März 2018 · Ben Scott und Dipayan Ghosh

Digitale Werbung und politische Propaganda

Wie mit Technologien der digitalen Werbeindustrie Desinformation im Netz verbreitet wird

Stiftung Neue Verantwortung

Think Tank für die Gesellschaft im technologischen Wandel

Vorwort

Dieser Bericht wurde gemeinsam von der New America Foundation und dem Shorenstein Center der Harvard University unter dem Titel "Digital Deceit – The Technologies Behind Precision Propaganda on the Internet" am 23. Januar 2018 in den USA veröffentlicht. Die Übersetzung und Überarbeitung erfolgte durch die Stiftung Neue Verantwortung, in der der Autor des Textes Ben Scott Teil des Vorstandes ist.

2019 wird das Jahr sein, in dem erstmals die Umsätze der digitalen Werbeindustrie die der klassischen Werbung weltweit ablösen. Grund dafür ist vor allem die Möglichkeiten der digitalen Werbeindustrie, extrem präzise aufdie Nutzer:innen zugeschnittene Werbung zu schalten. Mit Verhaltensdaten und persönliches Profilen lassen sich Online-Werbekampagnen orchestrieren, die weit über einzelne Webseiten oder Plattformen hinaus ihre Werbebotschaften präzise – und für die Öffentlichkeit verdeckt – setzen.

Diese Technologien der digitalen Werbeindustrie rücken aber auch zunehmend in den Blick derjenigen, die diese Technologien dazu nutzen, Desinformation im Netz zu verbreiten. Die Debatte in den USA um Fake News, Dark Ads und dem Einfluss Russlands auf die Präsidentschaftswahl 2016 zeigt aber nur einen kleinen Ausschnitt von dem, was sich heute bereits technisch umsetzen lässt.

Soziale Netzwerke, Webseiten, Suchmaschinen und Newsletter bieten neue Möglichkeiten für Desinformationskampagnen. Sie ermöglichen es, Wähler:innen auf unterschiedlichen digitalen Kanälen zu erreichen, für die wiederum mehr und mehr internetbasierte Angebote von Bedeutung sind, um sich täglich über das politische Geschehen zu informieren. Dabei wird es für die Nutzer:innen immer schwerer, die Güte einzelner Information im Netz zu beurteilen – vor allem wenn Desinformationskampagnen viel Geld investieren, um scheinbar seriösen Content zu verbreiten.

Der vorliegende Text von Ben Scott und Dipayan Ghosh beruht auf einer Analyse des amerikanischen Markts. Die aufgezeigten technischen Werkzeuge und Wirkungsmechanismen der digitalen Werbeindustrie – von Social-Media-Management-Software und Cookies über Suchmaschinenoptimierung

und das Erheben von Verhaltensdaten bis hin zum Einsatz Künstlicher Intelligenz zum Profiling und Targeting – kennen keine nationalen Grenzen.

Wir möchten die Analyse von Ben Scott und Dipayan Ghosh mit dieser Übersetzung deutschen Leser:innen zugänglich machen, da wir auch in Deutschland einen breiten gesellschaftlichen Diskurs über die Gefahren von Desinformation für unsere Demokratie brauchen. Dabei spielen die Instrumente der digitalen Werbewirtschaft zur Verbreitung und Verstärkung von Botschaften eine wichtige Rolle.

Executive Summary

2016 gab es Versuche aus Russland, mit Desinformationskampagnen auf großen Internetplattformen die US-Präsidentschaftswahl zu beeinflussen. Dies hat nicht nur in den USA, sondern auch in vielen europäischen demokratischen Staaten eine intensive und kontroverse Debatte ausgelöst, wie sich offene, vernetzte Gesellschaften gegen gezielte Desinformationskampagnen schützen können. Im Fokus dieser Debatte steht dabei häufig einerseits Russland. Andererseits wird intensiv über die Verantwortung der großen US-Internetunternehmen Google, Facebook und Twitter diskutiert, deren technische Plattformen die Einflussnahme ermöglicht haben.

Die Rolle Russlands sowie die großen Internetplattformen sind in der Diskussion um Lösungen von zentraler Bedeutung. Allerdings sind sie nur Teil eines tiefergehenden Problems. Analysen und Berichte aus den USA zeigen, dass ein Großteil der gezielten Falschinformation durch branchenübliche digitale Werbe- und Marketingtools verbreitet wurden, die durch die technologischen Entwicklungen des letzten Jahrzehnts enorm an Wirkmacht gewonnen haben. Diese Werbeinstrumente beschränken sich keineswegs auf die bekannten Anzeigenmärkte von Plattformen wie Google, Facebook und Twitter. Die Geschäftsmodelle der Plattformbetreiber bilden den Mittelpunkt eines wesentlich größeren Werbe-Ökosystems, mit dem sich Millionen von Menschen mit maßgeschneiderten und für die breitere Öffentlichkeit nicht sichtbaren Werbebotschaften erreichen lassen. Werden Praktiken und Technologien der modernen digitalen Werbewirtschaft – egal ob durch ausländische Staaten oder politische Gruppen im eigenen Land – für gezielte Falschnachrichten oder hetzerische politische Kampagnen eingesetzt, ist der Schaden für das öffentliche Interesse, die politische Kultur und das gesellschaftliche Zusammenleben erheblich.

Um Desinformation etwas entgegenzusetzen reicht es deshalb nicht aus, nur über Maßnahmen auf den Plattformen nachzudenken – von Transparenzregeln für das Schalten politischer Werbung bis hin zum Löschen von Inhalten. Wir müssen genauer verstehen, wie das digitale Werbe-Ökosystem funktioniert, auf dem Desinformation und Propaganda aufbaut: Vom System hoch-personalisierter Anzeigenschaltung bis hin zum gesamten Markt für Produkte und Dienstleistungen, mit denen sich die Stimmung über das Internet anheizen lässt. Gleichzeitig müssen wir die wirtschaftliche Dynamik der heutigen digitalen Werbewirtschaft verstehen. Eine entscheidende Rolle spielen dabei die Plattformen: Ihre wirtschaftlichen Interessen und die Ziele der Macher:innen von Desinformationskampagnen gehen nicht selten Hand

in Hand. Eine erfolgreiche Desinformationskampagne schafft ein hoch responsives Publikum, welches die Bindung auf der Plattform vorantreibt und letztendlich mehr Gewinne für alle Parteien generiert.

Im digitalen Werbemarkt gibt es vor allem fünf Bereiche, die für die Verbreitung von Desinformation wie Fake News, Propaganda oder gezielter Hetze relevant sind.

Verhaltensdaten

Der erste Bereich betrifft die Erfassung von Verhaltensdaten durch Web Tracking, Location Tracking und geräteübergreifendes Tracking. Durch das Aufsaugen und Kombinieren riesiger Mengen persönlicher Daten können Unternehmen – seien es soziale Netzwerke, Vermarktungsplattformen, spezialisierte Werbeagenturen oder Markenartikelhersteller – einzelne Personen oder gesellschaftliche Gruppen identifizieren sowie sehr detailliert deren Vorlieben und Einstellungen erfassen. Aus diesen Daten lässt sich vorhersagen, welche Menschen für welche Botschaften besonders empfänglich sind. Den Macher:innen digitaler Desinformation spielt dies in die Hände: Desto mehr sie über ihre Zielgruppen wissen, desto günstiger und genauer können sie diese ansprechen und manipulieren.

Online-Anzeigenkampagnen

Immer genauere Verhaltensdaten sowie Fortschritte bei Rechenleistung und Speicherkapazität haben in den letzten Jahren die Präzision und Wirkung von Online-Anzeigenkampagnen dramatisch erhöht. Der Markt für Online-Anzeigen ist ein Werkzeug, dass Daten einsetzt, um Einfluss auf Meinungen und Stimmungen zu nehmen. Die professionellsten Systeme erlauben es, die Wirkung tausender Variationen einer einzelnen Botschaft in kurzen Experimenten innerhalb einer gesellschaftlichen Gruppe zu testen. Diese Präzisionswerbung ermöglicht es, eine Gefolgschaft aufzubauen, die den eigenen Botschaften offen gegenüber steht und hilft, diese massenhaft zu verbreiten.

Suchmaschinenoptimierung

Im Markt für Suchmaschinenoptimierung (kurz SEO für Search Engine Optimization) werden Milliarden umgesetzt. Im Mittelpunkt der Branche steht der Suchalgorithmus von Suchmaschinen wie Google, der Millionen von Internetnutzer:innen auf Websites lenkt, die ganz oben in den Ergebnissen aufgelistet sind. Ziel der SEO ist es, Online-Inhalte so auf den Suchalgorithmus abzustimmen, dass sie besser gefunden werden. Die meisten Tools und

Taktiken in dieser Branche sind völlig legal. Die sogenannte "Black Hat SEO" hingegen, trickst den Algorithmus durch illegale (oder zweifelhafte?) Methoden aus , um etwa die Suchergebnisse während einer Nachrichtenwelle für einige Stunden mit manipulierten Inhalten zu bestimmen, bis der Suchmaschinenbetreiber die Verzerrung bemerkt.

Social Media Management-Software

Social Media Management-Services (SMMS) stehen für einen Bereich des digitalen Marketings, bei dem Verfahren des maschinelles Lernen mit konventionellen Werbetechnologien verbunden werden. Social Media Management-Dienste erlauben es, vorbereitete Botschaften oder Kampagnen automatisiert an verschiedene Zielgruppen über viele Medienkanäle wie Facebook, Instagram oder Twitter gleichzeitig zu senden. Hochentwickelte SMMS-Dienste nutzen Verhaltensdaten und beobachten in Echtzeit die Kommunikation in sozialen Medien, um Botschaften zur richtigen Zeit im jeweils geeigneten Kanal zu platzieren. Bisher ist nicht bekannt, ob diese Dienste bereits bei Desinformationskampagnen zum Einsatz kamen. Weil sie aber ein ideales Hilfsmittel sind, um während laufenden Nachrichten-Entwicklungen Botschaften schnell und breit zu streuen, gilt ihr Einsatz in Zukunft auch in diesem Zusammenhang als wahrscheinlich.

Fortschritte durch Künstliche Intelligenz

Auch im kommenden Jahrzehnt werden wir weitere technische Innovationen sehen, mit denen Werbetreibende, Agenturen und Verleger ihre Gewinne steigern. Dabei spielt die Wirkung der Künstlichen Intelligenz (KI) eine ganz wesentliche Rolle. Modernes Online-Marketing erfordert derzeit noch immer viele komplexe Entscheidungen darüber, welche Kundengruppe welche Botschaft in welcher Variation erhalten soll. Noch komplizierter ist diese Arbeit, wenn nicht nur das Kaufverhalten Einfluss genommen werden soll, sondern auf persönliche Werte oder politische Überzeugungen etwa bei Wahlen. Fortschritte bei KI-Technologien werden das Testen von Botschaften, die Verarbeitung von Verhaltensdaten oder die Segmentierung von Zielgruppen automatisieren oder stark vereinfachen. Dies wird auch die Wirkung von Desinformationskampagnen verstärken.

Inhaltsverzeichnis

Ben Scott und Dipayan Ghosh
März 2018

Digitale Werbung und politische Propaganda

Als im vergangenen Sommer enthüllt wurde, dass eine von Russland gestützte Desinformationskampagne große Internetplattformen in den USA genutzt hatte, um die Präsidentenwahl 2016 zu beeinflussen, ging eine Schockwelle durch die Nation. Geheimdienstuntersuchungen, investigative Berichte und forensische Daten aus Unternehmen belegen die Einflussnahme und liefern ein umfassenderes Bild über die Hintergründe des Geschehens. Facebook, Google und Twitter haben jetzt bestätigt, dass russische Akteure Versuche koordiniert haben, den politischen Prozess in den USA durch Verbreitung von polarisierenden Botschaften auf diesen Plattformen zu stören.[1] Allein auf Facebook erreichte der russische Einfluss mehr als 125 Millionen Nutzer.[2] Dennoch liegt ein Großteil der Geschehnisse im Dunkeln.

Die Schnittstelle von politischer Desinformation und Internet-Plattformtechnologien hat nicht nur eine öffentliche Grundsatzdiskussion entfacht, sondern auch eine breitere nationale Debatte über die Integrität der US-amerikanischen Demokratie. Umfang, Undurchsichtigkeit und Einfluss der politischen Kommunikation auf den größten digitalen Plattformen haben die führenden US-Internetunternehmen in den kritischen Blick der Öffentlichkeit gerückt. Ende 2017 haben Topanwält:innen von Facebook, Google und Twitter in einer Reihe weltweit veröffentlichter Anhörungen vor dem US-Kongress ausgesagt.[3] Im Rahmen dieser umfassenden und oftmals erbittert geführten Sitzungen machten die Kongressführer:innen keinen Hehl daraus, dass die Unternehmen ihrer Meinung nach deutlich mehr hätten tun müssen, um den Missbrauch ihrer Plattformen durch russische Akteure zu erkennen und zu verhindern.[4] Außerdem mussten sie zugeben, dass die bis-

1 Craig Timberg, Elizabeth Dwoskin, Russian content on Facebook, "Google and Twitter reached far more users than companies first disclosed, congressional testimony says," *Washington Post*, 30.10.2017.

2 Testimony of Colin Stretch, General Counsel, Facebook, Hearing Before the United States Senate Committee on the Judiciary Subcommittee on Crime and Terrorism, October 31, 2017; Mike Isaac, Daisuke Wakabayashi, "Russian Influence Reached 126 Million Through Facebook Alone," *New York Times*, 30.10.2017.

3 "Seth Fiegerman and Dylan Byers, Facebook, Twitter, Google Testify before Congress," CNN, 1.11.2017.

4 Issie Lapowsky, "Congress asks tech to face hard truths about Russia meddling," *WIRED*, 31.10.2017.

herigen Erkenntnisse über russische Aktivitäten vermutlich nur die Spitze des Eisbergs der politischen Desinformation ist.

Die Unternehmen haben versprochen, freiwillige Maßnahmen zu ergreifen. Zu den am häufigsten diskutierten Plänen gehören die Durchsetzung einer Kennzeichnung von politischer Werbung auf den Plattformen, um Nutzer:innen, die Opfer der russischen Desinformationskampagnen geworden sind, zu informieren, sowie die Einrichtung einer durchsuchbaren öffentlichen Datenbank digitaler Werbung samt Content-, Sponsor- und Targeting-Parameter.[5] Vor kurzem hat Facebook angekündigt, den Algorithmus seines Flaggschiffs, der News Feeds, zu überarbeiten, um Inhalte von Freund:innen und Familie zu priorisieren und im Gegenzug Texte und Videos von Nachrichtenanbietern herabzustufen. Außerdem plant das Unternehmen, die Nutzer:innen nach ihrem Vertrauen in Nachrichtenquellen zu befragen, um die Sichtbarkeit von nicht vertrauenswürdigen Quellen zu reduzieren.

Das alles sind wichtige und positive Schritte. Aber sie reichen nicht aus. Denn das tiefgreifende Problem sprengt den Rahmen der aktuellen Debatte.

Das vorliegende Papier liefert eine tiefer gehende Untersuchung von internetbasierter Werbung und Medienplattformen und erkundet, inwiefern diese die Verbreitung politischer Desinformation ermöglichen. Derzeit liegt der Fokus stark auf der Einflussnahme Russlands und den vor allem von Google, Facebook und Twitter entwickelten und betriebenen werbetechnischen Plattformen. Doch die digitalen Tools, die den Machern von Desinformationskampagnen zur Verfügung stehen, sind keineswegs auf die Dienste dieser drei Formen beschränkt. Die Plattformbetreiber stehen im Mittelpunkt eines umfassenden Service-Ökosystems, das eine sehr gezielte politische Kommunikation möglich macht, die Millionen von Menschen mit maßgeschneiderten und für die breitere Öffentlichkeit nicht sichtbaren Botschaf-

5 Olivia Solon, "Twitter plans to make political ads more transparent amid Russia revelations," *The Guardian*, October 24, 2017; Issie Lapowsky, "Eight revealing moments from day two of the Russia hearings," *WIRED*, 1.11.2017.

ten erreicht. In dieser Analyse beleuchten wir den gesamten Werkzeugkasten der Präzisionspropaganda, darunter:

- die Erfassung von Verhaltensdaten
- digitale Werbeplattformen
- Suchmaschinenoptimierung (SEO)
- Social Media Management-Software
- algorithmische Werbetechnologie

Die Kombination aus miteinander verbundenen Tools stellt eine brillante technologische Maschinerie dar, mit der sich die wirtschaftlichen Interessen von Werbetreibenden und Plattformbetreibern aufeinander abstimmen lassen. Je erfolgreicher eine Werbekampagne ist, desto mehr Geld machen alle Beteiligten. Dabei werden alle Werbetreibenden auf diesem Markt gleich behandelt – ganz gleich, ob sie Einzelhandelsprodukte, Nachrichten, politische Kandidat:innen oder Falschmeldungen bewerben. Wenn es um die Anwendung dieser Tools geht, versuchen alle Werbetreibenden, die erfolgreichsten und überzeugendsten Strategien anzuwenden. Es werden also alle Tools zur Erfassung von Verhaltensdaten, die für die gezielte Kommunikation an hoch responsive Zielgruppen zur Verfügung stehen für politische Desinformationskampagnen eingesetzt.

