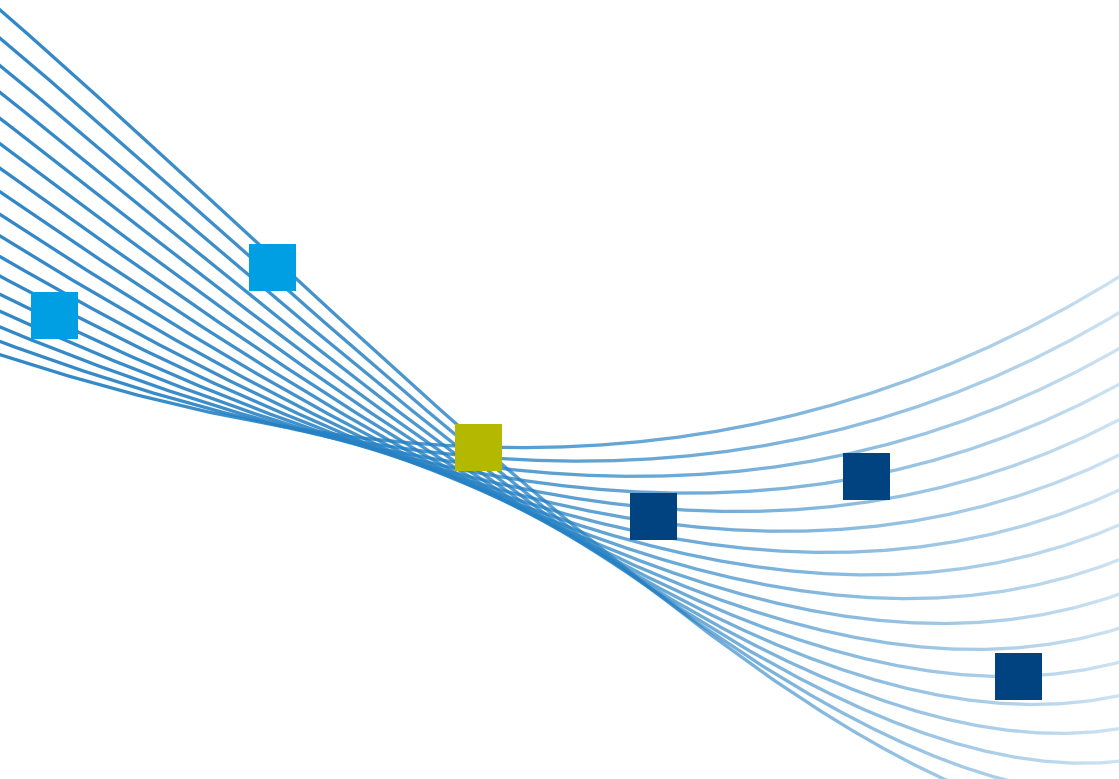
Konrad Adenauer Stiftung

Tim Hwang

Digitale Desinformation

GRUNDLAGEN



Tim Hwang

Digitale Desinformation

GRUNDLAGEN

Eine Veröffentlichung der Konrad-Adenauer-Stiftung e.V.

Herausgeberin:
Konrad-Adenauer-Stiftung e.V. 2017, Sankt Augustin/Berlin

Gestaltung und Satz: Janine Höhle, KOM/Konrad-Adenauer-Stiftung.
Die Printausgabe wurde bei der Druckerei Kern GmbH, Bexbach, klima-neutral produziert und auf FSC-zertifiziertem Papier gedruckt.
Printed in Germany.
Gedruckt mit finanzieller Unterstützung der Bundesrepublik Deutschland.

ISBN 978-3-95721-377-8

Vorwort

Daphne Wolter und Nico Lange

Presse- und Meinungsfreiheit sind grundlegende Voraussetzungen für die Funktionsfähigkeit einer Demokratie. In Deutschland und in den meisten Ländern Europas gehören Medienfreiheit und Medienvielfalt zu den Selbstverständlichkeiten einer demokratischen Gesellschaft.

Journalismus hat eine öffentliche Funktion und ist ein wichtiges Bindeglied zwischen Politik und Bevölkerung. Medien und Demokratie funktionieren aber nur mit einem unabhängigen professionellen Journalismus: Für einen offenen Meinungs- und Willensbildungsprozess braucht die Gesellschaft Medien, die aus verlässlichen Quellen Sachverhalte und Werte glaubwürdig vermitteln, erklären und einordnen. Die besondere Bedeutung der klassischen Medien bei der politischen Willensbildung wird jedoch geringer. Gleichzeitig befinden sich die sozialen Netzwerke in einem postfaktischen Zustand. Die Selektion durch Algorithmen anhand des Kriteriums der größtmöglichen Aufmerksamkeit statt anhand der gesellschaftlichen Relevanz, gefährdet die wichtige Filterrolle von Presse und Rundfunk.

