische Kommission, 2024a). Es sollte im Interesse staatlicher Akteure sein, Aktivitäten illegitimer prorussischer Einflussnahme in Echtzeit zu erfassen, den Plattformen zu melden und eine sorgfältige Bearbeitung einzufordern. Wo immer diese nicht erfolgt, sollte das an die Bundesnetzagentur als deutschem Digital Services Coordinator und/oder die EU-Kommission gemeldet werden, um die Durchsetzung des DSA als Regulierungsinstrument zu unterstützen.

Wo Plattformen ihrer Verantwortung nicht gerecht werden, muss Regulierung für Handlungsanreize sorgen. Regulierende

Akteure müssen dabei der Herausforderung gerecht werden, mit der Handlungsgeschwindigkeit der Problem-Akteure mitzuhalten.

Wirksame Eindämmungsbemühungen sind auf schnelle, gezielte und koordinierte Gegenmaßnahmen angewiesen. Dafür braucht es eine angemessene Priorisierung des Themas, die sich in einer ausreichenden Ausstattung mit finanziellen und personellen Ressourcen sowie effizienten Prozessen und wirksamer, vertrauensvoller Vernetzung aller benötigten Akteure ausdrückt. Ergänzend sollte ein beständiges Monitoring zu staatlichen Webpräsenzen erfolgen. Denn während der Schwerpunkt der gefälschten Seiten der Kampagne bisher auf Medienplagiaten liegt, sind auch immer wieder kopierte Regierungsseiten berichtet worden (Bernhard, 2023). Staatliche Institutionen sollten im Eigeninteresse deshalb regelmäßig überprüfen, ob Plagiate ihrer Webpräsenzen im Umlauf sind und diese frühzeitig unterbinden.

Plattformbetreiber müssen die Verbreitung auf sozialen Medien unterbinden

Da Social-Media-Plattformen der Ort sind, wo die Inhalte ihrer Zielgruppe zugeführt werden sollen, müssen die Plattformbetreiber handeln. Die konstante Dokumentation der Vorgehensweise von Doppelgänger ermöglicht den Plattformen ein internes Monitoring entsprechender Aktivitäten. Einerseits sollten entsprechende Erkenntnisse genutzt werden, um retrospektiv noch abrufbare Inhalte zu löschen und die dazugehörigen Accounts zu sperren, andererseits ist ein kontinuierliches Echtzeit-Monitoring nötig. Wo Forschende wie CeMAS von außen in der Lage sind, mit auf Erfahrungswerten basierender Mustererkennung neue Aktivitäten aufzudecken, sind Plattformbetreiber das auch. Die ihnen darüber hinaus zusätzlich zur Verfügung stehenden Daten sollten dabei als weitere Hinweisquellen auf das auf ihren Plattformen ohnehin untersagte unauthentische, koordinierte Verhalten dienen (Meta, o. D. a; X Hilfe-Center, 2023). Interne Ermittlungen zur Eindämmung von illegitimen Einflusskampagnen sollten dabei nicht reaktiv erfolgen, sondern proaktiv und kontinuierlich umgesetzt und dem sich entwickelnden Vorgehen angepasst werden. Darüber hinaus sollten Erkenntnisse zu entsprechenden Kampagnen, die extern an Betreiber herangetragen werden, zeitnah sorgfältig geprüft und in Löschungen und Sperrungen umgesetzt werden. Eine Rückmeldung über die getroffene Entscheidung an die Meldenden sollte

auch in diesen Fällen erfolgen, analog zu den Rückmeldevorgaben des DSA über das interne Meldesystem (Verbraucherzentrale, 2024). Zur Eindämmung des Problems sollten externe Forschende mittels Datenzugriff befähigt werden, Aktivitäten frühzeitig und umfassend erfassen zu können. Nutzerunfreundliche Zugriffsinstrumente wie X' Werbebibliothek werden zurecht von der EU-Kommission kritisiert, da sie den Anschein von Transparenz erwecken, praktisch aber nicht einsetzbar sind (Europäische Kommission, 2024b).