Es ergibt sich allerdings ein Problem: Wenn die Betreiber von Falschinformationen dieses System für die Präzisionspropaganda nutzen, ist der Schaden für das öffentliche Interesse, die politische Kultur und die Integrität von Demokratie erheblich und hat ein völlig anderes Ausmaß als bei anderen Werbearten. Unsere These lautet, dass wir den gesamten Markt der digitalen Werbung untersuchen und die Ausrichtung wirtschaftlicher Interessen entwirren müssen, um den bestmöglichen Weg zu finden, „Bad Guys“ zu identifizieren und den öffentlichen Schaden so gering wie möglich zu halten. Dabei offenbart sich ein sehr viel komplexeres und vermutlich auch verstörenderes Bild des Problems. Fehlt dieser umfassendere Blickwinkel aber, können wir keine Strategien zur effektiven Abwehr von Desinformationsaktivitäten entwickeln.

Der Vorfall der russischen Desinformationskampagnen, der diese Kontroverse entfacht hat, veranschaulicht diese Annahmen. Bei den von den Russ:innen eingesetzten Technologien handelt es sich um branchenübliche digitale Werbe- und Marketingtools, die sich ganz einfach auf jede beliebige Desin-

formationskampagne von jedem beliebigen Akteur zuschneiden lassen. Es ist verlockend, die russische Digitalpropaganda von einer rein nationalen Sicherheitswarte, anstatt von einer politisch-ökonomischen zu betrachten. Doch die politische Desinformation stellt – ganz unabhängig vom Akteur dahinter – ein öffentliches Übel dar und der Großteil dieser Desinformation in den USA werden von inländischen Akteuren verbreitet.[6] Dieses eher allgemeine Problem ist sehr viel schwieriger zu beheben. Nicht nur, weil es oftmals umstritten ist, was genau eine Falschinformation ist, sondern auch weil viele Desinformationsaktivitäten wahrscheinlich vollkommen legal und in den USA sogar unter dem First Amendment – dem Zusatzartikel zur Verfassung der Vereinigten Staaten – geschützt sind. Dadurch ergibt sich eine enorme Herausforderung, der sich Internetplattformen ganz aktiv stellen müssen.

Ausgehend von den hier präsentierten Analyseergebnissen sind wir überzeugt, dass effektive Lösungen auf die politische Ökonomie der digitalen Informationsmärkte abzielen müssen. Die finanziellen Interessen, die die Kerntechnologien der führenden Internetplattformen befeuern, und die Ziele der Macher von Desinformationskampagnen gehen nicht selten Hand in Hand. Die Plattformen sind davon alles andere als begeistert; dennoch lassen sich die gemeinsamen Interessen nicht leugnen, schließlich eignet sich der digitale Anzeigenmarkt hervorragend für die Zwecke von Desinformationsaktivitäten. Oftmals setzen Kampagnen dieser Art auf Sensationsthemen und extrem polarisierte politische Inhalte. Inhalte also, die die Verbraucher:innen aufmerksam machen und fesseln, was wiederum Gewinne für internetbasierte Inhalte generiert.[7] Eine erfolgreiche Desinformationskampagne schafft ein hoch responsives Publikum, welches die Bindung auf der Plattform vorantreibt und letztendlich mehr Gewinne für alle Parteien ermöglicht.

Dieses Problem lässt sich nicht durch das schlichte Blockieren von Inhalten lösen, die russischen Akteuren zugeschrieben werden, und ebenso wenig durch eine sisyphosartige Zensur mit blindwütigen Versuchen, bestimmte Inhalte zu löschen oder einen bestimmten Sprachgebrauch zu verbieten. Solche Ansätze schlagen fehl, weil die Systeme hinter den Kampagnen hoch anpassungsfähig und flüchtig sind. Selbst ein gut aufgestellter mul-

6 Siehe zum Beispiel: Yochai Benkler, Rob Faris, Hal Roberts und Ehtan Zuckerman, "Study: Breitbart-led rightwing media ecosystem altered broader media agenda," *Columbia Journalism Review*, 3.3.2017.

7 Für einen breiten Überblick über die wirtschaftliche Bedeutung von Aufmerksamkeit siehe: Tim Wu, Attention Merchants, New York: Vintage, 2017.

tinationaler Konzern wird nicht in der Lage sein, bei diesem Kampf gegen Windmühlen schnell genug zu reagieren. Noch wichtiger aber ist: Ein Großteil der Falschinformationen sind rechtlich geschützte politische Willensbekundungen. Transparenz bezüglich der Sponsoring-, Reichweiten- und Targeting-Parameter von Werbung ist ein hilfreicher Schritt. Sie ist jedoch nur dann am effektivsten, wenn sie eine kleine Gruppe von "Bad Guys" bloßstellt, deren Verhalten im krassen Gegensatz zum Verhalten aller anderen steht. Wenn Transparenz zu Tage fördert, dass das Problem systemischer Natur ist, könnte sie den Effekt haben, ein solches Verhalten zu normalisieren. Entsteht ein disziplinarischer Druck auf die Verbreiter von Falschinformationen, wenn eine Datenbank mit Online-Werbung, die hin und wieder von Nutzer:innen angesehen wird, beweist, dass Propaganda auf den Plattformen quasi epidemisch ist?

Um bessere Abhilfemaßnahmen zu finden, ist ein tiefer greifendes Verständnis des vorliegenden Problems erforderlich. Dieses Papier soll den Fokus erweitern – von der Analyse digitaler Anzeigenschaltung hin zu einer Analyse des gesamten Markts für Produkte und Dienstleistungen, die emotionalisierende Inhalte über das Internet verbreiten. Unser Ziel ist es, die These, politische Desinformation habe Erfolg, da sie der strukturellen Logik des breiteren digitalen Werbemarkts folgt, von dessen Produkten profitiert und seine Strategien perfektioniert, zu dokumentieren. Wenn sich diese These als richtig erweist, müssen wir ganz genau verstehen, wie dieses Ökosystem funktioniert. Wir müssen in Betracht ziehen, wie sich politische von nicht politischen Kampagnen auf Internetplattformen unterscheiden, um uns auf erstere und deren Auswirkung auf die Demokratie zu konzentrieren. Wir müssen kreative Wege finden, um den Bürger:innen die Macht zu geben, Manipulation durch die Medien zu erkennen, bloßzustellen und zu diskreditieren. Und wir müssen uns kritische Gedanken darüber machen, wie wir nicht nur die heutigen Probleme rund um Falschinformationen bewältigen, sondern auch die zukünftigen.

Erfassung von Verhaltensdaten

Daten sind das Herzblut des e-Commerce. Jeder Post, jeder Klick, jede Suche und jedes Teilen wird in einem Nutzer:inprofil protokolliert, in eine segmentierte Zielgruppe zusammengefasst und in Algorithmen eingespeist, die auf maschinellem Lernen basieren. Anhand dieser Daten können Werbetreibende Rückschlüsse auf die persönlichen Vorlieben, Verhaltensweisen und Überzeugungen von Individuen ziehen, welche extrem gezielte digitale Werbekampagnen ermöglichen. Die Macht der akkumulierten Daten treibt

außerdem Desinformationskampagnen an, die das Soziogramm von Personen nicht etwa dazu nutzen, Kaufentscheidungen zu beeinflussen, sondern die Stimmung, die politischen Ansichten und das Wahlverhalten – und zwar durch präzise Propaganda.

Die Werbeindustrie steht im Zentrum der Internetwirtschaft und ihr Wert leitet sich zunehmend von der Erfassung von Verhaltensdaten ab, mit denen Zielgruppen segmentiert und anvisiert werden. Das Geschäft hat sich rapide weiterentwickelt – von einer digitalen Version der konventionellen Anzeigenplatzierung samt Agenturen und Herausgeber hin zu einem mittlerweile datengesteuerten Markt, der sich auf Zielgruppensegmentierung und gezielte Botschaften konzentriert.[8] Algorithmische Technologien bestimmen den Inhalt, das Timing und die Zielgruppe für die Bereitstellung und Anzeige von Online-Werbung.[9] Durch das Aufsaugen riesiger Mengen an persönlichen Daten können Unternehmen im gesamten digitalen Werbe-Ökosystem – seien es Social-Media-Plattformen, Vermarktungsplattformen, spezialisierte Werbeagenturen oder Markenunternehmen – anfangen, die persönlichen Vorlieben einer Person zu erkennen und deren Empfänglichkeit für unterschiedliche Werbeformen vorherzusagen.[10]

Dabei kann gar nicht genug betont werden, wie wichtig persönliche Daten für den nachhaltigen Erfolg des Ökosystems der digitalen Werbung sind. Daten befeuern den Handel im Internet; jedes verbraucherorientierte Internetunternehmen mit starker Präsenz in der Online-Werbung erfasst und teilt Informationen über einzelne Nutzer:innen, um den Erfolg seiner Werbekunden zu unterstützen.[11] Ähnliches gilt für politische Kampagnen, die Wähler:innenverzeichnisse und demografische Daten nutzen, um komplexe Profile von Wahlbezirken zu erstellen. Und das gilt auch für Kampagnen, die politische Desinformation verbreiten.

Technologisch betrachtet haben die Nachverfolgung und Profilerstellung von Internetnutzer:innen zum Zwecke gezielter Werbung nichts Neues. Dennoch bekommen diese Praktiken eine ganz neue Valenz, wenn aus der Verhaltensüberwachung stammende Daten jetzt nicht mehr eingesetzt werden,

8 Susan Young, "Getting the Message: How the Internet is Changing Advertising," *Working Knowledge*, 16.5.2000.

9 Keith Kirkpatrick, "Advertising via Algorithm," Communications of the ACM, 18.2.2016.

10 "Getting to know you," *The Economist*, 11.9.2014.

11 "The World's Most Valuable Resource is No Longer Oil, But Data," *The Economist*, 6.5.2017.

um Produkte zu verkaufen, sondern um Wähler:innen zu manipulieren und in die Irre zu führen. Wie aber erfassen die Unternehmen im digitalen Werbe-Ökosystem diese Daten? In diesem Abschnitt erläutern wir drei Kategorien von weit verbreiteten Technologien, die eine Identifizierung und Profilerstellung möglich machen.

Web Tracking

Wenn ein:e Internetnutzer:in zu einem Artikel auf einer Nachrichtenwebsite navigiert, beispielsweise zu www.bbcnews.com, spielen sich hinter den Kulissen hunderte von digitalen Transaktionen ab. Wenn ein Webbrowser eine Seite aufruft und lädt, liefert er weitaus mehr als lediglich den wesentlichen Content. Am deutlichsten zeigt sich dies in den Werbeanzeigen von Dritten, die dafür zahlen, auf der Seite zu erscheinen. Für unsere Zwecke aber viel wichtiger – und für das Auge der Nutzer:innen unsichtbar – lädt die Seite sämtliche integrierten Web Tracking-Technologien. Die grundlegendste Tracking-Technologie ist der Standard-Webcookie.

Webcookies können entweder First-Party- oder Third-Party-Cookies sein. In der Regeln werden die sogenannten First-Party-Cookies von dem Betreiber der Website entwickelt und platziert, Third-Party-Cookies dagegen werden von anderen Entitäten in Zusammenarbeit mit dem Websiteeigentümer entwickelt und platziert.[12] Oft setzen Webseiten Cookies ein, damit sich der:die Nutzer:in problemlos auf der Seite anmelden kann und sein:ihr Konto geladen wird. Das US-amerikanische Buchhandelsunternehmen Barnes & Noble oder Amazon beispielsweise nutzen einen First-Party-Cookie, sodass sich die Online-Shopper auf der Seite anmelden können und eine Echtzeitliste der Artikel in ihrem Warenkorb sehen.

Genauso häufig aber setzen Websites (First-Party- oder Third-Party-) Cookies ein, um die Aktivitäten einzelner Nutzer:innen auf der Website zu verfolgen und persönliche Gewohnheiten und Verhaltensweise zu erfassen.[13] Diese Art der Verhaltenserfassung erfolgt in der Regel, damit die Website oder die verbundenen Partner im Laufe der Zeit Dinge wie Vorlieben, Interessen und Überzeugungen der Nutzer:innen ableiten können. Diese Informationen können dann unter anderem dazu verwendet werden, Nutzer:innen für spezifische Werbeanzeigen anzuvisieren, beispielsweise zu den neuesten Hon-

12 Tim Peterson, "A Google Cookie Replacement Could Upend Online Advertising," *AdAge*, 19.9.2013.

13 Annie Lowrey, "How Online Retailers Stay a Step Ahead of Comparison Shoppers," *Washington Post*, 11.12.2010.

da-Modellen oder Chanel-Parfums, abhängig von ihrer Persönlichkeit und dem Verhalten bei ihrer bisherigen und aktuellen Internetnutzung.[14]

Unternehmen speichern Verhaltensdaten in großen Datenbanken, die die Nutzer:innenaktivitäten im Laufe der Zeit aufzeichnen. Diese Daten können mit einer IP-Adresse verknüpft werden, also dem eindeutigen Identifikationcode, der einem bestimmten Computer oder Mobilgerät zugewiesen ist. Trotzdem geben viele Menschen ganz freiwillig ihre persönlichen Daten heraus, indem sie per Kreditkarte einkaufen, eine E-Mail-Adresse angeben oder sich über ihre privaten Online-Konten mit einer bestimmten Website verbinden. Damit verknüpfen sie ihre Verhaltensdaten noch enger mit ihrem individuellen Profil.[15] Einige Unternehmen nutzen diese Daten ausschließlich zur Vermarktung ihrer eigenen Produkte und Services. Andere wiederum verkaufen sie an Dritte, die sie mit zusätzlichen Informationen kombinieren und dann an andere Werbetreibende weiterverkaufen. Mit der Zeit können Verhaltensdatenprofile sehr umfangreich und detailliert werden.

Für Internetfirmen, die global agieren, darunter Suchmaschinen und Social-Media-Plattformen, verspricht das Sammeln und Speichern von Nutzer:innenverhaltensdaten einen enormen potenziellen Mehrwert. Es gibt zwei wichtige Gründe, weshalb die Erfassung von Verhaltensdaten zu einer ökonomischen Aufwärtsspirale führen. Zum einen gilt: Je mehr Verhaltensdaten ein Unternehmen zu einem:einer Nutzer:in sammeln kann, desto besser kann es ihm:ihr gezielte und auf die individuelle Interessen zugeschnittene Anzeigen präsentieren. Und zum anderen kann das Unternehmen diese Nutzer:innen länger auf der Plattform halten, wenn es ihm relevante Inhalte anzeigen kann, und damit die potenzielle Werbefläche für diese Nutzer:innen maximieren. Diese vertikale Integration des „Behavior Trackings“ und des Geschäfts mit der Online-Werbung ist für die Marktmacht globaler Internetplattformen von zentraler Bedeutung.

Im Falle von Plattformen wie Google, Facebook und Twitter lässt sich die Nutzer:innenbindung mit den digitalen Inhalten, einschließlich Anzeigen, Likes für bestimmte Seiten, Klicks auf einzelne Suchergebnisse oder die Interaktion mit News-Feeds, aufzeichnen und in Verhaltensdatenprofile zusammenfassen, mit denen die Unternehmen einzelnen Benutzer:innen dann noch gezielter relevante Inhalte und Anzeigen bereitstellen können. In

14 Veronica Marotta, et. al., Who Benefits from Targeted Advertising?, FTC Comment, 8.10.2015.

15 Manoush Zomorodi, "Do You Know How Much Private Information You Give Away Every Day?" *Time*, 29.3.2017.

der Regel ist diese Art von Verhaltensdaten nur für die Plattform, auf der die Interaktionen stattgefunden haben, zugänglich. Vor allem aus Gründen des Datenschutzes der Nutzer:innen, der Wettbewerbsfähigkeit und des Schutzes von geistigem Eigentum liegt es im Interesse der jeweiligen Plattform, derartige Informationen an niemanden herauszugeben – auch nicht an den:die Nutzer:in, dessen Aktionen diese Daten generiert haben. Neben anderen haben insbesondere Google und Facebook mit der vertikalen Integration von „Behavior Tracking“ und „Ad Targeting“ einen unglaublichen kommerziellen Erfolg erzielt.