Die fortschreitende Disruption der Meinungsbildung kann jedoch auch als eine Chance für das Entstehen neuer Formen der politischen Debatte gesehen werden. Die Entwicklung einer neuen Infrastruktur für die politische Debatte hängt eng mit dem Wechselverhältnis von Mediennutzern und Meinungsmachern zusammen. Die große Herausforderung für beide Akteure wird sein, zu lernen und analysieren, wie Versuche der digitalen Desinformation schneller erkannt werden können. Hierbei muss die Vermittlung der digitalen Medienkompetenz gesellschaftspolitisch eine noch größere Rolle erlangen.

Enthüllungen zu russischen Versuchen, durch den Einsatz von Bots, Falschmeldungen und Hacks die US-Präsidentschaftswahl im Jahr 2016 oder die französische Wahlen 2017 zu beeinflussen, haben das Problem der „Fake News" und der Manipulation sozialer Medien in den Blickpunkt der Öffentlichkeit gerückt.

Das vorliegende Papier ist eine Einführung zu diesem Phänomen, in dem Schlüsselbegriffe, Hauptakteure und mögliche Maßnahmen der Politik vorgestellt werden.

Der nachfolgende Text erschien ursprünglich in englischer Sprache in den USA und wurde in Kooperation mit dem Atlantic Council verfasst. Die vorliegende Anpassung für den deutschen Markt erfolgte in Zusammenarbeit des Auslandsbüros der Konrad-Adenauer-Stiftung in Washington und der Hauptabteilung Politik und Beratung in Berlin. Das englischsprachige Original ist unter http://www.kas.de/usa/en/publications/50251/ abrufbar.

Schlüsselbegriffe

Künstliche Intelligenz (KI)/Artificial Intelligence (AI)
Umgangssprachlich der Bereich der Informatik, der sich mit der Entwicklung von Maschinen befasst, die kognitive Funktionen nachahmen können.

Social Bot
Im Zusammenhang mit sozialen Medien ein Nutzerkonto, das autonom von einer Software kontrolliert wird. Diese Konten erwecken oftmals den Eindruck, dass es sich dabei um echte Nutzer sozialer Medienplattformen wie Twitter oder Facebook handle. Durch ihr massenhaftes Auftreten können sogenannte Botnetze Trends manipulieren.

Rechnergestützte Propaganda
Verwendung von Algorithmen, Automatisierung und Instrumentalisierung von Menschen („Human Curation") zur willentlichen Verbreitung von Falschinformationen in sozialen Netzen.

Desinformation
Vorsätzliche Aktionen von Individuen oder Gruppen, die – wissentlich oder unwissentlich – zur Verbreitung falscher oder irreführender Informationen führen.

Echokammer
Soziale Räume, in denen Ideen, Annahmen und Auffassungen in einer Gruppe ähnlich gesinnter Mitglieder ständig wiederholt und verstärkt werden.

Meme
Entstehen aus Bildern, Videos, Blogs, Texten oder ganzen Webseiten, die sich wie Lauffeuer über das Internet verbreiten. Die Intention der Urheber ist neben Unterhaltung und Werbung immer häufiger auch politische Propaganda.

Maschinelles Lernen
Teilbereich der künstlichen Intelligenz, der sich mit Systemen befasst, die sich anhand von Daten selbst verbessern und weiterentwickeln. Jüngste Erfolge auf diesem Feld haben die Begeisterung für die künstliche Intelligenz erhöht. Beide Begriffe werden im täglichen Sprachgebrauch oft synonym verwendet.

MADCOM
Maschinengestützte Kommunikation (Machine driven communications). Die Nutzung von Techniken der KI und des maschinellen Lernens zur Erstellung von Text-, Audio- und Videoinhalten, mit dem Ziel vor allem Informationen online zu verbreiten.

Metadaten
Daten, die andere Daten beschreiben. Die Analyse von nutzergenerierten Metadaten auf Online-Plattformen ist für Anzeigenkunden, Forscher und die Plattformen selbst zu einem wichtigen Faktor für das Verständnis des Verbraucherverhaltens geworden.

Plattform
In diesem Zusammenhang Unternehmen, die über Onlinedienste verfügen und diese betreiben, wozu üblicherweise die Bereitstellung und gemeinschaftliche Verwendung nutzergenerierter Inhalte gehört (z.B. Facebook, Twitter, Instagram) sowie die Verwaltung von Inhalten Dritter, die vom Nutzer aufgerufen werden können (z.B. Google).