Auf Facebook ist der Zugang zur Verbreitung von politischer Werbung über als nicht-politisch gekennzeichnete Werbeanzeigen einzuschränken. Die verschärften Regelungen für politische Werbung verfehlen jegliche Wirkung, wenn Desinformationskampagnen problemlos daran vorbei veröffentlicht werden können. Hier ist die Plattform in der Pflicht, die Kategorisierung von Werbung als politisch nicht allein den Urheber:innen zu überlassen. Darüber hinaus sollte die massenhafte Registrierung nicht-authentischer Accounts und Seiten erschwert werden – insbesondere dort, wo diese zur Schaltung von Werbeanzeigen zum Einsatz kommen. Außerdem wäre die technische Machbarkeit von erweiterten Content-Blockierungen auf Basis der Ziel-URLs zu prüfen: Laut Meta hatte das Blockieren bekannter Doppelgänger-Domains dazu geführt, dass die Kampagne ihre Vorgehensweise auf Facebook anpassen musste und zeitweise ganz auf Links verzichtete (Franklin et al., 2024). Auf X wurden zwar noch Links gepostet, allerdings über das bereits erwähnte Weiterleitungsschema. Hierbei variieren zwar die konkreten URLs im Beitrag, diese führen über technisch erfassbare Redirects aber zu bereits bekannten Domains. Die Plattformen sollten diese abrufbaren Daten nach Möglichkeit nutzen, um auch das Redirect-Pattern trockenzulegen.

Forschung und Zivilgesellschaft

Die möglichst tiefgreifende und kontinuierliche Kenntnis des aktuellen Modus Operandi der Kampagne ist die Grundlage, auf der die Bewertungen und Gegenmaßnahmen aufsetzen. Dementsprechend sind beständige Forschungsbemühungen zu Erkenntnissen über die Entwicklung der Kampagne zentral. Neben einem Monitoring bereits dokumentierter Muster sollten außerdem mögliche neue Vorgehensweisen antizipiert und überprüft werden. Vor dem Hintergrund der konstanten Wandlungsfähigkeit der Kampagne braucht es zudem innovative und experimentelle Recherchewinkel. Die Bandbreite an technischen Indikatoren ist durch den starken Kampagnenfokus auf Domainportale groß und sollte genutzt werden. Ziel sollte es sein, mit der dynamischen Manifestation des latenten Desinformationsbestrebens nicht nur Schritt zu halten, sondern die potenziell schädliche Kommunikation möglichst früh zu entdecken. Zur Erweiterung des Sichtfelds bieten sich ergänzende Suchwinkel an, die sich auf die strukturellen Muster der Beiträge stützen, ohne durch die Nutzung von Keywords auf Basis bereits bekannter Schwerpunktthemen das eigene Sichtfeld einzuschränken. Wie CeMAS erfolgreich zeigen konnte, bietet dieser Ansatz vielversprechendes Potenzial für künftige Forschungsbemühungen. Letztlich sollten neben den bisher bezüglich Doppelgänger stärker beleuchteten Plattformen auch andere Orte des digitalen Austauschs in den Blick genommen werden, wie insbesondere durch die im SDA-Leak zusätzlich genannten sozialen Netzwerke verdeutlicht wurde. Neben Plattformen, zu denen bereits konkrete Hinweise vorliegen, sollten auch weitere verbreitete Dienste überprüft werden. Auch wenn beispielsweise auf LinkedIn bisher weniger mit Doppelgänger-Content gerechnet wird, sollte diese Einschätzung in Antizipation möglicher Vorgehensadaptionen auf regelmäßigen Tests basieren.