Da Cookies das Ziel haben, Online-Aktivitäten und -Verhalten zu verfolgen, werden sie als gravierender Eingriff in die Privatsphäre von Internetnutzer:innen betrachtet. In Europa beispielsweise haben Aufsichtsbehörden angeordnet, dass Websites eine Browserwarnung für die Besucher:innen einblenden, wenn sie Cookies verwenden.[16] Angesichts dieser Hintergründe beschließen manche Internetnutzer:innen, die Cookies zu löschen. Websites und Werbetreibende aber reagieren mittlerweile darauf und setzen Technologien ein, die so genannten Local Shared Objects (LSO) oder Flash-Cookies, die von den Nutzer:innen gelöschte Cookies erneut installieren.[17]

Eine weitere übliche Praxis ist das Einbetten von Cookies in E-Mails. Mit E-Mail-Cookies können Unternehmen erfahren, wann und wo eine E-Mail geöffnet wurde. Unternehmen, die diese Art des E-Mail-Trackings einsetzen, können außerdem feststellen, auf welchem Gerät welche E-Mail geöffnet wurde. Oft werden diese Dienste ähnlich eingesetzt wie webbasierte Standard-Cookies: durch 1x1 Pixel. Der Tracking Service-Provider kann sehen, ob dieses Pixel auf dem Gerät der E-Mail-Empfänger:innen heruntergeladen oder an andere Geräte weitergeleitet und dort heruntergeladen wurde. Diese Dienste werden als vorgefertigte Software-Pakete von den unterschiedlichsten Firmen entwickelt und bereitgestellt.[18] Ein aktueller Bericht von einer

16 Olivia Solon, "A simple guide to cookies and how to comply with EU cookie law," *WIRED*, 12.5.2012.

17 Erik Larkin, "Are Flash Cookies Devouring Your Privacy?" *PC World*, 23.10.2009.

18 Ana Gotter, "The 5(+5) Best Email Tracking Services of 2017," AdEspresso by Hootsuite, 2.5.2017.

dieser Firmen schätzt, dass mehr als 40 Prozent aller täglich versendeten 269 Milliarden E-Mails mit Tracking-Technologien versehen sind.[19]

Bekleidungshersteller wie Nike oder Einzelhändler wie Macy's könnten ein Interesse am E-Mail-Tracking haben, um zu verstehen, wie stark Kund:innen auf die unterschiedlichen Arten von Marketing-E-Mails ansprechen. Noch interessanter aber mag sein, dass webbasierte Dienstleister wie Amazon und Facebook das E-Mail-Tracking sehr umfassend einsetzen – auch in den E-Mails, die sie ihren Kund:innen senden –, um das User Engagement im Hinblick auf ihre Services zu steigern. Diese Art des E-Mail-Trackings kann einen Beitrag zu den riesigen Datenmengen leisten, die diese Unternehmen über ihre Nutzer:innen speichern. Was aber wahrscheinlich am kritischsten ist: E-Mail-Tracking kann den Serviceanbietern helfen, einen besseren Einblick in die Standortgewohnheiten der einzelnen Nutzer:innen zu gewinnen.

Ein weiteres Internet-Tracking-Tool ist das so genannte Web-Beacon oder schlicht Beacon. Diese Tools sind programmierte Objekte, die in eine Website eingebaut werden – meist von einer Drittpartei, die für dieses Vorrecht zahlt. Wenn ein:e Nutzer:in die Seite lädt, wird auch das Beacon geladen. Der Drittbetreiber des Beacons erhält das Signal, dass ein:e Nutzer:in die Website besucht hat. Diese Technik wird auch als Server Call (Serveraufruf) bezeichnet. Bei Eingang des Signals sendet die Drittpartei das Web-Beacon an den Websiteeigentümer, damit es im Webbrowser des Nutzers gerendert werden kann.[20]

Das Entscheidende an Web-Beacons aber ist, dass sie für den:die Nutzer :in typischerweise unsichtbar oder nur sehr schwer zu entdecken sind, schließlich haben sie nicht den Zweck, Content bereitzustellen, sondern vielmehr zu ermitteln, ob der:die Nutzer:in die Seite besucht hat. Je nach Inhalt dieser Seite kann die Drittpartei mit Web-Beacons Rückschlüsse auf die Vorlieben der Nutzer:innen ziehen, insbesondere weil diese kleinen Tools oft eingesetzt werden, um die Nutzeraktionen auf der Seite in Echtzeit zu verfolgen, beispielsweise Mausklicks, Hand- oder Cursor-Bewegungen. Eine Vermarktungsplattform, die Web-Beacons über ein ganzes Netz von Websites installiert hat, kann außergewöhnlich viel Macht ausüben, da sie durch Tracking der Online-Bewegungen von Besucher:innen eine enorme Informationsfülle anhäuft. Alle diese Daten können mit der IP-Adresse einer Person, mit per-

19 Brian Merchant, "How email open tracking quietly took over the web," WIRED, 11.12.2017.

20 John Kennedy, "Beacons: Better than display advertising?" *Marketing Tech News*, 17.8.2016.

sönlich identifizierbaren Informationen oder “persistent identifiers” (dauerhaften Bezeichnern) verknüpft werden. Wenn Werbetreibende auf diese Daten zugreifen, um ihre Anzeigenkampagnen mit Informationen zu füttern und zu pushen, können sie einzelne Nutzer:innen extrem gezielt ansprechen – nicht zuletzt mithilfe der von Web-Beacons gesammelten Daten.

Location Tracking

Moderne Smartphones sind wahre Wunderwerke der Technik. Und sie sind äußerst effektive Ortungsgeräte. Jedes Mobilteil enthält eine satellitengestützte Technologie, die das US-Militär einst für den militärischen Einsatz entwickelt hatte: das Global Positioning System (GPS). Die GPS-Technologie umspannt ein Netz aus mehr als 30 Satelliten in der Erdumlaufbahn, von denen jeder seine Echtzeitposition über ein simples Kommunikationsprotokoll an die Erdoberfläche sendet. So lange ein mit GPS ausgestattetes Gerät die Positionssignale von mindestens vier dieser GPS-Satelliten empfängt, lässt sich die aktuelle Position des Geräts äußerst präzise bestimmen.[21] Auf diesem System basieren die Karten-Apps von Smartphones, die mittlerweile auf fast jedem Gerät vorinstalliert und genutzt werden.

GPS-Daten sind jedoch nicht die einzigen Standortdaten, die Telefonhersteller und Systembetreiber sammeln. Insbesondere in städtischen Räumen, in denen GPS-Signale durch Gebäude blockiert werden können, werden die Daten häufig mit Triangulationsdaten aus Mobilfunknetzen, WLAN-SSID und Bluetooth-Konnektivitätsdaten kombiniert, um den physischen Standort einer Person punktgenau zu bestimmen. Präzise und hoch genaue Standortdaten sind ein wertvoller Bestandteil des Ökosystems der Anzeigentechnologie, da sie extrem viel Kontext zu den Interessen, Vorlieben, Ansichten und Verhaltensweisen eines Menschen zu Tage fördern können.

Von adressspezifischen Standortdaten lassen sich eine Vielzahl von Informationen ableiten. Ein Smartphone-Hersteller oder ein Entwickler eines mobilen Betriebssystems kann mit hoher Genauigkeit vorhersagen, wo eine Person lebt, wo sie arbeitet, wie sie zur Arbeit kommt, mit wem, wo und wie sie diese Zeit verbringt, welche Geschäfte sie in der realen Welt frequentiert und was sie in ihrer Freizeit tut: sei es Baseball spielen, Filme gucken, nahe gelegene Kneipen besuchen oder am Wochenende Wahlkreise abklappern.[22]

21 Jeffrey Hightower und Gaetano Borriello, "Location Sensing Techniques," *IEEE Computer*, 30.7.2016.

22 Stephen Wicker, Cellular Convergence and the Death of Privacy, Oxford University Press, 19.9.2013.

Diese Informationen über Routineaktivitäten liefern wichtige Signale darüber, wie gezielte digitale Anzeigen auf die persönlichen Interessen der jeweiligen Person zugeschnitten werden können.[23] Der US Supreme Court prüft zurzeit einen Präzedenzfall, der entscheiden wird, ob Strafverfolgungsbehörden die Standortdaten einer Person als so sensibel behandeln müssen, dass für den Zugriff auf diese Daten eine Sondergenehmigung erforderlich ist.[24]

Standortdaten werden von zahllosen kommerziellen Akteuren erfasst – das können der Netzwerkbetreiber und der Gerätehersteller[25] aber auch die Betreiber des mobilen Betriebssystems und der installierten Apps sein. Mittlerweile muss man bei vielen beliebten mobilen Diensten den Zugriff auf die Standortdaten zulassen, um diese Dienste überhaupt nutzen zu können. Viele moderne Apps – zum Beispiel Navigation, Mitfahrgelegenheiten, Gaming und soziale Medien – können nur in vollem Umfang genutzt werden, wenn der:die Nutzer:in den Zugriff auf seine Standortdaten erlaubt. Nicht selten werden die Nutzer:innen dazu gedrängt, ihre Standortdaten mit den unterschiedlichsten Unternehmen zu teilen, die diese Nutzerdaten oder gewonnenen Erkenntnisse wiederum an diverse Dritte weitergeben können.[26] In der Regel wissen die Nutzer:innen nicht, dass ihre Daten weitergeleitet werden.

Der Standortdienst einschließlich GPS-Funktion ist auf Smartphones meist ein Opt-out-Service, das heißt, Nutzer:innen können ihn über die Einstellungen in ihrem mobilen Betriebssystem deaktivieren. Aber das ist eher unüblich und kann recht lästig sein, da viele beliebte Apps wie Yelp oder Uber ständig den Zugriff auf Standortdaten anfordern, sobald der:die Nutzer:in

23 Drew Fisher et. al., Short paper: location privacy: user behavior in the field, SPSM '12 Proceedings of the second ACM workshop on Security and privacy in smartphones and mobile devices, 19.10.2012.

24 Alex Emmons, "Supreme Court Hears Arguments about Cellphone Location Tracking in Landmark Privacy Case," *The Intercept*, 29.11.2017.

25 Kelsey Finch, "Location Tracking: Now Coming to a Government, Employer and Retailer Near You," *The Privacy Advisor*, 29.10.2013.

26 Andrew J. Hawkins, "Uber Wants to Track Your Location Even When Your Not Using the App," *The Verge*, 30.11.2016.

den Standortdienst deaktiviert oder die Freigabe von Standortdaten an diese bestimmten Apps außer Kraft setzt.[27]

Die Aktivierung der Standortdienste und die Freigabe der Daten an Apps können eine Reihe weiterer Datenschutzprobleme mit sich bringen. Obwohl Anwendungen Standortdaten ausschließlich erfassen sollten, um die technische Funktion ihres Dienstes zu ermöglichen, gibt es in den USA keine klaren Regulatorien hinsichtlich der Erfassung von Standortdaten. Vielmehr müssen sich Unternehmen meist nur an das halten, was sie ihren Nutzer:innen im Kleingedruckten ihrer Datenschutzrichtlinie zusagen. Das führt zu Situationen, in denen manche mobilen Apps Standortdaten erfragen oder sogar anfordern, obwohl unklar ist, inwiefern diese Daten für die Funktionalität der App von Belang sind.[28] Angesichts des florierenden Datenmakler-Ökosystems und der enormen Nachfrage nach älteren Standortdaten ist dies ganz besonders alarmierend. Und selbst wenn Nutzer:innen die Standortdienste deaktivieren, können mobile Betriebssysteme wie iOS und Android trotzdem den Standort nachverfolgen, unter anderem durch die Ortung über Mobilfunk-Masten.[29]

In den kommenden Jahren werden sehr wahrscheinlich immer neue Methoden für das Standort-Tracking entwickelt; ein Grund hierfür ist die technologische Weiterentwicklung in Bereichen wie der virtuellen Realität und der Künstlichen Intelligenz, ein anderer die standardmäßige Kontrolle im Bereich Sicherheit und Datenzugriff. Ende 2017 zeigte ein Forscher, dass jede App, die auf die iPhone-Fotogalerie zugreifen kann, auch sehen kann, wo die einzelnen Fotos aufgenommen wurden – vorausgesetzt, der:die Nutzer:in hat das Geotagging seiner Fotos aktiviert.[30]

Geräteübergreifendes Tracking

In den USA greifen die Verbraucher:innen in der Regel nicht nur über ein Gerät auf das Internet zu, sondern über diverse Geräte zuhause und am

27 David Kaplan, "Overwhelming Number Of Smartphone Users Keep Location Services Open," *GeoMarketing*, 22.4.2016.

28 Lisa Gutermuth, "How to Understand What Info Mobile Apps Are Collecting About You," *Slate*, 24.2.2017.

29 Keith Collins, "Google Collects Android Users' Location Even When Location Services are Disabled," *Quartz*, 21.11.2017.

30 Mix, "Googler proves an iPhone app with camera permission can secretly record you," *The Next Web*, 26.10.2017.

Arbeitsplatz. Letztes Jahr besaß ein durchschnittlicher nordamerikanischer Haushalt über sieben mit dem Internet verbundene Geräte.[31] Für die digitale Werbeindustrie kann diese Situation ein Problem darstellen: Meist wollen Werbetreibende ein und derselben Person nicht identische Anzeigen über mehrere Geräte schicken.[32] Sie möchten zumindest erfassen, wie oft ein:e Nutzer:in eine bestimmte Anzeige gesehen hat, ob mobil oder über den PC. Zwar kann es sich positiv auf die Bindung der potenziellen Kund:innen auswirken, wenn sie eine Anzeige mehrfach sehen, aber der Werbetreibende will kontrollieren können, wann und wo diese Anzeige erscheint. Zu diesem Zweck hat die digitale Werbeindustrie eine Reihe robuster Technologien für das geräteübergreifende Tracking entwickelt. Einige der Signale beinhalten Informationen aus dem IP-Adress-Tracking, von Standortdaten und Web Tracking.[33] Während Regulierungsbehörden und Anwält:innen viele Bedenken zu dieser Praktik – speziell im Hinblick auf die Privatsphäre einer Person – äußern, haben Verbraucher:innen zurzeit nur wenig Wahl. Sie müssen die freiwilligen Standards der Internetunternehmen wohl oder übel akzeptieren.[34] Sobald diese geräteübergreifenden Aktivitäten zuverlässig durchgeführt werden können, könnten viele Unternehmen, darunter Apple, Facebook und Google, einen so genannten dauerhaften oder "persistent/unique identifier" (eindeutigen Bezeichner) mit dem:der Nutzer:in verknüpfen.[35] Der Bezeichner wird damit zum zentralen Anker für die über diverse Anwendungen, Plattformen und Geräte hinweg gesammelten Nutzerdaten. Somit können Nutzer:innen auch durch die Verwendung verschiedener Geräte ihre Privatsphäre nicht schützen, da sie durch die Verwendung bestimmter Webservices oder anderer Signale eindeutig zugeordnet werden können.

Eine mit dem geräteübergreifenden Tracking verwandte Praktik ist das Browser-Fingerprinting. Der Fingerprint, also Fingerabdruck, eines Browsers besteht normalerweise aus einem Datensatz mit Informationen zur Konfiguration des Browsers oder Betriebssystems. Dazu können Informationen über den Anbieter und die Version des Browsers, das Betriebssystem

31 Laura Hamilton, "How Many Active Connected Devices Does a Home in North America Average?" *CED Magazine*, 24.8.2016.

32 Joshua Koran,"The truth about cross-decive tracking," *AdAge*, 1.8.2013.

33 Justin Brookman et. al., "Cross-Device Tracking: Measurement and Disclosures, Proceedings on Privacy Enhancing Technologies," *De Gruyter*, 2017.

34 The Federal Trade Commission, "FTC Releases New Report on Cross-Device Tracking," 23.1.2017.

35 Zach Rodgers, "With Atlas Relaunch, Facebook Advances New Cross-Device ID Based On Logged In Users," *AdExchanger*, 28.9.2014.

und dessen Version, die Spracheinstellung, eine Liste der Browser-Plugins, Nicht-Verfolgen-Einstellungen (Do Not Track), den Einsatz von Ad-Blockern, die Zeitzone und die Browser-Schriftart und ähnliches gehören.[36] Da es so viele Browser-Konfigurationsmöglichkeiten gibt und Nutzer:innen sie oft an ihre Vorlieben anpassen, kann über den Browser-Fingerprint sogar ein:e einzelne:r Internetnutzer:in identifiziert werden. So hat ein oft zitiertes Projekt der Electronic Frontier Foundation 2015 herausgefunden, dass 84 Prozent der Internetnutzer:innen, die an dem Experiment teilnahmen, eindeutige Browser-Fingerprints produzierten.[37]Bedenklich ist auch, was eine Forscher:innengruppe erst kürzlich herausgefunden hat: Websites können den Browser-Fingerprint einzelner Internetnutzer:innen aufspüren, selbst wenn der:die Nutzer:in unterschiedliche Browser einsetzt.[38] Nutzer:innen können dieses Aufspüren entweder durch datenschutzerweiternde Software, zum Beispiel von Ghostery und anderen Firmen, oder durch Funktionen wie beispielsweise Flash und Javascript einschränken.[39] Doch trotz allem hat sich die Gefährdung der Privatsphäre durch das Aufkommen des Browser-Fingerprintings deutlich erhöht.

Auswirkungen für Desinformationskampagnen

Wie alle übrigen Werbetreibenden profitieren auch die Verbreiter von Falschmeldungen in hohem Maße von der Erfassung von Verhaltensdaten. Ihr Ziel ist es, so viele Informationen wie möglich über potenzielle Zielgruppen zu sammeln, um organischen Content – also Text, Audio oder Videos, die im Gegensatz zur digitalen Werbung auf sozialen Netzwerken gepostet werden, für deren Platzierung oder Bewerbung aber nicht zwangsläufig gezahlt werden muss, – über die unterschiedlichsten Medienkanäle und gezielten Anzeigen auf Internetplattformen zuzuschneiden.

Dazu bieten sich verschiedene Vorgehensweisen an: Wenn der Betreiber ein oder mehrere Web-Präsenzen hat, können die Daten direkt über First-Party-Cookies erfasst werden. Verbreiter von Falschinformationen betreiben oftmals Fake News-Seiten wie Blogs und Social-Media-Kanäle, auf denen

36 Lance Cottrell, "Browser fingerprints, and why they are so hard to erase," *Network World*, 17.2.17.

37 Nick Nikiforakis und Gnes Acar, "Web advertisers are stealthily monitoring our browsing habits – even when we tell them not to," *IEEE Spectrum*, 25.7.2014.