Kollektive Intelligenz
Auffassung, dass die zusammengefassten Beobachtungen von Nutzern dabei helfen können, Ungenauigkeiten und Fehler zu beheben. Es wird unterstellt, dass sich bei einer ausreichenden Nutzerzahl der nutzergenerierte Inhalt einer Plattform im Wesentlichen selbst nach vertrauenswürdigen Informationen filtert. Die Gestaltung verschiedener Plattformen – wie etwa Twitter und Reddit – orientiert sich an diesem Konzept.

Warum ist Desinformation ein wichtiges Thema?

Was vor ein paar Jahren noch prophezeit wurde, etabliert sich immer mehr als Trend: Die politische Meinungsbildung erfolgt zunehmend im Netz. Die deutsche Medienlandschaft ist zwar nach wie vor stark. In ihrer großen Mehrheit stammen Nachrichten, die auf Social Media-Plattformen verbreitet werden, noch von etablierten Medienhäusern oder Nachrichtenagenturen. Doch in den USA ist die Sachlage bereits anders: Fast 60 Millionen Amerikaner haben in den vergangenen zwei Jahren das Internet dafür genutzt, „wichtige Entscheidungen zu treffen oder sich in wichtigen Lebensfragen zu orientieren."[1] Es ist zunehmend der Kanal, über den Informationen verbreitet und aufgenommen werden. Da das Internet eine Quelle für Informationen zum Weltgeschehen geworden ist, der viele vertrauen, können wirksame Manipulationen durch böswillige Akteure Meinungsbilder formen und demokratische Prozesse, Märkte und die Stabilität eines Landes bedrohen. In den vergangenen Jahren haben Forscher und Journalisten festgestellt, dass genau das von einer Anzahl verschiedener internationaler Akteure versucht wird.

Es sollte nicht unterschätzt werden, dass breit angelegte Desinformationskampagnen unabhängig von ihrer Wirksamkeit zersetzend sein können. Indem sie das Vertrauen in Informationen allgemein erschüttern, können solche Kampagnen auch die Glaubwürdigkeit vertrauenswürdiger Online-Informationsquellen beeinträchtigen. Damit kann Desinformation die Fähigkeiten von Journalisten untergraben, für Verlässlichkeit und Transparenz in der Gesellschaft zu sorgen.

1| *John B. Horrigan und Lee Rainie, The Internet's Growing Role in Life's Major Moments, http://www.pewinternet.org/2006/04/19/the-internets-growing-role-in-lifes-major-moments/.*

Wichtige Akteure

Obwohl die Bedrohung durch Desinformation auch die öffentliche Wahrnehmung, die Massenmedien und viele andere Faktoren betrifft, sind es Internetplattformen, die eine Schlüsselrolle dabei spielen, wie mit diesen Kampagnen Botschaften verbreitet werden. Einige davon sind für die Öffentlichkeit besonders wichtig:

Twitter

Gegründet 2006. Twitter ist ein Online-Nachrichtenportal und soziales Netzwerk, in dem Nutzer auf maximal 280 Zeichen beschränkte Botschaften („Tweets") einstellen und damit interagieren können. Nur registrierte Nutzer können Tweets einstellen, aber die meisten können online von jedermann gelesen werden.

Facebook

Gegründet 2004. Die Nutzer erstellen Profile, auf denen Name, Beruf, Bildungsweg und weitere Informationen genannt werden können. Sie vernetzen sich mit anderen Nutzern, stellen Statusmeldungen und Bilder ein und teilen Videos und Nachrichten. Mit dem Newsfeed – ein Kernstück von Facebook – wird diese Tätigkeit im Rahmen eines Netzwerks von „Freunden" automatisch betreut.

Google

Gegründet 1998. Bekannt vor allem durch seine Suchmaschine, die relevante Inhalte im Netz als Antwort auf Anfragen anzeigt. Google bietet eine Palette an Internet-Dienstleistungen, zu denen auch die Verwaltung nutzergenerierter Videos gehört (YouTube) sowie ein Dienst, der durch Algorithmen Nachrichten aus dem Web sammelt (Google News).

Reddit
Gegründet 2005. Reddit ist eine Seite, auf der Nachrichten zusammengestellt und diskutiert werden. Registrierte Reddit-Nutzer können Inhalte, wie Texte oder Bilder, einstellen und Links zu externen Quellen einschließlich Videos setzen. Die Nutzer stimmen dann darüber ab und erstellen so eine Liste „heißer" Inhalte auf der Eingangsseite des Portals.

Instagram
Gegründet 2010. Instagram ist eine Anwendung, die es Nutzern ermöglicht, nutzergenerierte Fotos und Videos zu teilen, zu kommentieren und zu nutzen. Die App unterstützt auch die Bearbeitung dieser Inhalte durch digitale Filter, die das Aussehen von Bildern verändern. 2012 wurde die Plattform von Facebook erworben.