Forschende im Bereich Desinformation sollten zur Synergiebildung Kooperationen und Wissensaustausch ausweiten. Berichte zu aufgedeckten Aktivitäten sollten standardmäßig um Aufstellungen von gefundenen Assets wie Kampagnen-Accounts und -Websites ergänzt werden – die im Rahmen dieses Reports dokumentierten Assets sind zum Beispiel über die Open Science Foundation (OSF) einsehbar. Eine zentrale Sammlung von zugeordneten Kampagnen-Ressourcen würde darüber hinaus so manchen Forschungsprozess beschleunigen. Rechercheergebnisse sollten

systematisch aufbereitet und den Plattformen sowie den betroffenen Staaten als auch der EU-Kommission bereitgestellt werden. So können sich Forschungsinteressen und Regulierungsbemühungen zur Verbesserung der Lage systematisch ergänzen. Zuletzt können die von der Kampagne genutzten Dienste auch seitens zivilgesellschaftlicher Akteur:innen für ein Deplatforming angesprochen werden. Wo die Kampagne systematisch nur auf einen Dienst setzt, macht sie ihr Vorgehen auch von dessen Zugang abhängig.

Für den Zeitraum 1. bis 16. August 2024 wurden über Meltwater Social Listening deutschsprachige Beiträge auf X erfasst, die über 300 Shares und unter 100 Likes aufwiesen, von Accounts mit unter 100 Followern stammten und einen Link enthielten. Dies ergab einen Datensatz von 104 X-Postings, von denen am 6. September 2024 noch 78 abrufbar waren. Die Weiterleitungskette der Beiträge mit Doppelgänger-Links wurde über urlscan.io aufgeschlüsselt und dokumentiert. Alle Beiträge und Zielseiten wurden archiviert. Am 9. September 2024 wurde dieser Datensatz u.a. an X gemeldet. Am 24. September 2024 waren 47 Postings weiterhin abrufbar, am 1. Oktober 2024 waren die Accounts gesperrt.

Ergänzend wurden rückblickend außerdem Beiträge nach gleichem Muster für Juli 2024 über Meltwater abgerufen. Ein zusätzlicher Datensatz mit 666 Beiträgen mit demselben Muster im retrospektiv betrachteten Zeitraum November 2023 bis April 2024 wurde am 21. August 2024 über Meltwater abgerufen. Hiervon waren am 1. Oktober 2024 noch 581 Beiträge online.

kzweckszweck

2024-07-01 http://
2024-07-01 http://
2024-07-01 http://
2024-07-01 http://
2024-07-02 http://
2024-07-05 http://
2024-07-05 http://
2024-07-05 http://
2024-07-05 http://
2024-07-05 http://
2024-07-05 http://
2024-07-05 http://
2024-07-05 http://
2024-07-05 http://
2024-07-05 http://
2024-07-05 http://
2024-07-05 http://
2024-07-05 http://
2024-07-05 http://
2024-07-05 http://
2024-07-05 http://
2024-07-05 http://
2024-07-05 http://
2024-07-05 http://
2024-07-05 http://
2024-07-05 http://
2024-07-08 http://
2024-07-08 http://
2024-07-08 http://
2024-07-08 http://
2024-07-08

2024-07-21 http://
2024-07-21 http://
2024-07-21 http://
2024-07-21 http://
2024-07-21 http://
2024-07-21 http://
2024-07-21 http://
2024-07-21 http://

2024-07-24 http://
2024-07-27 http://
2024-07-27 http://
2024-07-27 http://
2024-07-27 http://
2024-07-27 http://

Literaturverzeichnis

Alaphilippe, A., Machado, G., Miguel, R., Poldi, F. (2022, 27. September). Doppelganger – Media clones serving Russian propaganda. EU DisinfoLab. https://www.disinfo.eu/doppelganger/

Aleksejeva, N., Osadchuk, R., Gelava, S., Le Roux, J., Caniglia, M., Suárez Pérez, D., Kann, A. (2022, 27. September). Russia-based Facebook operation targeted Europe with anti-Ukraine messaging. Network uncovered by the DFRLab promoted Kremlin narratives in Germany, France, Italy, Ukraine, Latvia and the UK. Medium. https://medium.com/dfrlab/russia-based-facebook-operation-targeted-europe-with-anti-ukraine-messaging-389e32324d4b