38 Dan Goodin, "Now sites can fingerprint you online even when you use multiple browsers," *Ars Technica*, 13.2.2017.

39 Mark Stockley, "Browser fingerprints – the invisible cookies you can't delete," *Naked Security*, 1.12.2014.

sie ähnliche Inhalte verbreiten. Verhaltensdaten, die eine Interaktion mit diesem Content widerspiegeln, sind besonders wertvoll für die anschließende Entwicklung von Messages und Anzeigen, die auf bestimmte demographische Gruppen abzielen. Betreiber können auch Third-Party-Cookies auf inhaltlich relevanten anderen Websites einbetten und so die Reichweite der Erfassung ausweiten. Darüber hinaus steht ihnen eine Fülle an Optionen zur Verfügung, um den Zugriff auf Verhaltens- und Standortdaten von kommerziellen Verkäufern, zum Beispiel Datenmaklern, zu kaufen. Außerdem könnten die Betreiber über First-Party-Cookies gewonnene Verhaltensdaten mit persönlich identifizierbaren Informationen verknüpfen, indem sie E-Mail-Adressen für Abonnementservices oder Mobiltelefonnummern für Textnachrichten einholen.

Facebook bietet Webseitenbetreibern einen beliebten Dienst an, mit dem es individuelle Aktivitäten auf Websites von Dritten verfolgen kann: Dazu sind in die Seiten dieser Websites Engagement-Objects von Facebook eingebettet – beispielsweise klassisch durch „Like"-Buttons. Facebook kann Verhaltensdaten erfassen – darunter Daten, die sowohl mit Facebook-Nutzer:innen als auch mit Menschen verknüpft sind, die kein Facebook-Konto haben, – und diese mit seinem Audience-Network-Service verlinken, mit dem Kund:innen Werbung außerhalb der Facebook-Anwendung und auf anderen mobilen Apps präsentieren können.[40] Dieser Service liefert dem Werbetreibenden keine persönlichen Daten, ermöglicht ihm aber, diese in die Anzeigenservices von Facebook zu integrieren. Auf diese Weise lassen sich sehr effektiv unterschiedliche demografische Gruppen segmentieren und Einzelpersonen ansprechen, die auf bestimmte Botschaften stark reagieren – auch ohne Facebook-Konto. Einige Regulierungsbehörden haben in der Vergangenheit versucht, mehr Klarheit über diese Praktiken zu gewinnen, und den Firmen bestimmte Auflagen erteilt.[41]

Aus all diesen Daten ergibt sich ein sehr nuanciertes Bild der aktuellen und potenziellen Zielgruppen. Je mehr die Betreiber von Falschmeldungen über ihre Zielgruppen wissen, desto leichter können sie diese aufspüren, manipulieren und irreführen.

40 Amar Toor, "Facebook begins tracking non-users around the internet," *The Verge*, 27.5.2016.

41 Lisa Vaas, "Belgium to Facebook: Stop tracking non-Facebook users or face $26K daily fines," *Naked Security*, 11.11.2015; Natasha Lomas, "Facebook Ordered To Stop Tracking Non-Users in France," *TechCrunch*, 9.2.2016.

Online- Werbekampagnen

Die große Menge der im Internet gesammelten Verhaltensdaten hat ein zentrales Ziel: Anzeigen effektiver und gezielter zu schalten, um mehr Nutzer:innen mit Inhalten, Vertriebsstrategien, Stimmungen und Beeinflussungen zu erreichen. Nicht zuletzt aufgrund der Fortschritte in den Bereichen Rechenleistung und Speicherkapazität in den letzten Jahren haben die Raffinesse und Präzision gezielter Anzeigen dramatisch zugenommen – sie nutzen automatisierte Experimente zur Effektivität von Tausenden von Nachrichtenvarianten zusammen mit dem Nutzer:innen-Profiling. Die Analyse der Zielgruppensegmentierungen bietet eine kosteneffiziente Möglichkeit, damit Desinformationskampagnen zwei ihrer wichtigsten Ziele erreichen: erstens, responsive Zielgruppen über ihre Kernkund:innenkreise hinweg zu erreichen und zu pflegen und zweitens, aus beliebten Nachrichten virale Phänomene zu machen, indem man Kanäle mit dem beworbenen Content überflutet.

Die äußerst wertvollen Nutzer:innendaten, die über die digitalen Tracking-Tools gewonnen wurden, werden für die Zielgruppensegmentierung und die gezielte Anzeigenschaltung eingesetzt – Praktiken, die die Werbebranche in den letzten zehn Jahren revolutioniert haben. Schon immer haben Werbetreibende versucht, Botschaften zu kreieren, die bei bestimmten demografischen Gruppen – definiert nach Einkommen, Bildungsniveau, Geschlecht, Alter, Wohnsitz, sexueller Orientierung, Sprache und ethnischer Zugehörigkeit – besonders gut ankommen. Bevor es das Internet gab, war dies eine recht schwammige Wissenschaft. Das ist längst vorbei. Große Werbeagenturen haben sich von den Print- und TV-Medien abgewandt. Im vergangenen Jahr übertrafen die Gewinne aus digitaler Werbung zum ersten Mal die der TV-Werbung.[42] Die begehrtesten Kanäle, um mit Anzeigen eine maximale Bindung zu schaffen, sind heute Internetplattformen wie Facebook, Google und Twitter.[43]

In den letzten Jahren haben Internetfirmen immer effektivere Tools entwickelt, um mit intelligenter digitaler Werbung einzelne Personen und ihre jeweiligen Vorlieben zu erreichen. Das Geschäftsszenario ist simpel: Je relevanter die Anzeige ist, desto mehr fühlt sich der:die Nutzer:in von der angezeigten Werbung angesprochen und desto länger verweilt er:sie auf der

42 George Slefo, "Desktop and Mobile Ad Revenue Surpasses TV for the First Time," *AdAge*, 26.4.2017.

43 Randolph E. Bucklin and Paul R. Hoban, "Marketing Models for Internet Advertising," *Handbook of Marketing Decision Models*, 14.7.2017.

Plattform.[44] Eine von einer programmatischen Anzeigenschaltung gestützte Echtzeitbereitstellung liefert Werbetreibenden einen so großen Wert, dass sie sich zum Branchenstandard entwickelt hat.[45]

Der Targeting-Prozess wird von Daten gestützt, die aus nutzer:innengeneriertem Content stammen, oder direkt aus dem Nachverfolgen des Nutzer:innenverhaltens – entweder auf der eigenen Internetpräsenz des Werbenetzwerks oder auf anderen Websites. Mit der Zeit werden diese Datensätze immer größer und detaillierter und erlauben Internetunternehmen, spezifische Profile von diversen Nutzer:innentypen zusammenzustellen, die dann an Werbetreibende verkauft werden können. Neben detaillierten demografischen Profilen können Werbetreibende im Laufe der Zeit die Interessen, Vorlieben, Überzeugungen und Verhaltensweise einzelner Personen, die mit dem Online-Content interagieren, ablesen, um besonders präzise Nutzer:innenprofile zu kreieren.[46] Meist pflegen sie diese Profile in großen Datenbanken; manchmal finden sich in diesen Datenbanken sogar Personen, die keine aktiven Nutzer:innen ihrer Dienstleistungen sind. Man kann sich eine solche Datenbank als Excel-Tabelle vorstellen, in der die Nutzer:innen jeweils in einer Zeile abgebildet sind und in den Spalten demografische Daten, Vorlieben, Überzeugungen der Nutzer:innen erfasst sind. Während einige dieser Daten mit persönlich identifizierbaren Informationen (PII) verknüpft sein können, ist ein Großteil mit individuellen und von Internetunternehmen gespeicherten Benutzer:innenkonten verbunden und steht in ihrer deanonymisierten Form Dritten nicht zur Verfügung.

Diese Datenbank wird mit einer so genannten Advertising-Technology-Plattform, einer Anzeigentechnologieplattform, verlinkt. Über die Plattform können Werbetreibende die Communitys auswählen, die sie mit ihrer Anzeigenkampagne hauptsächlich erreichen wollen. Ein kleines Unternehmen beispielsweise, das sich auf den Verkauf von Herren-Sneakers in New York City spezialisiert hat, könnte es auf Männer zwischen 18 und 35 abgesehen haben, die sich für Basketball interessieren, in den vergangenen sieben Tagen die Website eines bekannten Schuhherstellers besucht haben und in

44 Dhruv Grewal et. al., "Mobile Advertising: A Framework and Research Agenda," *Journal of Interactive Marketing*, Mai 2016.

45 Shuai Yuan et. al., "Real-time Bidding for Online Advertising: Measurement and Analysis," in *Proceedings of the Seventh International Workshop on Data Mining for Online Advertising*, 2013.

46 Ewan Duncan, Developing a fine-grained look at how digital consumers behave, McKinsey & Co., Juli 2013; Cade Metz, "How Facebook's Ad System Works," *New York Times*, 12.10.2017.

New York City leben. Moderne Anzeigentechnologien ermöglichen einem solchen Unternehmen genau das – und zwar mit enormer Genauigkeit und zu geringen Kosten.[47] Geschickte Anzeigenschalter testen Variationen derselben Botschaft über eine große Bandbreite von Nutzer:innenprofilen hinweg, um den Werbeinhalt zu optimieren und die am stärksten ansprechenden Profile anzuvisieren. Bei dieser Art von Tests, bei denen verschiedene Bedingungen berücksichtigt werden, können die Werbetreibenden manchmal mehrere Tausend Anzeigen pro Tag schalten.

Da die Services über Anzeigenplattformen bereitgestellt werden, die in der Regel eher durch algorithmische Sensortechnologien als durch eine menschliche Prüfung gestützt werden, können gezielte Anzeigen automatisch über Tausende von Websites und Social Media-Feeds gleichzeitig laufen. Die Engagement-Statistiken werden sofort protokolliert und trainieren sowohl den Werbetreibenden als auch den Plattformalgorithmus bezüglich der erfolgreichsten Targeting-Strategien. Je mehr Geld und Zeit ein Inserent in das Testen von Marktsegmentierung und Message-Responsiveness investiert, desto effektiver kann er seine Listen hoch responsiver Kund:innenkreise verfeinern und ausbauen.[48]

Heute steht Werbetreibenden eine Fülle an Optionen für das Gestalten von Digitalanzeigen zur Verfügung. Ein gravierender Unterschied allerdings besteht zwischen Content, der in separaten Anzeigenfeldern erscheint, und solchem, der als beworbener Content beispielsweise im News-Feed von sozialen Medien angezeigt wird. Ersterer ist quasi ein Nachfahre der traditionellen Anzeigenschaltung und kann in einem Seitenfenster neben Suchergebnissen oder dem News-Feed angezeigt werden. Letzterer umfasst Content, den der Werbetreibende möglicherweise in seinem Social-Media-Account posten möchte; er zahlt dafür, dass der Inhalt häufiger in den Timelines der Nutzer:innen erscheint.

Die führenden Internetplattformen haben der gezielten Anzeigenschaltung zu einer ganz neuen Dimension verholfen, indem sie Inserenten die Möglichkeit bieten, mit ihren Anzeigen ganz bestimmte Kund:innenzielgruppen zu

47 Aske Christiansen, "The Ultimate Guide to Facebook Ads Interest Targeting Research (Advanced Methods Exposed)," AdEspresso by Hootsuite, 27.3.2017.

48 Devin Guan, "Machine learning is helping martech lead the AI revolution," *AdAge*, 19.6.2017.

erreichen.[49] Diese Zielgruppen, beziehungsweise spezifische Personengruppen, die einen bestimmten Internetdienst nutzen, setzen sich in der Regel aus Menschen zusammen, die bereits als Kund:innen der werbenden Marke bekannt sind. Marken können ihre Kund:innenzielgruppen auf unterschiedliche Weise zusammensetzen; die vermutlich einfachste ist, die persönlichen Daten der Nutzer:innen zu sammeln – also Name, E-Mail-Adresse oder Telefonnummer –, sobald sie die Website oder eine Filiale der Marke besuchen. Die Nachrichten- und Kommentarplattform Breitbart beispielsweise fordert Besucher:innen auf ihrer Website permanent zur Eingabe von persönlichen Informationen auf. Für viele Online-Services ist die Erfassung von persönlichen Kontaktdaten eine Standardpraktik, die zwei Ziele verfolgt: erstens, den Kunden Nachrichten und Angebote per E-Mail zu senden, zweitens – und wahrscheinlich noch viel wichtiger – zu erfahren, um wen es sich bei der Zielgruppe genau handelt. Dadurch kann Breitbart diese Personen auf Werbeplattformen wie Facebook, die eine Zielgruppensegmentierung von zuvor vom Inserenten gesammelten „persönlich identifizierbaren Informationen“ (PII) ermöglichen, gezielt ansprechen.

Für die Zusammenstellung von Kundenzielgruppen nutzen Werbetreibende noch cleverere Methoden. Eines der besten Beispiele ist das Tool Facebook-Pixel, eine 1x1-Grafik, das manche Webentwickler auf ihren Seiten einsetzen, um eine gezielte Anzeigenschaltung über Facebook zu ermöglichen. Wenn jemand eine Website besucht, auf der das Pixel installiert ist, erhält Facebook automatisch Informationen über diesen Besuch. Obwohl die Übertragung von persönlich identifizierbaren Informationen an den Website-Betreiber nicht zwangsläufig Teil der Datentransaktion ist, kann der Website-Betreiber später Facebook-Nutzer ansprechen, die seine Website in den letzten Monaten besucht und das Facebook-Pixel geladen haben.[50]

Häufig sind Kundenzielgruppen nur das Einfallstor, um eine breitere Bevölkerungsgruppe noch umfassender und automatisiert zu erreichen. Die führenden Internetplattformen ermöglichen ihren Inserenten mittlerweile, Kundenzielgruppen-Listen hochzuladen und ihre Werbekampagnen an eine größere Gruppe von gleichgesinnten Personen, die diese Plattformen

49 George Slefo, "LinkedIn Debuts New Targeting Feature for Marketers," *AdAge*, 1.3.2016; Ginny Marvin, "Google To Let Advertisers Upload And Target Email Lists in AdWords With Customer Match," *Marketing Land*, 28.9.2015; Josh Constine, "Facebook Lets Businesses Plug in CRM Email Adresses to Target Customers with Hyper-Relevant Ads," *TechCrunch*, 20.9.2012.

50 Greg Finn, "Facebook pixels get upgrade to track actions & page data," *Marketing Tech News*, 27.4.2017.

nutzen, weiterzuvermarkten.[51] Bei Facebook wird diese Werbefunktion das Erreichen einer “Lookalike-Zielgruppe“ genannt.[52] Theoretisch könnte eine Werbemarke eine Liste seiner 5.000 repräsentativsten Kunden haben und mehr Menschen wie diese erreichen wollen. Die Marke könnte diese Liste mit E-Mail-Adressen oder Telefonnummern auf der Werbeplattform von Facebook hochladen. Die E-Mail-Adressen werden dann mit Facebook-Konten abgeglichen, um eine Kundenliste zu erstellen. Über die „Lookalike“-Funktion könnte Facebook dann 5.000 weitere Personen identifizieren, die den ursprünglichen 5.000 Kunden ähnlich sind. Die Gesamtanzahl der identifizierten „Doppelgänger“ hängt zum Teil davon ab, wie viel der Werbekunde investiert hat. Diese Ähnlichkeiten können auf beliebigen Informationen basieren, die die Werbeplattform über die Nutzer besitzt, einschließlich Geschlecht, ethnische Zugehörigkeit oder das Interesse an einer bestimmten Sportart. Damit kann der Werbekunde eine sehr viel größere Zielgruppe an Personen erreichen, von denen viele möglicherweise noch nie mit seiner Marke interagiert haben. Wenn nun einer dieser potenziellen Neukunden die Website des Inserenten besucht, kann dieser die persönlichen Daten erfassen und seine Kundendatenbank weiter ausbauen.

Im Laufe der Zeit können der Inserent und dessen Partner – darunter sogar Werbeagenturen oder Werbeplattformen – die Kontaktliste verfeinern und Algorithmen einsetzen, um potenzielle Kunden noch besser zu erreichen und Lookalike-Kunden zu identifizieren. Andere “Conversion Tracking-Technologien”, zum Beispiel Web-Tools wie Web-Beacons, Überwachungsskripte für mobile Apps oder tatsächliche Verkaufsdaten, mit denen Werbetreibende den Erfolg ihrer digitalen Kampagnen messen können, lassen sich ebenfalls nutzen, um künftig gezieltere Anzeigen zu entwickeln und Kunden so effektiv wie möglich einzubinden.

Auswirkungen für Desinformationskampagnen

Die Tools der Zielgruppensegmentierung und gezielten Anzeigenschaltung sind für Desinformationskampagnen die wichtigsten Features, wenn es um digitale Werbung geht. Sämtliche Behavior Tracking-Tools, die Erfassung persönlicher Informationen und das Profiling von Zielgruppen, die Betreiber von Falschmeldungen zur Verfügung stehen, zielen im Großen und Ganzen

51 Ginny Marvin, "Google Rolls Out Similar Audiences for Search and Shopping," *Search Engine Land*, 1.5.2017; Facebook, Target Facebook Ads to People on Your Contact List.

52 Ingrid Lunden, "Facebook expands dynamic ad retargeting to Instagram and travel sector, ramps up 'lookalikes'," *TechCrunch*, 10.5.2016.

darauf ab, die Effektivität von gezieltem Advertising zu erhöhen. In sozialen Medien als organischer Content gepostete Falschinformationen erreichen nur die Nutzer, die den Feeds des Anbieters folgen oder die Posts von Freunden sehen, die diese Art von Inhalten verbreiten. Um ein neues Publikum mit einem anderen demografischen Hintergrund und anderen Vorlieben zu erreichen oder eine Social-Media-Plattform mit bestimmten Botschaften zu überschwemmen, muss man Anzeigen schalten oder für die Bewerbung von Content zahlen, der sonst organisch gepostet würde. Das alles sind zunehmend gebräuchliche Taktiken unter Desinformationskampagnen, wie beispielsweise ein aktueller Bericht über die Wahlkampftaktiken vor den nationalen Wahlen in Kenia illustriert.[53]

Diese Online-Werbekampagnen vertiefen die Bindung zu bekannten Zielgruppensegmenten und weiten sie auf neue Zielgruppen aus. Außerdem katapultieren sie Content, der eindeutig populistisch ist, über eine bestimmte Grenze, so dass er viral wird und dank der Netzwerkeffekte großer Internetplattformen Millionen von Nutzern erreicht. Zusätzlich zu all diesen Vorteilen profitiert die Desinformationskampagne von den in der Plattform selbst integrierten Targeting-Informationen (das heißt, sie erhält benutzerdefinierte Listen, mit denen sie Lookalikes identifizieren kann). Im Gegenzug trägt die Kampagne dazu bei, den zugrunde liegenden Algorithmus mit jeder neuen Botschaft und jedem neu getesteten Zielgruppensegment immer präziser zu machen. Mit anderen Worten: Je erfolgreicher eine Online-Kampagne ist (was auch Falschmeldungs-Kampagnen einschließt), desto effektiver werden folgende Online-Kampagnen sein, da die Werbeplattform Zielgruppen präziser bestimmen kann. Das führt zu einem typischen “Erfolgskreislauf” von Werbeinserenten und Werbeplattform: Beide profitieren vom Erfolg des anderen.

Suchmaschinenoptimierung (SEO)

Der Suchalgorithmus steht im Brennpunkt der Internetwirtschaft – Tag für Tag lenkt er Millionen von Internetnutzern auf die Websites, die ganz oben in den Suchergebnissen aufgelistet sind. Es hat sich eine milliardenschwere Branche entwickelt, in der sich alles darum dreht, die Ergebnisse in Suchmaschinen für alle Arten von kommerziellen Webseiten zu optimieren, und zwar durch genaue Beobachtung und Reverse-Engineering des Ranking-Algorithmus von Google. Die meisten Tools und Taktiken in dieser Branche sind völlig legal und haben lediglich das Ziel, die Webseiten von Unternehmen

53 Reuter Staff, "Kenya president's election campaign used firm hired by Trump: privacy group," Reuters, 14.12.2017.

bei der Suche nach bestimmten Begriffen in den Suchergebnissen ganz oben zu platzieren. Aber es gibt auch andere Techniken – das so genannte „Black Hat SEO" –, die den Algorithmus austricksen und die Suchergebnisse für einige Stunden im Nachrichtenzyklus dominieren, ehe Google diese Verzerrung behebt. Im Arsenal der Präzisionspropagandisten ist dies eine ganz entscheidende Waffe.

Eine wichtige Taktik von Desinformationskampagnen ist die strategische Manipulation von Suchmaschinen-Ergebnisseiten (Search Engine Results Pages, SERP). Zahlreiche, seit den US-Wahlen im Jahr 2016 veröffentlichte Berichte unterstreichen die äußerst ungewöhnlichen Suchergebnisse zu sensiblen Themen. So war beispielsweise eine Woche nach der Wahl das Top-Ergebnis in der Google-Suche nach „final election results", also dem endgültigen Wahlergebnis, ein Link zu einem undurchsichtigen Blog namens „70 News", der behauptete, Donald Trump hätte die Mehrheit der Stimmen der Bürger gewonnen.[54] Im Januar 2017 ergab die Suche nach Begriffen, die mit US-Geheimdienstberichten zur russischen Einmischung in die US-Wahl zu tun hatten, viele Links, die auf Inhalte von Russia Today verwiesen, die diese Vorwürfe bestritten.[55] Anfang Oktober, am Morgen nach dem Anschlag in Las Vegas, waren die Top-Suchergebnisse auf Google Verschwörungs-Blogs, die behaupteten, der Schütze sei ein liberaler Trump-Gegner mit Verbindungen zum IS.[56]

Wie kann das passieren? Google sagt, das seien kleine Störungen in seinen Algorithmen, die umgehend behoben werden. Manchmal mag das stimmen. Aber möglicherweise sind diese Vorfälle das Ergebnis ganz bewusster Versuche, kommerzielle Suchalgorithmen zu manipulieren und die Nutzer zu ganz bestimmten Inhalten zu lenken. Seit Jahren kämpft Google mit diesen Problemen. In den meisten Fällen versuchen Werbetreibende, potenzielle Kunden zu einem Produkt statt zu einem anderen zu leiten – dahinter stecken also Wettbewerbsgründe. Die Bemühungen von Desinformationskampagnen,

54 Philip Bump, "Google's Top News Link for 'Final Election Results' Goes to a Fake News Site with False Numbers," *Washington Post*, 14.11.2016.

55 Kaveh Waddell, "Kremlin-Sponsored News Does Really Well on Google," *The Atlantic*, 25.1.2017.

56 Kevin Roose, "After Las Vegas Shooting, Fake News Regains Its Megaphone," *New York Times*, 2.10.2017.

Suchergebnisse zu manipulieren, ist ein neueres Phänomen. Und sie haben Google wiederholt in Erklärungsnot gebracht.

Zwar arbeitet Google intensiv daran, diese Art der Verzerrung zu bekämpfen, doch das Katz- und Mausspiel bringt immer wieder verstörende Vorfälle hervor, bei denen Verschwörungstheorien, Fake News und andere Falschinformationen die Nachrichten und Fakten in den Suchergebnissen überlagern. Das ist ein echtes Problem, denn zweifelsohne spielen Suchergebnisse zu tagespolitischen Themen eine große Rolle bei der öffentlichen Meinungsbildung. Und weil Google über 75 Prozent des Suchmaschinenmarkts in den Vereinigten Staaten gehört, ist die Integrität seines Suchalgorithmus auch direkt mit der Integrität der öffentlichen Debatte verknüpft. Die Tatsache, dass die Manipulation von Suchergebnissen trotz der Macht und der technischen Kapazitäten von Google Erfolge verzeichnet, beweist die intensiven Bemühungen, das System auszutricksen.

Es ist unklar, wer dahinter steckt. Klar aber sind die Motive. Das oberste Ziel derjenigen, die versuchen, über Suchmaschinen Meinung zu machen, besteht darin, die eigenen Inhalte in den Suchergebnissen ganz nach oben zu befördern. Studien zeigen, dass etwa ein Drittel der Internetsurfer auf den ersten Link in den Suchergebnissen klickt, der keine Werbung darstellt. Die ersten fünf Suchergebnisse erhalten rund 75 Prozent des Traffics.[57] Die erste Seite der Links, also die Top 10, erhält 95 Prozent.[58] Daher ist es äußerst lohnenswert, ganz oben platziert zu sein – ganz gleich, ob man Tennisschuhe verkauft oder politische Nachrichten veröffentlicht. Das hat eine Branche hervorgebracht – die Suchmaschinenoptimierung (SEO) –, die es locker mit Google aufnehmen kann und dabei überraschend häufig als Siegerin hervor-

57 Siehe z.B.: Jessica Lee, "No.1 Position in Google Gets 33% of Search Traffic [Study]," Search Engine Watch, 20.6.2013; und Madeline Jacobson, "How Far Down the Search Engine results Page Will Most People Go?," Leverage Marketing.

58 Lauren Kaye, "95 Percent of Web Traffic Goes to Sites on Page 1 of Google Serps (Study)," Brafton, 21.6.2013.

geht.[59] Die gesamte Online-Content-Branche ist in vielerlei Hinsicht als Reaktion auf den Google-Algorithmus konzipiert.[60]

SEO ist ein großes Geschäft: 2016 betrug der Gesamtumsatz, den Google mit Suchanzeigen machte, 24,6 Milliarden US-Dollar.[61] So viel zahlten Inserenten, um ihre Anzeigen auf den Suchergebnisseiten zu platzieren. Die Größe der SEO-Branche, die versucht, die obersten unbezahlten Plätze auf der Ergebnisseite zu ergattern, beläuft sich Schätzungen zufolge auf einen Jahresumsatz von 65 bis 70 Milliarden US-Dollar.[62] Wenn diese Schätzung stimmt, geben Unternehmen fast dreimal so viel für die Optimierung der organischen Suchergebnisse aus wie für den Kauf von Suchanzeigen. Selbst angesichts der Tatsache, dass das Suchanzeigengeschäft von Google ein geradezu geschichtsträchtiger Verkaufsschlager ist, ist dies außergewöhnlich.[63]

Die mit SEO verbundenen Kosten ergeben sich aus der Komplexität des Problems, das die Optimierer zu lösen versuchen. Die Suchalgorithmen von Google, die als „Hummingbird“ zusammengefasst werden, nutzen zur Bestimmung der Ergebnisreihenfolge einen fast schon sagenumwobenen Satz aus 200 unterschiedlichen (geheimen) Ranking-Signalen. Teil dieses Systems ist die Machine Learning-Software RankBrain. Sie wird laufend aktualisiert. Einer Schätzung zufolge ändert Google seinen Suchalgorithmus fünf- bis sechshundert Mal pro Jahr. Diese Updates beeinflussen die Suchergebnisse und somit die Umsätze, weshalb die SEO-Branche sie genauestens beobachtet.[64] Darüber hinaus veröffentlicht Google einen umfassenden Satz aus Richtlinien für die Auswerter der Suchqualität. Dabei handelt es sich um Tausende von Personen rund um den Globus, die im Auftrag von Google Suchergebnisse auf Grundlage unterschiedlicher Faktoren evaluieren. Die von

59 Wir betonen die Bedeutung von Google in diesem Abschnitt allein deshalb, da es der dominierende Marktführer in diesem Bereich ist. SEO Fachliteratur behandelt quasi keine anderen Suchmaschinen neben Google.

60 Anil Dash, "Underscores, Optimization & Arms Races," *Medium*, 29.11.2017.

61 Tess Townsend, "Google's Share of the Search Ad Market is Expected to Grow," *Recode*, 14.3.2017.

62 Jayson DeMers, "The SEO Industry is Worth $65 Billion; Will It Ever Stop Growing?" *Search Engine Land*, 9.5.2016. Diese Schätzung könnte zu hoch sein. Aber auch konservativere Schätzungen sehen die SEO-Industrie auf dem selben Level wie die Erträge aus Google Anzeigenschaltungen.

63 Erin Griffith, "Bad News for Google Parent Alphabet: The 'G' Will Still Foot the Bill," *Fortune*, 10.8.2015.

64 Moz, "Google Algorithm Change History."

den Auswertern übermittelten Beobachtungen fließen aber nur mittelbar in den Suchalgorithmus ein.[65]

Die Mission der Suchmaschinenoptimierung ist im Wesentlichen, den Google-Suchalgorithmus durch "Reverse Engineering" nachzuvollziehen, um Websites so anzupassen, dass sie eine höhere Platzierung im Ergebnis-Ranking erzielen. Natürlich erhalten sie von Google keine klare Anleitung, wie das funktioniert. Was sie aber haben, sind die Ergebnisse unzähliger Trial-and-Error-Suchen, die sich in akribischen A/B-Tests untersuchen lassen, um zu ermitteln, welche Features einer Website besonders günstig im Suchergebnis-Ranking von Google wegkommen. Es ist, als würde man die Schatten an der Wand vermessen, um die Objekte, die diese Schatten werfen, zu zeichnen.

Im Laufe der Zeit hat die Branche auf bestimmte Standardpraktiken etabliert, die die Grundlage jeder konventionellen SEO-Strategie bilden. Zu diesen Techniken gehören Standardmethoden aus den Bereichen Website-Architektur, Content-Formatierung und Link-Building (das heißt, so viele Sites wie möglich mit der eigenen Site zu verlinken). Im kommerziellen Internet sind diese Praktiken sehr üblich. Diese „White Hat"-Suchmaschinenoptimierung passt Websites an die Crawling-, Indizierungs-, Such- und Ranking-Methoden von Google an. Die Taktiken werden einheitlich angewendet und entwickelt, um eine Unternehmenswebsite in den Top-Ergebnissen zu platzieren und dort zu halten.

Es gibt aber auch andere, episodisch auftretende und flüchtige Taktiken, die als „Black Hat"-Suchmaschinenoptimierung bezeichnet werden. Sie sollen eine bestimmte Website oder mehrere Seiten für kurze Zeit – zum Beispiel für die Dauer eines Nachrichtenzyklus – oben in den Suchergebnissen platzieren. Die Taktiken sind besonders für die Betreiber von Desinformationskampagnen von Bedeutung. Einige der Tools versuchen, den Google-Suchalgorithmus so auszutricksen, dass er eine Ergebnisplatzierung zuweist, die nicht mit der inhaltlichen Qualität, der Reputation der Quelle oder selbst den themenrelevanten Antwort auf die Suchanfrage übereinstimmt.

Auf das Wesentliche reduziert, geht es im SEO-Business – und damit im Such-Business – um drei Dinge: Content, Links und Reputation. Das sind die gemeinsamen Nenner der unzähligen SEO-Leitfäden und -Handbücher, auf

65 Siehe: Google Search Quality Evaluator Guidelines, 27.7.2017.

die Unternehmen zurückgreifen können.[66] Und sie sind die grundlegenden Komponenten sowohl der White Hat- als auch der Black Hat-SEO-Techniken.

- **Content:** Der Algorithmus von Google „kriecht" in die semantische Struktur ganzer Seiten, um zu bestimmen, wie stark sie mit den Suchbegriffen übereinstimmen („Crawling"). Je reichhaltiger und spezifischer der Content ist, desto besser ist das Ranking. Keywords sind bis zu einem bestimmten Grad wichtig, insbesondere im Ankertext von URLs, in Seitentiteln und Artikel-Headern. Eine logische Linkstruktur zwischen den Seiten innerhalb einer Domain, eine mobilgerätefreundliche Anzeige und eine schnelle Ladezeit gehören heute ebenfalls zu den Standard-SEO-Empfehlungen.

- **Links:** Das Herzstück der Suchmaschinenoptimierung ist der Linkaufbau, auch Link Building genannt, also die Verlinkung anderer Websites mit der eigenen (Backlinks). Backlinks von hoch glaubwürdigen Sites erhöhen die Trefferquote, Backlinks von Spam-Websites dagegen wirken sich negativ darauf aus. Social-Media-Links (über Facebook und Twitter) scheinen auch zu zählen, jedoch nicht so sehr wie organische Backlinks.

- **Beliebtheit:** Der Erfolg der Suchmaschinenoptimierung zieht Erfolg nach sich, da die Click-Through-Rate (CTR) ebenfalls ein Faktor beim Such-Ranking ist. Jedes Mal, wenn ein Nutzer auf ein Suchergebnis klickt, verbessert sich die Reputation der Seite und der Domain. Neue Artikel zu ähnlichen Themen, die ebenfalls Aufmerksamkeit auf sich ziehen, erhöhen das Ranking weiter.

Online-Werbekampagnen auf der Suchseite haben keinen Einfluss auf die CTR-Reputation. Doch sie helfen, die Keywords in den Fokus zu rücken, die die besten Konversionsraten liefern und zu einem optimierten Content beitragen.

Keines dieser SEO-Elemente ist grundsätzlich unrechtmäßig oder verzerrt automatisch den Suchalgorithmus. Doch sie lassen sich alle bis zu einem gewissen Grad ausspielen, vor allem, wenn das Ziel ist, Suchergebnisseiten kurzfristig zu dominieren.

Angesichts der Tatsache, dass so viel Geld und so zahlreiche Techniken in die SEO fließen, darf man annehmen, dass sich anormale oder verzerrte Su-

66 Siehe z.B.: Aleh Barysevich, "4 Most Important Ranking Factors According to SEO Industry Studies," *Search Engine Land*, 3.2.2017; Danielle Antosz, "Google Releases the Top 3 Ranking Factors," *Search Engine Journal*, 25.3.2016; SEO PowerSuite, "8 Mayor Google Ranking Signals of 2017," *Search Engine Land*, 11.7.2017.

chergebnisse nicht immer auf Funktionsstörungen zurückführen lassen. Es gibt sie, weil jemand Geld und Anstrengungen investiert hat, um sie einzusetzen – sowohl durch rechtmäßige als auch durch zweifelhafte Mittel. Und der Häufigkeit von Berichten über verzerrte Suchergebnisse nach zu urteilen, scheint dieser Ansatz auch zu funktionieren.[67] Es darf erneut darauf hingewiesen werden, dass die absichtliche Verzerrung von Suchergebnissen kein neues Phänomen ist. Doch ihre Relevanz für die noch junge Praktik umfassender Desinformationskampagnen dagegen nimmt stetig zu.

Googles übliche Reaktion – den Algorithmus zu ändern, um die Betrüger zu frustrieren – erweist sich als immer schwieriger. Wenn SEO-Ergebnisse auf einer Suchseite Falschmeldungen beinhalten, die in eine bestimmte ideologische Richtung weisen, bringt das den Betreiber der Suchmaschine in eine sehr viel unangenehmere Situation. Denn wenn er dieses Problem „behebt“, wirft ihm die eine Seite Voreingenommenheit vor. Behebt er das Problem aber nicht, so wirft ihm die andere Seite dasselbe vor. In der Zwischenzeit erträgt der Betreiber die unangenehme Situation, in regelmäßigen Abständen erklären zu müssen, weshalb seine Suchergebnisse Desinformationskampagnen zu unterstützen scheinen. Ob diese Vorfälle das Ergebnis einer hinterhältigen Suchmaschinenoptimierung sind oder nicht, ist für den Nutzer fast nie zu erkennen.