Amaury, L. (2024, 30. Mai). Unchecked political ads: A surge of pro-Russian propaganda on Meta's platforms ahead of EU elections. CheckFirst. https://checkfirst.network/unchecked-political-ads-a-surge-of-pro-russian-propaganda-on-metas-platforms-ahead-of-eu-elections/

Antoniuk, D. (2024, 17. Juni). Fake anti-Ukraine celebrity quotes recently surged on social media. The Record. https://therecord.media/fake-celebrity-quotes-anti-ukraine-doppelganger-bot-blocker

Auswärtiges Amt (AA). (2024). Deutschland im Fokus der pro-russischen Desinformationskampagne „Doppelgänger". https://www.auswaertiges-amt.de/blob/2660362/73bcc0184167b438173e554ba2be2636/technischer-bericht-desinformations-kampagne-doppelgaenger-data.pdf

Bayrisches Landesamt für Verfassungsschutz (BayLfV). (2024). „Doppelgänger". Interne Details zu russischer Desinformationskampagne. https://www.verfassungsschutz.bayern.de/mam/anlagen/baylfv_vollanalyse_doppelgaenger.pdf

Bernhard, M. (2023, 23. Juni). Fake-Regierungsseiten, Drogen-Selenskyj, AfD-Politiker: Prorussische Desinfo-Kampagne wütet weiter auf Facebook. https://correctiv.org/faktencheck/hintergrund/2023/06/23/russland-desinformation-kampagne-auf-facebook-gegen-ukraine-selenskyj-und-fuer-afd-politiker/

Bernhard, M. (2024, 30. April). Äußerte sich Til Schweiger zu Korruption in der Ukraine? Hinweise deuten auf Kreml-Kampagne. https://correctiv.org/faktencheck/2024/04/30/aeusserte-sich-til-schweiger-zu-korruption-in-der-ukraine-hinweise-deuten-auf-kreml-kampagne/

Bernhard, M., Hock, A., Thust, S. (2024a, 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/

Bernhard, M., Hock, A., Thust S. (2024b, 11. Juli). Russische Propaganda: Bundesregierung ignoriert Hinweise auf Spuren in Deutschland. https://correctiv.org/faktencheck/russische-desinformation/2024/07/11/russland-propaganda-doppelgaenger-bundesregierung-ignoriert-hinweise-auf-spuren-in-deutschland/

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/

Blum, P., Flade, F., Milling, P., Riedel, K., Zöller, L., Bewarder, M., Pittelkow, S. (2024, 16. September). Desinformations-Leak. Tiefe Einblicke in Putins Lügenmaschine. https://www.tagesschau.de/investigativ/ndr-wdr/russland-propaganda-fakenews-sda-deutschland-100.html

Bouchaud, P., Amaury, L. (2024). Supporting Evidence: Pro-Russian ads campaigns approved by Meta from May 1 to May 27, 2024 in Italy, Germany, France & Poland. AI Forensics. https://cmsbackend.aiforensics.org/uploads/Meta_Ads_Follow_up_27_May_24_46d87a3953.pdf

Bouchaud, P., Faddoul, M., Buse Çetin, R. (2024). No embargo in sight. Meta lets pro-Russia propaganda ads flood the EU. AI Forensics. https://aiforensics.org/uploads/No_Embargo_in_Sight_AI_Forensics_Report_ad7ede416b.pdf

Brewster, T. (2024, 10. Januar). Musk's X fired 80 % of engineers working on trust and safety, Australian government says. Forbes. https://www.forbes.com/sites/thomasbrewster/2024/01/10/elon-musk-fired-80-per-cent-of-twitter-x-engineers-working-on-trust-and-safety/

Buchmann, L.-B. (2023, 2. Oktober). Décision de la commission administrative. Etat français contre Zhao Xiaotian. Litige No. DFM2023 – 0001. Organisation Mondiale de la Propriété Intellectuelle. https://www.wipo.int/amc/en/domains/decisions/pdf/2023/dfm2023-0001.pdf

Chavane, C., G., A., Seznec, K. (2024, 21. Mai). Master of Puppets: Uncovering the DoppelGänger pro-Russian influence campaign.