Beweise für diese „Black Hat“-SEO-Taktiken finden wir, wenn die Suchergebnisse zu einem bestimmten Nachrichtenthema von Blogs mit ähnlichen und oft extremen Standpunkten dominiert werden, die glaubhaftere Nachrichtenquellen von der ersten Seite verdrängen. Der Content auf jeder Seite ist in der Regel sehr umfangreich und dringt tief in ein bestimmtes Thema ein. Nach der Veröffentlichung wird er in leicht veränderten Formen und mit hoher Frequenz erneut veröffentlicht, damit der Aktualitätsfaktor hoch bleibt. Anschließend verlinken sich eine Reihe koordinierter Domains mit ähnlichen Storys so oft wie möglich miteinander und etablieren eine robuste Backlink-Ökonomie, mit der es andere Storys im kurzen und lärmigen Nachrichtenzyklus kaum aufnehmen können. Die Links werden über soziale Medien und mithilfe von hohen Werbeausgaben aggressiv beworben und drücken die Zahl der Social Media-Links und die CTR nach oben. Ein Beispiel für diese zurzeit sehr beliebte Vorgehensweise ist das koordinierte Posten einer bestimmten URL (oder mehrerer URLs) auf Reddit. Hunderte oder Tausende

67 Siehe: Danny Sullivan, "A deep look at Google's biggest-ever search quality crisis," *Search Engine Land*, 3.4.2017; Olivia Solon und Sam Levin, "How Google's search algorithm spreads false information with a rightwing bias," *The Guardian*, 16.12.2016; Roger Sollenberg, "How the Trump-Russia Data Machine Games Google to Fool Americans," *Paste Magazine*, 1.6.2017.

von Posts aus relevanten Reddit-Sub-Threads werden vom Google-Suchalgorithmus durchforstet und indiziert und können eine Verbesserung in der Ergebnisplatzierung bewirken, ehe Moderatoren von Reddit eingreifen oder Google eine Anomalie feststellt.[68]

Von der technischen Warte aus betrachtet, ist diese Verwebung miteinander verlinkter Aktivitäten zu einem topaktuellen Nachrichtenthema oft erst dann von einem echten Medien-Hype zu unterscheiden, wenn Nutzer anfangen, sich zu beschweren, dass die Suchergebnisse von russischer Propaganda, Verschwörungs-Blogs und anderen Arten von Falschmeldungen dominiert werden.

Als Reaktion auf die regelmäßigen Berichte zu Falschinformationen in Suchergebnissen hat Google versprochen, verstärkte Wachsamkeit beim Aktualisieren seines Algorithmus walten zu lassen, um solche SEO-Söldner zu überlisten. In der Vergangenheit konnte Google bereits sehr erfolgreich gebräuchliche „Black Hat"-Taktiken identifizieren und stilllegen und hat sogar Ranking-Sanktionen für die Nutzer solcher Taktiken eingeführt.[69] Ob diese Sanktionen dauerhaft abschrecken werden, ist ungewiss. In der Zwischenzeit hat der Suchmaschinenbetreiber im Rahmen seiner neuen Initiative „Project Owl" versprochen, Nutzern die Möglichkeit zu geben, problematische Ergebnisse aus der Autovervollständigung (wenn die Suche bei der Eingabe automatisch einen Begriff vorschlägt) oder von Snippets (Content, der auf der Suchergebnisseite als besonders relevant gekennzeichnet wird) zu melden.[70] Daneben hat sich das „Trust Project", eine von Medienforschern und Nachrichtenorganisationen angeführte Initiative, dem Messen und Beschreiben von Vertrauensindikatoren für Nachrichteninhalte verschrieben. Zusammen mit Facebook, Twitter und Google stellt sie die Beschreibungen Nutzern zur Verfügung.[71] Beide Initiativen möchten die Prävalenz von Desinformationen angehen, indem sie Suchergebnisse – basierend auf unterschiedlichen Formen von Nutzereingaben – auf glaubwürdigere und verlässlichere Inhalte

68 Kimberly Coleman, "This is how Redditors Manipulated Google's Image Search Engine," Edgy Labs, 9.12.2016. Diese Technik wurde auch durch SEO-Expert:innen bestätigt.

69 Barry Schwartz, "Unconfirmed Google Algorithm Update May Be Better at Discounting Links and Spam," *Search Engine Land*, 3.2.2017.

70 Ben Gomes, "Our Latest Quality Improvements For Search," The Keyword, 25.4.2017; Danny Sullivan, "Google's 'Project Owl' –a Three-Pronged Attack on Fake News & Problematic Content," *Search Engine Land*, 25.4.2017.

71 Sarah Perez, "Facebook, Google and Others Join The Trust Project, An Efort to Increase Transparency Around Online News," TechCrunch, 16.11.2017.

lenken. Dass Google immer wieder dafür kritisiert wird, bestimmte Ansichten und Perspektiven zu marginalisieren, beweist, wie schwierig es ist, guten von schlechtem Content zu unterscheiden.[72]

Auswirkungen für Desinformationskampagnen

Der Nachweis von gemeldeten Anomalien in Suchergebnissen legt nahe, dass die Suchmaschinenoptimierung bereits als Desinformationstaktik eingesetzt worden ist. Und so lange sie effektiv ist, wird dies wohl auch in Zukunft so sein. Um herauszufinden, wie stark das Phänomen verbreitet ist, und ob es je nach Markt, Sprache oder Thema variiert, sind weitere Untersuchungen erforderlich. Daneben könnte die SEO eine bedeutende Rolle spielen – weniger beim Bewerben von eindeutig falschem Content, sondern vielmehr in der Grauzone zwischen bösartigen Desinformationskampagnen und denjenigen digitalen Medienkanälen, die kommerziell oder politisch von der Bewerbung dieser Storys und Themen profitieren. Diese Sites könnten sich zwar durch Click-Through-Rates und eine Backlink-Ökonomie Glaubwürdigkeit und Beliebtheit erarbeitet haben, aber gelegentlich die Suchmaschinenoptimierung einsetzen – zynischerweise, um Falschinformationen zu propagieren. Auch sollten wir nach Belegen für SEO-Taktiken Ausschau halten, die ähnlich wie Zero-Day-Angriffe [AS5] fungieren, bei denen Hacker bisher unbekannte Lücken in beliebter Software ausnutzen und die Cybersicherheit verletzen. Die Betreiber von Desinformationskampagnen können Möglichkeiten finden, um die Platzierung in Suchergebnissen zu manipulieren. Mit diesem Tool können sie dann eine bestimmte Story während eines Nachrichtenzyklus einmalig pushen, in der Hoffnung, dass die Geschichte viral geht, ehe Google entsprechend reagieren kann. Es sei darauf hingewiesen, dass es quasi keine Interessensüberschneidung zwischen Black Hat-SEO und Google (beziehungsweise Bing oder Yahoo!) gibt. Verzerrte Suchergebnisse wirken sich negativ auf die Suchmaschinenmarke aus, sodass Nutzer andere Alternativen nutzen. Spätestens hier sollten sich Unternehmen mit anderen Stakeholdern zusammentun, um Praktiken, die öffentliche Schäden verursachen, den Garaus zu machen. Der Kampf gegen die Suchmanipulation könnte eine frühzeitige Möglichkeit für eine gemeinsame Strategie über Unternehmensrichtlinien, Medienkonsumforschung und Nutzerbindung hinweg sein.

72 Daisuke Wakabayashi, "As Google Fights Fake News, Voices on the Margins Raise Alarm," New York Times, 26.9.2017.

Social Media Management-Software

Eine neue Generation von digitalen Marketingunternehmen – die Social-Media-Management-Services (SMMS) – stellen die wahrscheinlich vielversprechendste Schnittstelle zwischen Maschinenlernalgorithmen und der Werbetechnologie dar. SMMS bieten Werbetreibenden eine vollständig integrierte Lösung, die Kampagnen mit den unterschiedlichsten Botschaften für unterschiedliche Zielgruppen vorkonfiguriert – sowohl für Standard-Posts in sozialen Medien als auch für bezahlten Content. Die Software setzt auf komplexe Verhaltensdatenanalysen, untersucht soziale Medien mit Listening-Tools in Echtzeit, um zur richtigen Zeit die richtige Botschaft zu platzieren, und wird automatisch und gleichzeitig über diverse Kanäle hinweg koordiniert. Sie testet und lernt, die Überzeugungskraft für jeden investierten Euro beziehungsweise Dollar zu maximieren. Für Werbetreibende ist die Software eine brillante Innovation. Und für den Präzisionspropagandisten ist sie ein fein abgestimmter Desinformationsmotor.

In den vergangenen zehn Jahren ist eine Vielzahl von sozialen Netzwerken entstanden, über die sich Menschen aus aller Welt miteinander verbinden können. Die größte und präsenteste Plattform ist eindeutig Facebook. Aber soziale Netzwerke kommen in vielfältigen Formen und für viele unterschiedliche Personengruppen vor. Auf YouTube kann jeder Videos im Internet teilen und ansehen, Twitter ist die bekannteste Micro-Blogging-Site im Netz und Snapchat hat unter Jugendlichen, die sich über ihren eigenen flüchtigen Messaging-Service austauschen möchten, exponentiell an Beliebtheit gewonnen. Die Liste der führenden Social Media-Websites aber geht weit über diese Handvoll amerikanischer Marken hinaus. Es gibt Dutzende von sozialen Netzwerken und virtuellen Communitys im Internet, die mindestens eine Million Nutzer verzeichnen. Und jede von ihnen bietet eine Plattform an, über die sich Ideen und Inhalte schnell mit anderen austauschen lassen.

Angesichts der Bedeutung und Reichweite von sozialen Medien haben Werbetreibende früh den enormen Wert erkannt, der sich mit gut getimten und gezielten Anzeigenkampagnen über Social Media erzielen lässt. Dabei standen sie aber immer vor einem Problem: Wie kann man effektive Kampagnen über die unterschiedlichsten sozialen Netzwerke gleichzeitig und in Echtzeit managen und dabei möglichst große Wirkung bei möglichst geringen Kosten erzielen?

In den letzten Jahren hat sich eine florierende neue Industrie der Social-Media-Management-Plattformen entwickelt, die Marken bei der komplexen Aufgabe hilft, Anzeigenkampagnen und Content-Sharing über mehrere So-

cial-Media-Kanäle handzuhaben.[73] Angeführt von Marken wie Hootsuite, Sprinklr, Hubspot und Sprout Social, umfasst der Sektor auch Firmen, die Marken beim effektiven Managen ihrer Social-Media-Accounts und dem Koordinieren von Kampagnen unterstützen.

Nehmen wir an, ein globaler Softdrink-Hersteller wie Pepsi möchte eine Marketingkampagne für eine neue Mineralwasserreihe entwickeln. Anstatt sein Marketingteam mit der manuellen Verwaltung seiner einzelnen Accounts in den sozialen Medien wie Facebook, Twitter und Instagram zu betrauen, möchte Pepsi lieber dafür sorgen, dass das Team alle diese Accounts über eine zentrale Schnittstelle managt.

Genau das bieten die Social-Media-Management-Plattformen. Hootsuite beispielsweise ermöglicht seinen Kunden, Content zu erstellen und ihn mit wenigen Klicks über die kommerzielle Web-Anwendung des Unternehmens zu teilen. Dadurch können Marken ihre Marketingbotschaften im Hinblick auf den entwickelten Content, die ausgewählten Plattformen, den Zeitpunkt des Postens und die gewünschte Zielgruppe besser steuern.

Das Management des Social-Media-Accounts eines Kunden beschränkt sich jedoch nicht auf effizientes Teilen oder Bewerben von Inhalten bei den Zielgruppen. Da die Social-Media-Management-Branche immer wettbewerbsfähiger wird und neue Player auf den Markt treten, setzen Plattformanbieter verstärkt auf die Automatisierung ihrer Services, damit Kunden ihre Medienkampagnen mit noch weniger menschlicher Beteiligung vorantreiben können.[74] Bedenklich ist, dass Social-Media-Management-Plattformen jetzt Maschinenlernalgorithmen in die Workflows ihrer Kunden einbinden, um Empfehlungen zu Zielgruppen, Content, Timing und anderen Faktoren zu unterstützen.[75]

Diese Art von Technologie kann enorme kommerzielle Auswirkungen für Marken haben, die eine robuste Marketingkampagne entwickeln möchten. Interessanterweise bieten Social Media Management-Plattformen ihren

73 John Koetsier, "28 Social Media Management Tools, Rated, Scored and Reviewed," *VentureBeat*, 21.4.2015.

74 Rob Marvin und Alyson Behr, "The Best Social Media Management & Analytics Tools of 2017," *PC Magazine*, 1.9.2017.

75 Siehe z.B.: Ciler Ay Tek, "Why Machine Learning Is a Game-Changer for Social Media Managers," *AdWeek*, 8.3.2017; und Barry Levine, "This new AI-powered social marketing tool can predict engagement or write the post for you," MarTech Today, 23.3.2017.

Kunden mittlerweile an, Reichweitenstrategien, die auf bestimmten Ereignissen/Kontingenzen basieren, zu entwickeln. In einem solchen Szenario können Kunden ihre Accounts so einstellen, dass diese ein bestimmtes Anzeigenkonzept oder eine bestimmte Kampagne initiieren, sobald bestimmte Ereignisse eintreten.[76] So könnte eine verbraucherorientierte Marke wie Sprite beispielsweise eine Kontingenz erstellen, um beworbene Anzeigen über ihr Getränk immer dann auszulösen, wenn LeBron James in einem Sprite-bezogenen Hashtag erscheint oder ein Spiel der Cleveland Cavaliers im Fernsehen gezeigt wird.

Im Zusammenhang mit politischer Kommunikation kann dieses Gesamtpaket an Anzeigentechnologien einen erstaunlichen Effekt bewirken. Die Betreiber von politischen Werbekampagnen könnten zunächst versuchen, mithilfe überzeugender Botschaften zur Eignung beziehungsweise Nichteignung eines bestimmten Kandidaten gewisse Online-Zielgruppen zu erreichen. Um zu ermitteln, welche Personengruppen sich online am besten erreichen lassen, könnten die Betreiber persönliche und Verhaltensdaten erfassen. Diese können bei politischen Einrichtungen und Datenmaklern gekauft oder online über alternative Methoden abgegriffen werden. Anschließend können politische Kommunikatoren mit SMMS-Plattformen und ähnlichen Services die unterschiedlichen Zielgruppen nach ihrem demografischen Hintergrund, ihrem Standort und anderen Signalen segmentieren. Mithilfe der SMMS-Plattformen können politische Werber die in diesem Papier beschriebenen Tools miteinander kombinieren, damit der Kommunikator eine überzeugende Kampagne kreieren kann, die Wähler über beworbenen und organischen Content in sozialen Medien wie Facebook und Twitter auf Anhieb anspricht. Daneben können Anzeigen auf YouTube und in der Google-Suche geschaltet werden. Bestimmte Merkmale der SMMS bieten Werbetreibenden zudem die Möglichkeit, kontingenzbasierte, automatisierte Content-Platzierungen zu managen. Dadurch kann der Kunde automatisch eine Online-Anzeigen- und Content-Kampagne starten, sobald ein bestimmtes Ereignis eintritt – zum Beispiel das Statement des US-Präsidenten, ein Statement eines ausländischen Politikers, der Wahlsieg eines Kandidaten oder ein plötzlicher öffentlicher Aufschrei nach einem Verbrechen, das aus Hass begangen wurde („Hate Crime“). Im Laufe der Zeit können die Werbe-

76 Erna Alfred Liousas und Jessica Liu, "Social Media Management Solutions, Q2 2017," The Forrester Wave, 12.6.2017.

treibenden ihr Wissen über die individuellen Nutzerprofile verfeinern, die sie mit Echtzeit-Listening und anderen Online-Diensten verfolgen.

Die modernen SMMS sollten Kunden helfen, eine automatische Antwort auf jede einzelne Kombination der Komponenten in diesem mehrdimensionalen Ereignisraster zu erstellen. Kritischer aber ist, dass diese Services anfangen könnten, Aktionen im Namen des politischen Auftraggebers zu automatisieren, und zwar basierend auf unterschiedlichen politischen Live-Ereignissen. Da der SMMS den Aufwand für den Content der politischen Kampagne permanent verwaltet, könnte der Service beispielsweise frühere Ad-Targeting-Parameter automatisch aufzeichnen und diese dann verfeinern und anpassen, damit sie eine optimale Wirkung erzielen. Zusätzlich könnte der SMMS den Kunden befähigen, weitere Online-Kampagnen durchzuführen, die die Zielgruppe unterschiedlich segmentiert, zum Beispiel mit aggregierten geografischen oder anderen demografischen Datenmerkmalen. SMMS und ähnliche Kundenservices könnten dem Kunden sogar ermöglichen, die subtileren Stimmungslagen der Wähler anhand von Social-Media-Listening-Diensten zu erfassen. Die Services können die internetbasierten Kampagnenreaktionen außerdem automatisch auslösen. Wenn dann viele Menschen beginnen, beispielsweise negative Tweets über den türkischen Präsidenten zu posten, wird die SMMS-basierte Kampagne losgetreten und an die Poster gesendet.