Sekoia TDR. https://blog.sekoia.io/master-of-puppets-uncovering-the-doppelganger-pro-russian-influence-campaign/

Châtelet, V., Osadchuk, R. (2024, 12. März). Doppelganger targets Ukrainian and French audiences via Facebook ads. DFRLab. https://dfrlab.org/2024/03/12/doppelganger-operation-targets-ukraine/

ClearSky Cyber Security. (2024). Doppelgänger NG. Cyberwarfare campaign. https://www.clearskysec.com/wp-content/uploads/2024/02/DoppelgangerNG_ClearSky.pdf

Council of the European Union. (2023, 28. Juli). Information manipulation in Russia's war of aggression against Ukraine: EU lists seven individuals and five entities. https://www.consilium.europa.eu/en/press/press-releases/2023/07/28/information-manipulation-in-russia-s-war-of-aggression-against-ukraine-eu-lists-seven-individuals-and-five-entities/

Erb, S., Salem S., Schmitt J., Verschwele L., Weinmann L. (2024, 16. September). Propaganda vom Fließband. Süddeutsche Zeitung. https://www.sueddeutsche.de/projekte/artikel/politik/russland-propaganda-desinformation-social-design-agency-ilja-gambaschidse-sofia-sacharowa-facebook-telegram-memes-karikaturen-putin-ukraine-krieg-in-der-ukraine-e843184/

Europäische Kommission. (o. D.). DSA: Sehr große Online-Plattformen und Suchmaschinen. https://digital-strategy.ec.europa.eu/de/policies/dsa-vlops

Europäische Kommission. (2023, 18. Dezember). Kommission leitet im Rahmen des Gesetzes über digitale Dienste ein förmliches Verfahren gegen X ein. https://ec.europa.eu/commission/presscorner/detail/de/ip_23_6709

Europäische Kommission. (2024a, 30. April). Kommission leitet förmliches Verfahren gegen Facebook und Instagram im Rahmen des Gesetzes über digitale Dienste ein. https://ec.europa.eu/commission/presscorner/detail/de/ip_24_2373

Europäische Kommission. (2024b, 12. Juli). Kommission übermittelt X vorläufige Feststellungen wegen Verstoßes gegen Gesetz über digitale Dienste. https://ec.europa.eu/commission/presscorner/detail/de/IP_24_3761

Europäischer Auswärtiger Dienst (2024, Juni). Doppelganger strikes back: FIMI activities in the context of the EE24. EAD. https://euvsdisinfo.eu/uploads/2024/06/EEAS-TechnicalReport-DoppelgangerEE24_June2024.pdf

Franklin, M., Hundley, L., Torrey, M., Agranovich, D., Dvilyanski, M. (2024a). Adversarial Threat Report. Meta. https://transparency.fb.com/sr/Q1-2024-Adversarial-threat-report

Franklin, M. Torrey, M. Agranovich, D. & Dvilyanski, M. (2024b). Adversarial Threat Report. https://transparency.fb.com/sr/Q2-2024-Adversarial-threat-report

Frühwirth, L., Nazari, S. (Hrsg.) (2024). Fool me once. Russian influence operation Doppelganger continues on X and Facebook. https://alliance4europe.eu/wp-content/uploads/2024/09/CDN-Report---Fool-Me-Once_-Russian-Influence-Operation-Doppelganger-Continues-on-X-and-Facebook---September-2024.pdf

Harfanglab (2024, 25. Juli). Mid-year Doppelgänger information operations in Europe and the US. Harfanglab. https://harfanglab.io/insidethelab/doppelganger-operations-europe-us/