Auswirkungen für Desinformationskampagnen

Am Beispiel der SMMS-Branche zeigt sich ein Aspekt, den wir in diesem Papier mehrfach erwähnen: Nämlich, dass alle diese Werbetechnologien in koordinierte Kampagnen eingebunden werden können, die zur Marketingoptimierung sowohl menschliche als auch maschinelle Informationen nutzen. Auch wenn sich Desinformationskampagnen diese Services bisher noch nicht zunutze machen (oder sie zu internen Zwecken anpassen), ist es nur eine Frage der Zeit. Die zunehmend automatisierte, kontingenzbasierte Natur dieser Managementservices macht sie zu einem perfekten Werkzeug für Desinformationsaktivitäten, die so schnell wie möglich auf aktuelle Ereignisse reagieren müssen, um Nutzer zu einer bestimmten Deutung der Nachrichtenstory zu lenken. Die SMMS können große Mengen an gesammelten Verhaltensdaten verarbeiten, demografische Ad-Targeting-Parameter produzieren und diese verfeinern, sobald neue Besucher durch organischen und beworbenen Content auf der Website landen. Der Service kann gleichzeitig an Facebook, Twitter und YouTube gekoppelt werden und sowohl eigene Da-

tensätze als auch die Anzeigentechnologie-Algorithmen dieser Plattformen einsetzen.

Die Nutzung von Listening-Tools in sozialen Medien, um Stimmungen zu kartieren, das Vorladen von organischer und beworbener Content-Distribution und die Koordination über mehrere Plattformen und Websites, um eine Backlink-Ökonomie zu schaffen, die die SEO antreibt – all das sind die Waffen der Verbreiter von Falschinformationen. Es muss jedoch nochmals darauf hingewiesen werden, dass die Tools per se nicht schlecht sind. Sie sind absolut legal und entsprechen in den meisten Fällen auch den wirtschaftlichen Interessen der Plattformen. Alle Parteien in diesem Ökosystem profitieren in finanzieller Hinsicht von erfolgreichen Werbekampagnen.

Es wurden brillante Tools entwickelt, um Nutzer zu überzeugen. Gleichzeitig wurden einem Missbrauch Tür und Tor geöffnet, der der Öffentlichkeit schadet, indem er die Integrität der Demokratie unterminiert. Beispielsweise könnte ein Agent der russischen Regierung, die einen künftigen US-Wahlkampf unterwandern will, eine Briefkastenfirma gründen, die Anzeigen in sozialen Medien platziert. Über eine intern entwickelte oder über einen Service Provider erworbene SMMS-Plattform könnte der Agent in der frühen Wahlphase bis zum Wahltag selbst die Stimmungen in den sozialen Medien in allen wichtigen US-Wahlkampfbezirken verfolgen. Mit den Plattform-Tools könnte er messen, wie viele Menschen am Wahlabend in jedem Wahlkreis zur Urne gegangen sind. Und schließlich könnte unser Agent eine gezielte Content-Kampagne zur Wählerbeeinflussung in den Wahlbezirken lancieren, in denen noch nicht viele Wähler ihre Stimme abgegeben haben. Es ist zwar unwahrscheinlich, dass die Betreiber von Falschinformationen diese raffinierten Möglichkeiten im Jahr 2016 eingesetzt haben. Doch schon bald könnten sie gut gerüstet für künftige Wahlkämpfe sein.[77]

Fortschritte durch Künstliche Intelligenz

In den vergangenen 25 Jahren hat die digitale Werbebranche einen technologiegesteuerten Wandel durchlaufen. Und auch im kommenden Jahrzehnt werden wir weitere Innovationen sehen, mit denen Werbetreibende, Agenturen und Verleger mehr Gewinne machen – dabei spielt die Wirkung

77 Nitasha Tiku, "Russia's Facebook Ads Will Remain Secret, For Now," *WIRED*, 4.10.2017; Hannah Kuchler, "Facebook says Moscow sought to sow doubt over Trump win," *Financial Times*, 31.10.2017.

der künstlichen Intelligenz (KI) eine ganz wesentliche Rolle.[78] Wie bereits erörtert, beinhaltet das Online-Advertising oft hoch komplexe, kontingenzbasierte Entscheidungsfindungsprozesse, die bestimmen, welcher digitale Content an welche Zielgruppensegmente gesendet wird, falls bestimmte Ereignisse eintreten. Im politischen Kontext verstärkt sich diese Komplexität noch, da individuelle Stimmungen bezüglich politischer Ideen oder Kandidaten häufig besonders beeinflussbar und somit unbeständig sind. Die künstliche Intelligenz und die damit einhergehenden fortschrittlichen Algorithmus-Technologien werden also sehr wahrscheinlich eine wichtige Rolle bei politischen Desinformationen spielen, die über soziale Online-Plattformen propagiert werden.

Wenn es um Künstliche Intelligenz geht, unterscheiden Experten häufig zwischen „starker" und „schwacher" KI.[79] Erstere verdankt ihre Bezeichnung der Tatsache, dass sie sich auf viele Probleme und Situationen anwenden lässt – ähnlich der menschlichen Intelligenz. Ein Beispiel für diese konzeptionelle Form der KI, auch „Artificial General Intelligence" genannt, ist HAL 9000, das KI-System, das das Raumschiff im Film „2001: Odyssee im Weltraum" steuert. Eine so ausgeklügelte KI findet sich bisher nur in Science Fiction Filmen. Die meisten Wissenschaftler und Ingenieure sind überzeugt, dass es noch Jahrzehnte dauern wird, bis sich die starke KI durchsetzt.[80]

Schwache KI dagegen finden wir überall um uns herum. Sie kann in Form von fortschrittlichen maschinellen Lernsystemen auftreten, die in selbstfahrenden Autos, bei Entscheidungen über die Kreditwürdigkeit, das Seiten-Ranking in der Google-Suche und beim Content-Ranking in den News-Feeds sozialer Medien eingesetzt wird. Ein weiterer Bereich, in dem sich die schwache Künstliche Intelligenz durchsetzt, ist die Werbetechnologie.[81]

Die schwache KI hat die Fähigkeit, eine eng gefasste Umgebung zu verstehen, in der Regel mit einem Grad an Erinnerungsfähigkeit und Rechenleistung, der um ein Vielfaches größer ist als menschliche Intelligenz. In Anwendungsbereichen wie der Entscheidung über eine Kreditvergabe kann eine schwache KI, die Maschinenlerntechniken nutzt, im Nu Millionen von früheren Beispielen für ähnliche Entscheidungen analysieren. Anhand dieses

78 Liz Morrell, "IBM Launches AI Online Advertising Offering With Watson Ads," *Marketing Tech News*, 7.6.2016; Richard Oldale, "How AI is Changing SEO," *Marketing Tech News*, 30.6.2017.

79 James D. McCaffrey, "Strong vs. Weak Artificial Intelligence," 26.11.2016.

80 Jack Copeland, "What is Artificial Intelligence?" AlanTuring.Net, Mai 2000.

81 Kris Hammond, "What is Artificial Intelligence?" *Computer World*, 10.4.2015.

Training-Sets lernt sie bemerkenswert schnell, wie sich künftige Kreditwürdigkeitsentscheidungen am effektivsten treffen lassen. Durch eine solche Automatisierung könnte jedwede menschliche Intervention im Kreditvergabeprozess überflüssig werden.[82]

Der Wert einer schwachen KI, einschließlich maschinellem Lernen, erstreckt sich bis tief in die digitale Werbung. In der Regel möchten Marken programmgesteuert die Personen erreichen, die am wahrscheinlichsten auf ihre Produkte oder Botschaften reagieren. Ähnlich möchten Veröffentlichungs- und Customer Engagement-Plattformen wie soziale Medien Marken dabei unterstützen, ihre Anzeigen so schnell und effizient wie möglich zu platzieren. Angesichts der Fülle an persönlichen Daten, die Werbenetzwerken zur Verfügung stehen, der großen Vielfalt an Werbekunden und ihrer Bedürfnisse und des Live-Charakters von digitaler Anzeigenschaltung kann die Künstliche Intelligenz Marken effektiver als jede andere Technologie mit der optimalen Zielgruppe verbinden. Dieser neue Einsatzbereich der KI hat unter Experten und Verbrauchersprechern bereits gewisse ethische Bedenken ausgelöst.[83]

Ein praktisches Beispiel für dieses Gebiet ist die „Digital Ad Mediation", das heißt die Echtzeit-Vermittlung zwischen einem mobilen Herausgeber oder einer Consumer Engagement-Plattform (zum Beispiel die mobilen Apps der New York Times oder von Twitter) und einer Marke, um dem Endbenutzer Werbung anzuzeigen. Unnötig zu erwähnen, dass die Vermittlung angesichts des Content-Volumens und der Milliarden von App-Nutzern am effektivsten über programmatische oder automatisierte Anzeigenschaltungen erzielt wird. Mobile Herausgeber arbeiten normalerweise über eine Reihe von Ad-Netzwerken, um die Anzeigen zu platzieren, die die höchsten Einnahmen garantieren. Der Markt ist so konzipiert, dass die Ad-Netzwerke so viel wie möglich über die Leser des Herausgebers und die Eigenschaften der Marke wissen. Dadurch können sie das aggregierte User Engagement mit den geschalteten Anzeigen maximal kombinieren.[84] Dabei lässt sich leicht beobachten, wie sich das Maschinenlernsystem einer schwachen KI im Laufe der

82 Sean Illing, "Why Not All Forms of Artificial Intelligence Are Equally Scary," *Vox*, 8.3.2017.

83 Jason Jercinovic, "The Ethics of Using AI in Advertising," *AdAge*, 26.6.2017; AMA Triangle, Ethics in Advertising in the AI Age, American Marketing Association, 25.10.2017; Mark MacCarthy, "Ethical principles for algorithms," *CIO*, 13.10.2017; Jonathan Vanian, "How Powerful AI Technology Can Lead to Unforeseen Disasters," *Fortune*, 6.2.2017.

84 VB Staff, "Programmatic Ad Mediation: Stop Sending Your Ad Traffic Over the Waterfall," *VentureBeat*, 21.12.2015.

Zeit trainieren lässt, um optimale Umsätze für die Herausgeber zu erzielen und gleichzeitig die Bedürfnisse der Werbetreibenden zu erfüllen.

Die Ad Mediation kann eine außergewöhnlich hohe Effizienz für die Werbebranche schaffen. Aber die bestehenden Einsatzgebiete der KI gehen noch weiter. Unternehmen untersuchen zunehmend kombinatorische Tests für digitale Anzeigen, damit Werbeagenturen, Herausgeber und Marken verstehen, wie verschiedene Menschen auf Anzeigen reagieren, die sich in Inhalt, Bereitstellungszeitpunkt, Bereitstellungsmedium oder sonstigen Variablen unterscheiden. Zwischen dieser Art der anzeigenrelevanten KI und der von Google entwickelten KI, die erst kürzlich einen Profi-Spieler im Go schlug, gibt es viele Gemeinsamkeiten. Die Go-KI wurde darauf „abgerichtet", unterschiedliche kombinatorische Kontingenzen im Spiel zu untersuchen, indem sie automatisch viele verschiedene Szenarien durchspielte und den nächsten Zug auf Grundlage der Kontingenzmatrix entschied.[85]

Ein weiterer sich rasant ausweitender Use Case für KI in der Anzeigenindustrie sind Lookalike-Zielgruppen: Wie bereits erläutert, ermöglichen soziale Medien ihren Kunden, Nutzerlisten hochzuladen, um eine Zielgruppe für eine Anzeigenkampagne zu kreieren, die in der Regel aus Personen besteht, die sehr wahrscheinlich auch in Zukunft bei der Marke einkaufen werden. Doch Unternehmen wie Facebook ermöglichen zudem das Erstellen von Lookalike-Zielgruppen. Diese bestehen aus Nutzern, die nach Ansicht des Unternehmens Gemeinsamkeiten mit den Nutzern in der ursprünglichen Zielgruppenliste des Kunden haben. Da Social Media-Unternehmen ihre Nutzerlisten auf Ähnlichkeiten in Bezug auf Persönlichkeit und Vorlieben unter verschiedenen Personengruppen durchforsten, liegt es auf der Hand, dass solche Funktionen durch die Integration einer KI-gestützten Analyse und Entscheidungsfindung geradezu exponentiell gefördert werden.

Eine der effektivsten Anwendungen von Künstlicher Intelligenz, die sich immer noch rasant weiterentwickelt, ist der Bereich der Social-Media-Management-Software. In diesem Sektor ermöglichen führende Serviceanbieter wie Hootsuite, Sprinklr und Lithium Technologies ihren Kunden, öffentliche Stimmungen in Bezug auf ihre Marke zu verstehen – oft bis auf lokale Ebene –, Content und Anzeigenkampagnen in eine Warteschlange zu stellen, die mit einem einzigen Klick aktiviert werden kann, und die Stimmungsanalyse in Echtzeit mit vorbereiteten Anzeigenkampagnen abzugleichen. Dadurch kann die Kampagne automatisch veröffentlicht werden, sobald ein be-

85 Cade Metz, "Google's AI Wins Fifth and Final Game Against Go Genius Lee Sedol," *WIRED*, 16.3.2016.

stimmter Vorfall oder ein bestimmtes Ereignis eintritt. Wie bereits erörtert, kann die Künstliche Intelligenz die Effizienz und die Wirkung von Social-Media-Management drastisch erhöhen.

Und ihre Integration endet hier noch nicht. Die Branche entwickelt laufend Innovationen, um die KI in automatisierte Entscheidungsfindungsprozesse einfließen zu lassen, insbesondere in solche, die die zentralen gewinnbringenden Funktionen der Unternehmen, sprich: die Advertising-Technologie, befeuern. Aufgrund der Herausforderungen, die die KI im Hinblick auf Datenschutz und individuelle Autonomie mit sich bringt, hinterfragen viele derartige Integrationsbemühungen. Die führenden Internetfirmen haben Gespräche mit der Zivilgesellschaft über diese Bedenken aufgenommen.[86] Aber Communitys über die inhärenten ethischen Herausforderungen von KI zu informieren und diese Gruppen in die Diskussion um mögliche Lösungen einzubinden, bedeutet massive öffentliche Aufklärungsarbeit.

Auswirkungen für Desinformationskampagnen

Die rasanten Fortschritte der KI-Entwicklung überfrachten die digitale Anzeigenbranche. Techniken, die es seit vielen Jahren gibt, sind jetzt viel effektiver und skalierbarer. Die Künstliche Intelligenz wird die Dominanz des digitalen Werbeindustrie gegenüber den übrigen Medienkanälen zementieren. Dadurch wird sich die politische Werbung im Internet deutlich ausweiten. Die Entwicklungen im Hinblick auf eine zielgenaue Wähleransprache werden von Wahlzyklus zu Wahlzyklus drastische Fortschritte machen. Und damit wird auch die besorgniserregende Macht der Desinformationskampagnen zunehmen. Im Kern ist die Vermählung von Anzeigentechnologie und politischer Propaganda nichts weiter als das Einsetzen von Branchentools – Verhaltensdatenanalyse, Zielgruppensegmentierung und maßgeschneidertes und zielgenaues Platzieren von Botschaften – mit dem Ziel, sich Vorurteile zunutze zu machen. In jeder Phase dieses Prozesses wird die Künstliche Intelligenz für weitere Fortschritte sorgen. Diese Aussichten führen zu der Frage, was getan werden kann oder soll, um diesem Trend Einhalt zu gebieten – oder zumindest die negativen Folgen für das öffentliche Interesse einzudämmen.

86 Siehe z.B. die Partnerschaft im Bereich der Künstlichen Intelligenz des AI NOW Institutes.

Fazit

Die vorliegende Analyse der Digital-Advertising-Technologien und ihre Relevanz für die Verbreitung von Desinformation im Internet soll den Fokus in der aktuellen öffentlichen Debatte vergrößern – und zwar weit über russische Agenten, die Online-Kampagnen in den sozialen Medien betreiben, hinweg. Denn die Probleme sind sehr viel weitreichender und geben aus unterschiedlichen Gründen Anlass zur Beunruhigung. Unsere Analyse verweist auf die zentrale Herausforderung: die Entwirrung der Interessensüberschneidungen zwischen den kommerziellen Bestrebungen digitaler Plattform-Betreiber und dem Erfolg von auf Falschinformationen setzenden politischen Werbetreibenden.

Es wäre ein Fehler, sich allein auf Russland zu konzentrieren. Russland ist nur einer von vielen Betreibern von Online-Desinformation, die US-Bürger im Visier haben. Zukünftige Desinformationskampagnen könnten genauso gut von inländischen wie von anderen ausländischen Akteuren durchgeführt werden. Dabei werden sie höchstwahrscheinlich die vorherrschenden US-Internetplattformen nutzen, um zehn bis hundert Millionen Amerikaner zu erreichen. In ihrer vollen Tragweite könnten diese Desinformationskampagnen zu einem schweren öffentlichen Schaden führen. Insbesondere können sie die Integrität unserer Demokratie peu à peu schwächen, indem sie Bürger von Fakten fernhalten und unsere politische Kultur polarisieren.