Herbig, D. (2023, 5. Oktober). X zeigt keine Headlines mehr – „bessere Ästhetik". Heise online. https://www.heise.de/news/Twitter-X-zeigt-bei-Links-keine-Headlines-mehr-an-nur-noch-Bilder-9325705.html

InfoEpi Lab. (2024a). Lost in distranslation: Voiceovers on celebrity videos used to launder pro-Kremlin claims. https://infoepi.org/posts/2024/04/19-lost-in-distranslation.html

InfoEpi Lab. (2024b). How Doppelgänger hides ist engagement. https://infoepi.org/posts/2024/05/01-doppelganger-hides-engagement.html

Institute for Strategic Dialogue (ISD). (2024a). Pro-Kremlin responses to the Moscow terrorist attack in Russia, Germany and Italy. https://www.isdglobal.org/digital_dispatches/pro-kremlin-responses-to-the-moscow-terrorist-attack-in-russia-germany-and-italy/?cmplz-force-reload=1723456361335

Institute for Strategic Dialogue (ISD). (2024b). Pro-Kreml-Kampagnen in Deutschland vor der Wahl zum Europäischen Parlament. https://isdgermany.org/wie-russland-versucht-in-deutschland-vor-der-europawahl-stimmung-zu-machen/

Institute of Strategic Dialogue (ISD). (2022a). Pro-Kremlin network impersonates legitimate websites and floods social media with lies. https://www.isdglobal.org/digital_dispatches/pro-kremlin-network-impersonates-legitimate-websites-and-floods-social-media-with-lies/

Institute of Strategic Dialogue (ISD). (2022b). Deutsche Wahrheit: a pro-Kremlin effort to spread disinformation about Ukraine refugees. https://www.isdglobal.org/digital_dispatches/deutsche-wahrheit-a-pro-kremlin-effort-to-spread-disinformation-about-ukrainian-refugees/

Laine M., Morozova A. (2024, 16. September). Leaked Files from Putin's Troll Factory: How Russia Manipulated European Elections. VSquare, Delfi Estonia. https://vsquare.org/leaked-files-putin-troll-factory-russia-european-elections-factory-of-fakes/

Lamberty, P. & Frühwirth, L. (2023, 19. Juni). Informationsmanipulation als komplexe Herausforderung. https://cemas.io/publikationen/integratives-modell-desinformation

Lehn, J. (2024, 25. April). „Doppelgänger"-Kampagne verbreitet gefälschte „Spiegel"-Artikel und schaltet Werbung in sozialen Medien. AFP Faktencheck. https://faktencheck.afp.com/doc.afp.com.34P26MD

Lorenz, T. (2022, 8. April). Internet 'algospeak' is changing our language in real time, from 'nip nops' to 'le dollar bean'. https://www.washingtonpost.com/technology/2022/04/08/algospeak-tiktok-le-dollar-bean/

Lothian, A. D. S. (2022, 11. November). Administrative Panel Decision. Süddeutscher Verlag GmbH, Süddeutsche Zeitung GmbH, and Süddeutsche Zeitung Digitale Medien GmbH v. Iakov Shultz. Case No. DME2022 – 0020. World Intellectual Property Organization. https://www.wipo.int/amc/en/domains/decisions/pdf/2022/dme2022-0020.pdf

Lyndell, D. (2024, 4. März). Spam, scams, and propaganda: The state of Twitter 15 months into Elon Musk's reign. The Insider. https://theins.press/en/society/269668

Meta. (o. D. a). Irreführendes Verhalten. Richtliniendetails. Abgerufen am 4. September 2024 von https://transparency.meta.com/en-gb/policies/community-standards/inauthentic-behavior/

Meta (o. D. b) Autorisierung für Wahlwerbung bzw. Werbung zu politisch oder gesellschaftlich relevanten Themen erhalten. Meta. https://www.facebook.com/business/help/208949576550051?id=288762101909005

Milenkoski, A. (2024, 22. Februar). Doppelgänger. Russia-aligned influence operation targets Germany. SentinelOne. https://www.sentinelone.com/labs/doppelganger-russia-aligned-influence-operation-targets-germany/

Neutsch, J. (2023, 24. April). Blauer Haken bei X (ehemals Twitter): Bedeutung erklärt. Praxistipps Chip. https://praxistipps.chip.de/blauer-haken-bei-twitter-was-bedeutet-er-noch-und-wer-hat-ihn_38410

Nimmo, B. & Agranovich, D. (2022, 27. September). Removing coordinated inauthentic behavior from China and Russia. Meta. https://about.fb.com/news/2022/09/removing-coordinated-inauthentic-behavior-from-china-and-russia/

Nimmo, Gleicher, Franklin, Hundley & Torrey. (2023, November). Third Quarter: Adversarial Threat Report. Meta. https://transparency.fb.com/sr/Q3 – 2023-Adversarial-threat-report

OpenAI. (2024, 30. Mai). Disrupting deceptive uses of AI by covert influence operations. https://openai.com/index/disrupting-deceptive-uses-of-AI-by-covert-influence-operations/

Qurium. (2024, 11. Juli). How Russia uses EU companies for propaganda. https://www.qurium.org/alerts/exposing-the-evil-empire-of-doppelganger-disinformation/

Recorded Future (2023, 5. Dezember). Obfuscation and AI Content in the Russian Influence Network "Doppelgänger" Signals Evolving Tactics. Recorded Future. https://go.recordedfuture.com/hubfs/reports/ta-2023 – 1205.pdf

Reset Tech. (2024). Doppelganger revamped: Network of verified accounts spreads multilingual propaganda on X. https://web.archive.org/web/20240831184410/https:/www.reset.tech/uploads/reset-tech-research-note-doppelganger-revamped-network-of-verified-accounts-spreads-multilingual-propaganda-on-x.pdf

Rosenbach, M., Schult, C. (2024, 16. Januar). Baerbocks Digitaldetektive decken russische Lügenkampagne auf. Spiegel online. https://www.spiegel.de/politik/deutschland/desinformation-aus-russland-auswaertiges-amt-deckt-pro-russische-kampagne-auf-a-765bb30e-8f76 – 4606-b7ab-8fb9287a6948

Literaturverzeichnis

The Insider. (2024a, 25. März). Kremlin bot network spreads articles claiming ISIS not responsible for Crocus City Hall terrorist attack, points fingers at Kyiv, UK, U.S. https://theins.press/en/news/270225

The Insider. (2024b, 8. Mai). Kremlin botnet launches wave of disinformation claiming Havana Syndrome doesn't exist. https://theins.press/en/news/271400

UDRP disputes. (2023, 15. Juni). Decision for dispute CAC-UDRP-105536. https://udrp.adr.eu/decisions/detail?id=64b1307e-8aa1b86c2906d7c5

U.S. Department of Justice. (2024, 4. September). Justice Department disrupts covert Russian government-sponsored foreign malign influence operation targeting audiences in the United States and elsewhere. https://www.justice.gov/opa/pr/justice-department-disrupts-covert-russian-government-sponsored-foreign-malign-influence

U.S. Department of The Treasury. (2024, 20. März). Treasury sanctions actors supporting Kremlin-directed malign influence efforts. https://home.treasury.gov/news/press-releases/jy2195

Verbraucherzentrale. (2024, 28. Mai). Digitale Dienste: Was regelt der Digital Services Act? https://www.verbraucherzentrale.de/wissen/digitale-welt/onlinedienste/digitale-dienste-was-regelt-der-digital-services-act-87852

VIGINUM (2023, 19. Juli). RRN: A complex and persistent information manipulation campaign. VIGINUM. https://www.sgdsn.gouv.fr/files/files/Publications/20230719_NP_VIGINUM_RAPPORT-CAMPAGNE-RRN_EN.pdf