Die nächste Generation der Desinformationsbetreiber wird ein robustes Digital-Advertising-Toolset nutzen, um ihre Ziele zu erreichen. Um zu verstehen, wie dies funktioniert, bedarf es einer sorgfältigen Analyse der in der digitalen Werbeindustrie vorherrschenden Praktiken und Technologien. Das geht weit über das Kaufen von Anzeigen auf Facebook, YouTube und Twitter hinaus. Die wahre Macht des Advertising Technology-Markts liegt in einer Kombination aus Tools, die diese Online-Kampagnen vorbereiten und ausweiten. Es fließen große Anstrengungen in die Erfassung von Verhaltensdaten, um Zielgruppen präzise zu segmentieren und ihnen eine Bandbreite von unterschiedlichen Botschaften zukommen zu lassen, die am wahrscheinlichsten eine Reaktion hervorrufen. Die Datenanalyse ist der Raketentreibstoff für die gezielte Anzeigenplatzierung auf Social-Media-Plattformen und in der breiteren Digital-Marketing-Industrie. Die Datenanalyse und das Targeting

werden zunehmend von Algorithmen übernommen, die auf maschinellem Lernen basieren und immer ausgeklügelter werden.

In der Zwischenzeit werden die Kampagnen zwar noch von Marketingbetreibern entwickelt, aber von Künstlicher Intelligenz implementiert und optimiert. Diese Technologie entwickelt sich in rasantem Tempo und wird immer effektiver, wenn es um das Identifizieren, Targeting und Überzeugen von Zielgruppen geht. Die KI-gestützte Welt ermöglicht es einzelnen Betreibern, Desinformationskampagnen zu realisieren, die mit einer Echtzeit-Stimmungsanalyse in sozialen Medien, automatisierter Content-Verteilung über diverse Kanäle durch organische Posts und Anzeigenschaltung und kontingenzbasierten Reaktionen auf aktuelle Ereignisse einhergehen. Und dazu kommt noch das Potenzial von „Black Hat"-SEO, eine Story oder ein Thema durch das Grundrauschen der sozialen Medien zu pushen und dafür zu sorgen, dass es viral geht.

Leider bedeutet das Zusammenfließen von KI-gesteuerter Technologie und Advertising-Praktik, dass selbst schlecht umgesetzte Desinformationskampagnen funktionieren, da sie von ähnlichen, besseren Kampagnen profitieren, die die Algorithmen trainiert haben. Es ist nicht unwahrscheinlich, dass die russische Desinformationskampagne trotz mittelmäßiger handwerklicher Fähigkeiten erfolgreich war. Die Targeting-Bemühungen waren Berichten zufolge wenig ausgeklügelt: Die Akteure haben sich schlicht und einfach die grundlegenden Tools der heutigen Informationsmärkte zunutze gemacht, mit denen gezielte, überzeugende Botschaften für wenig Geld und wenig transparent an Millionen von Menschen gesendet werden können. Außerdem profitierten sie von der Tatsache, dass eine Reihe anderer inländischer, politischer Akteure Ähnliches tat – nämlich bezahlten und unbezahlten Content in den sozialen Medien zu schalten, um anzügliche, spaltende oder emotional manipulative politische Botschaften zu bewerben. Wenn sich das KI-gestützte Zielgruppen-Targeting erst einmal auf eine erfolgreiche Kombination aus demografischen Daten, Botschaften und Nutzerverhalten eingeschossen hat, wird es ganz selbstverständlich alle ähnlichen Inhalte in dieselbe Richtung lenken. Diese Plattformökonomien sind dazu gedacht, Werbung im Internet zum Erfolg zu verhelfen.

Desinformationskampagnen unterscheiden sich praktisch kaum von anderen Advertising-Kampagnen und die führenden Internetplattformen sind mit erstklassiger Technologie ausgestattet, damit Werbetreibende ihre Zielgruppen erreichen und beeinflussen können. So läuft das Geschäft. Deshalb gehen die wirtschaftlichen Anreize der Plattformen und die politischen Ziele der Betreiber von Desinformationskampagnen Hand in Hand. Wenn wir Fort-

schritte erzielen möchten, müssen wir diese politisch-wirtschaftliche Verknüpfung an ihrer Wurzel anpacken.

Abschließend bieten wir einige übergeordnete Prinzipien, die in unseren Augen als Leitfaden für die vor uns liegende Arbeit dienen sollten. Wir sind überzeugt, dass in einer Ära der algorithmusbasierten Desinformation eine Kombination aus neuer Unternehmenspolitik, öffentlichen Gesetzen, Nutzererwartungen und gesellschaftlichen Normen helfen kann, dieses Problem zu lösen. Darüber hinaus schlagen wir eine vorläufige Orientierungshilfe für behördliche Untersuchungen der digitalen Anzeigentechnologie vor. Dabei handelt es sich um exploratorische Schlussfolgerungen in einem Bereich, in dem erhebliche technische Forschung und rechtliche Analysen erforderlich sind. Wir planen, in den kommenden Monaten weitere Analysen zu veröffentlichen, die auf der hier vorgestellten Problemdarstellung basieren und detailliertere Vorschlägen anbieten. Im Rahmen dieses Fazits behalten wir uns vor, eine übergeordnete Struktur für die nächste Arbeitsphase anzubieten. Einige dieser Ideen spiegeln sich in aktuellen Bemühungen wider und wurden von anderen Analysten und Beobachtern aufgegriffen.[87] Wir glauben, dass die Herausforderung enorm ist. Deshalb muss unsere Antwort entsprechend ambitioniert ausfallen – von den Fluren im Weißen Haus über die obersten Führungsetagen im Silicon Valley bis zu den Mobilgeräten der Internetnutzer.

- **Transparenz**: Wir müssen ein genaues und umfassendes Transparenzsystem für die politische Online-Werbung entwickeln, das nicht lediglich auf Gleichstellung mit alten Technologien ausgelegt ist, sondern die Bedürfnisse und Anforderungen einer digitalen öffentlichen Sphäre erfüllt. Dabei gilt es, mindestens drei Transparenzblickwinkel zu berücksichtigen: wie politische Werber Inhalte für die Offenlegung gegenüber Sponsoren kennzeichnen, wie Nutzer nach bekannten Desinfomation informiert werden und wie Plattformen Informationen über politische Werbung (zum Beispiel Sponsor, Ausgabenhöhe und Targeting-Parameter) zur Verfügung stellen. Weitere Untersuchungen könnten versuchen, aktuelle Vorschläge zur Kennzeichnung politischer Werbung in den digitalen Medien zu verfeinern. Wichtiger aber ist, dass wir prüfen sollten, inwiefern Plattformunternehmen ihre Zusicherung zur Erstellung einer durch-

87 Claire Wardle and Hossein Derakhshan, Information Disorder: Toward an interdisciplinary framework for research and policy making, Council of Europe, 27.9.2017; Alice Marwick und Rebecca Lewis, "Media Manipulation and Disinformation Online," Data & Society; Kelly Born und Nell Edgington, Analysis of Philanthropic Opportunities to Mitigate the Disinformation/Propaganda Problem, William and Flora Hewlett Foundation, Herbst 2017; und Anamitra Deb, Stacy Donohue, und Tom Glaisyer, "Is Social Media a Threat to Democracy?" Omidyar Group, Oktober 2017.

suchbaren Datenbank zu digitalen Anzeigen mit Informationen über Sponsoring und Targeting einhalten, um zu bestimmen, wie effektiv sie schlechtes Verhalten eindämmen kann.[88] Über freiwillige Transparenzmaßnahmen hinweg allerdings müssen alle Vorschläge zu einer verpflichtenden Transparenz hinsichtlich des First Amendment und möglicher Bedenken zur Meinungsfreiheit abgeglichen werden.

- **Sicherheit**: Obwohl die Cybersicherheit in der Desinformationsdiskussion keine prominente Rolle spielt, sollte sie als wesentlicher Bestandteil der Lösung betrachtet werden. Häufig treten Falschmeldungen und Cyberangriffe gemeinsam auf. Hacker knacken E-Mail-Konten oder sensible Dateien und spülen deren Inhalte in die Medien – oft vermischen sich dabei Wahrheit und Lüge. Wenn sensible Daten ungeschützt sind und Bürger sich nie sicher sein können, ob sich Desinformationskampagnen auf wahre aber entwendete Geheimnisse oder lediglich auf erfundenen Unsinn beziehen, kommen wir aus dieser Krise nicht so einfach heraus. Außerdem haben wir keine klaren Normen, wie Herausgeber, Plattformen und Verbraucher digitale Werbung behandeln sollen, die diese Art von Informationen verbreitet.

- **Aufklärung der Öffentlichkeit**: Einen nicht geringen Anteil an der Dysfunktion in unserem politischen Mediensystem hat die begierige Nachfrage nach schlüpfrigen, spaltenden und überzogenen Inhalten. Wenn es um die Nachfrage der Verbraucher geht, übertrumpft der Wunsch nach Unterhaltung die Aufgeklärtheit der Gesellschaft. Aber wir können mehr tun, um den Wert eines gut informierten Gemeinwesens in unserem Bildungssystem zu priorisieren, den Taktiken der Desinformation durch Projekte zu digitaler Kompetenz entgegenzuwirken und Plattformnutzern technische Optionen zur Hand zu geben, um einen gesünderen Umgang mit Informationen zu pflegen. In diesen Bereichen beobachten wir zahlreiche Initiativen und Anstrengungen.[89] Die besten Ergebnisse sollten bekannt und für ein möglichst großes Publikum aufbereitet werden.

- **Journalismus im Dienste der Öffentlichkeit**: Unser Mediensystem hat sich nicht über Nacht entwickelt. Es war ein jahrzehntelanger Prozess, bei dem der objektive Journalismus im Dienste der Öffent-

88 Facebook hat im Vorfeld der US-Wahlen 2018 vorgeschlagen, eine durchsuchbare Werbedatenbank zu erstellen. Außerdem haben sie ein Tool zur Verfügung gestellt, mit dessen Hilfe man einsehen kann, ob man während des Wahlkampfs 2016 russischen Desinformationskampagnen ausgesetzt war.

89 Siehe z.B.: Jason Horowitz, "In Italian Schools, Reading, Writing and Recognizing Fake News," *New York Times*, 18.10.2017; Lindsay Stein, "The News Literary Project, JWT Team Up to Combat Fake News," *AdAge*, 10.4.2017; und Sophia Boyd, "5 Ways Teachers Are Fighting Fake News," *NPR*, 16.2.2017.

lichkeit weniger wurde und durch Infotainment ersetzt wurde.[90] Diesen Trend gilt es, umzukehren. Teil eines solchen Projekts ist es, die Rolle der Anzeigentechnologie kritisch zu betrachten, wenn es um die Verschiebung der Umsätze aus dem traditionellen Nachrichtengeschäft geht.[91] Zudem beinhaltet diese Aufgabe den gemeinsamen Versuch, global und lokal einen Journalismus aufzubauen und zu pflegen, der nicht vollständig vom Anzeigengeschäft abhängt. Einen Anfang macht die Unterstützung der vielen Bemühungen, mehr kommunale Nachrichtenredaktionen aufzubauen. Und ein ganz besonderer Schwerpunkt sollte auf der investigativen Berichterstattung liegen.

- **Unternehmerische Verantwortung**: Die führenden Internetplattformen haben auf diese Krise mit einer Reihe von freiwilligen Maßnahmen zur Eindämmung von Falschinformationen reagiert. Dazu gehören eine transparente Anzeigendatenbank, eine verstärkte menschliche Prüfung von Online-Kampagnen und die Unterstützung von Initiativen zur Medienkompetenz. All diese Anstrengungen sollten fortgeführt werden. Zudem könnte man sich darauf konzentrieren, den Nutzern Tools zur Verfügung zu stellen, mit denen sich die Vertrauenswürdigkeit von Content überprüfen lässt, um Themen aus unterschiedlichen Perspektiven zu beleuchten und Desinformation zu melden.

- **Empowerment der Verbraucher**: Dass Verbraucherdaten im Zentrum von Desinformationskampagnen stehen, wirft die Frage auf, wie wir Verbraucher befähigen können, mehr Transparenz und Kontrolle darüber zu erhalten, welche Daten erfasst werden, wie diese eingesetzt werden und wie auf diesen Daten basierenden Content in den sozialen Medien sehen. Man könnte Verbrauchern beispielsweise die Option bieten, die vom Algorithmus priorisierten Signale anzupassen, um den News-Feed in einem sozialen Netzwerk zu gestalten. Oder man könnte ihnen ermöglichen, den sequenziellen Ablauf von Posts ihrer Social Media-Kontakte zu sehen, ohne dass der Algorithmus eingreift.

Auf dem Weg zu einer neuen politischen Wirtschaft für digitale Medien

Die schlichte Tatsache, dass Desinformationskampagnen und rechtmäßige Werbekampagnen auf den führenden Internetplattformen quasi nicht voneinander zu unterscheiden sind, steht im Mittelpunkt der Herausforderung.

90 Roy Greenslade, "Almost 60% of US newspaper jobs vanish in 26 years," T*he Guardian*, 6.6.2016.

91 Siehe Robert Kaiser, The Bad News About the News, Brookings Institution, 16.10.2014.

Sie nutzen dieselben Technologien, um Menschen zu beeinflussen, und erreichen mit gezielten Botschaften einen Anteil auf dem nationalen Markt, der bei bisherigen Medienformen undenkbar gewesen wäre. Doch wenn der Markt auch weiterhin die Interessen der Aufmerksamkeitsökonomie mit den Zielen politischer Desinformationskampagnen auf eine Linie bringt, wird es ein harter Kampf. Der Weg in die Zukunft besteht darin, effektive Wege zu finden, um die Ausnutzung persönlicher Daten – sprich: aus dem Online-Verhalten gewonnene soziale Profile – zum Zwecke der Präzisionspropaganda und der Isolation und Manipulation von Zielgruppen durch kommerzialisierte politische Falschmeldungen zu begrenzen. Möglichkeiten hier wären Einschränkungen bei der Datenerfassung, Regeln zur Nutzung der Datenerfassung sowie Maßnahmen zur Steigerung der Verbrauchertransparenz und -kontrolle. Unsere Aufgabe besteht darin, einen Kurs zu einem neuen gesellschaftlichen Pakt mit der Technologie festzulegen. Die Technologien der Präzisionspropaganda unterscheiden nicht zwischen Kommerz und Politik. Aber Demokratien tun dies sehr wohl.

Es gibt keine einfachen Antworten oder historische Vergleiche. Doch die politische Widerstandsfähigkeit der USA hat sich immer schon in unserem stillschweigenden Bekenntnis begründet, dass Märkte gegenüber der Demokratie in den Hintergrund treten müssen. Um dieses Ziel zu erreichen, braucht es eine Kombination aus neuen Richtlinien und Unternehmenspraktiken, neuen technischen Produktfunktionen, öffentlicher Aufklärung, Datensicherheit und Bürger-Empowerment.

Über die Stiftung Neue Verantwortung

Think Tank für die Gesellschaft im technologischen Wandel

Neue Technologien verändern Gesellschaft. Dafür brauchen wir rechtzeitig politische Antworten. Die Stiftung Neue Verantwortung ist eine unabhängige Denkfabrik, in der konkrete Ideen für die aktuellen Herausforderungen des technologischen Wandels entstehen. Um Politik mit Vorschlägen zu unterstützen, führen unsere Expertinnen und Experten Wissen aus Wirtschaft, Wissenschaft, Verwaltung und Zivilgesellschaft zusammen und prüfen Ideen radikal.

Über die Autoren

Dipayan Ghosh

Ghosh ist Fellow bei "New America" in Washington, D.C. und Joan Shorenstein Fellow am Shorenstein Center on Media, Politics and Public Policy der Harvard Kennedy School, wo er sich mit digitaler Privatsphäre, Künstlicher Intelligenz und Bürgerrechten beschäftigt. Er ist ausgebildeter Informatiker und hat bis vor Kurzem bei Facebook zu Global Privacy und Public Policy-Themen gearbeitet. Zuvor war Ghosh Berater des Weißen Hauses der Obama Administration im Bereich Technologie und Wirtschaft. Er war am Office of Science & Technology Policy und dem National Economic Council angestellt, wo er den Einfluss von Big Data auf die Privatsphäre von Verbraucher:innen untersucht hat. Er wurde an der Cornell Univeristy in Elektrotechnik und Informatik promoviert und erhielt seinen Bachelorabschluss von der University of Connecticut.

Ben Scott

Ben Scott ist Mitglied des Vorstands der Stiftung Neue Verantwortung und Teil des Führungsteams des Think Tanks. Zuvor arbeitete er als Innovationsberater im Stab der amerikanischen Außenministerin Hillary Clinton. Dort war er verantwortlich für den Umgang mit neuen Technologien und sozialen Netzwerken als Teil der US-Diplomatie. Vor seiner Zeit im US-Departement of State leitete er das Washington Büro von Free Press, einer Non-Profit Organisation die sich vor allem mit Medien und Kommunikationspolitik beschäftigt. Ben Scott promovierte an der University of Illinois. 2016 engagierte er sich ehrenamtlich als Experte für die politischen Fragen der Digitalisierung im Team der Präsidentschaftskandidatin Hillary Clinton.

Impressum

Stiftung Neue Verantwortung e. V.

Beisheim Center
Berliner Freiheit 2
10785 Berlin

T: +49 (0) 30 81 45 03 78 80
F: +49 (0) 30 81 45 03 78 97

www.stiftung-nv.de
info@stiftung-nv.de

Design:
Make Studio
www.make-studio.net

Layout:
Johanna Famulok

Free Download:

www.stiftung-nv.de