Walsh, D. (2024, 15. Juli). Elon Musk wirft EU „illegalen Geheim-Deal" vor – X droht wegen neuen EU-Digitalgesetz hohe Strafen. Euronews. https://de.euronews.com/next/2024/07/15/elon-musk-wirft-eu-illegalen-geheim-deal-vor-x-drohen-wegen-neuen-eu-digitalgesetz-hohe-st

Wienand, L., Steurenthaler, S., Loelke, S. (2022, 30. August). Infokrieg. Putins Troll-Armee greift Deutschland an. T-Online. https://www.t-online.de/nachrichten/deutschland/gesellschaft/id_100042596/ukraine-krieg-pro-russische-kampagne-das-steckt-hinter-den-fake-artikeln.html

X Hilfe-Center. (2023, März). Richtlinien zu Plattformmanipulation und Spam. https://help.x.com/de/rules-and-policies/platform-manipulation

ZEIT ONLINE (2024, 29. März). Baerbock bezeichnet Fake-News als Teil von Putins Kriegsarsenal. https://www.zeit.de/politik/deutschland/2024-03/annalena-baerbock-russland-nato-einflussnahme

Zholobova, M., Reiter, S., Pankratova, I., Pertsev, A. (2023, 25. September). Russia's sprawling wartime fake news machine. Meet the organization behind the Kremlin's disinformation about Ukraine. Meduza. https://meduza.io/en/feature/2023/09/25/russia-s-sprawling-wartime-fake-news-machine

Über CeMAS

CeMAS, das gemeinnützige Center für Monitoring, Analyse und Strategie bündelt jahrelange interdisziplinäre Expertise zu den Themen Verschwörungsideologien, Desinformation, Antisemitismus und Rechtsextremismus. CeMAS adressiert aktuelle Entwicklungen in diesen Themenfeldern durch systematisches Monitoring zentraler digitaler Plattformen und moderne Studiendesigns, um so innovative Analysen und Handlungsempfehlungen abzuleiten. Darüber hinaus berät CeMAS Entscheidungsträger:innen aus Zivilgesellschaft, Medien und Politik.

Über die Autor:innen und Mitarbeitenden

LF

Lea Frühwirth

Lea Frühwirth ist Psychologin und forscht bei CeMAS als Senior Researcher zu Desinformation, Propaganda und Verschwörungserzählungen.

JS

Julia Smirnova

Julia Smirnova untersucht als Senior Researcher bei CeMAS staatliche Einflusskampagnen und die Verbreitung von Desinformation im Internet.

AM

Anna Meyer

Anna Meyer ist Politikwissenschaftlerin mit Spezialisierung im IT-Bereich und untersucht bei CeMAS als studentische Hilfskraft die Verbreitung von Desinformation im Internet.


GRENZEZANK
Dumbarton Oaks Konferenz:
Polnischer Premier spuckt
Experten sehen gute
DEN
ITSLOSIGKEIT DER
TION FÜHRT
D IN DEN RUIN
offensive wird
sten treffen
ZUM ENDE LESEN TEILT DIE
DEN SOZIALEN NETZWERKEN. ES IST
CHER
HEN
ICHT
Deutschland
ür verbotene

A Better Internet is Possible—

A Better World is necessary.

CeMAS

CeMAS, das gemeinnützige Center für Monitoring, Analyse und Strategie bündelt jahrelange, interdisziplinäre Expertise zu den Themen Verschwörungsideologien, Desinformation, Antisemitismus und Rechtsextremismus. CeMAS adressiert aktuelle Entwicklungen in diesen Themenfeldern durch systematisches Monitoring zentraler digitaler Plattformen und moderner Studiendesigns, um so innovative Analysen und Handlungsempfehlungen abzuleiten. Darüber hinaus berät CeMAS Entscheidungsträger:innen aus Zivilgesellschaft, Medien und Politik.

Web:
cemas.io

Social:
@cemas_io

Kontakt:
info@cemas.io

Presse:
presse@cemas.io