Snapchat
Gegründet 2011. Snapchat ist eine Plattform zum Nachrichtenaustausch, die es Nutzern ermöglicht, Bilder und Videos mit Beschriftung zu teilen, die nur kurze Zeit abrufbar sind und dann „verschwinden". Die Plattform unterstützt auch das Teilen und Entdecken im Bereich von „Stories", also Bildersammlungen, die eine kurze Geschichte ergeben.

Schwachstellen und Beschränkungen

Plattformen sind in vierfacher Hinsicht eingeschränkt, woraus sich eine ständige Anfälligkeit für Desinformationskampagnen ergibt und eine wirksame Gegenwehr verhindert wird:

Ideologische Beschränkungen

Viele Plattformen lassen den Nutzern weitgehend freie Hand, was den Wahrheitsgehalt von Inhalten auf ihren Seiten angeht. Dies beruht auf dem grundlegenden Glauben an die freie Meinungsäußerung und die „kollektive Intelligenz". Dazu gehören Unternehmer wie Twitter-Mitbegründer Ev Williams, der sagte, die Grundidee der Plattform sei, dass „die Welt automatisch besser wird, wenn sich alle frei äußern und Informationen und Ideen austauschen können"[2], sowie Facebook-Mitbegründer Mark Zuckerberg, der 2016 anmerkte, sein Unternehmen müsse „extrem vorsichtig dabei sein, selbst über Wahrheit oder Unwahrheit zu befinden."[3] Auch die Gestaltung von Plattformen wie Reddit, deren Inhalte je nach Zustimmung oder Ablehnung der Nutzer verwaltet werden, beruht auf diesem Prinzip.

Technische Beschränkungen

Zur Schaffung einer wirksamen Abwehr gegen Online-Desinformation bedarf es einer Lösung, die rasch und maschinell auf Millionen und Milliarden von täglich durch Nutzer hochgeladene Inhalte angewendet werden kann. Falsche oder irreführende Informationen können jedoch in vielerlei Gestalt auftreten, und Nutzer mögen unterschiedlicher Ansicht darüber sein, was „wahr" ist. Das macht die Erstellung eines allgemeinen Filters für Desinformation zu einem technisch schwierigen Unterfangen.

2| *David Streitfeld, „The Internet is Broke: @ev is Trying to Save It", https://www.nytimes.com/2017/05/20/technology/evan-williams-medium-twitter-internet.html?mcubz=1.*

3| *Mark Zuckerberg, Status-Aktualisierung – 12. November 2016, https://www.facebook.com/zuck/posts/10103253901916271.*

Fehlende rechtliche Beschränkungen

Plattformen sind bis heute nahezu nicht reguliert. Dadurch wurden zwar nutzergenerierte Plattformen weitgehend funktionsfähig, aber auch weniger aktiv bei der Bekämpfung von Aktivitäten wie Belästigung, Hassreden und Fehlinformationen, als sie es vielleicht bei einer stärkeren Regulierung wären.[4] Das am Ende der vergangenen Legislaturperiode vom deutschen Bundestag verabschiedete Netzwerkdurchsetzungsgesetz[5] soll die Plattformbetreiber mehr in die Verantwortung nehmen. Durch das Netzwerkdurchsetzungsgesetz werden gesetzliche Compliance-Regeln für soziale Netzwerke eingeführt: Vorgesehen sind u.a. eine Berichtspflicht über den Umgang mit Hasskriminalität und ein wirksames Beschwerdemanagement. Verstöße sollen mit Bußgeldern geahndet werden. Die zukünftige Praxis wird zeigen, ob es dadurch zu einer Verringerung von Hassreden und Fehlinformationen kommen wird.

Finanzielle Beschränkungen

Viele Online-Plattformen sind zu ihrer Finanzierung auf Anzeigen angewiesen. Damit wird eine Plattformgestaltung gefördert, bei der ein Nutzerkonto leicht erstellt werden und der Nutzer dazu verleitet werden kann, möglichst viel Zeit auf dieser Seite zu verbringen. Die kommerziellen Interessen können Anreize für die Plattformbetreiber sein, sich Änderungen zu verweigern, mit denen – etwa um das Auftreten von Bots zu vermeiden – ein Zugang erschwert werden kann oder Desinformationen entschlossen angegangen werden können.

4| Vgl. Sarah Jeong, The Internet of Garbage.

5| Vgl. https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/DE/NetzDG.html.

Bekannte Übeltäter

Desinformationskampagnen werden von verschiedenen Täterkreisen mit unterschiedlicher Motivation betrieben. Es gibt drei wichtige Kategorien von Akteuren, die bei diesen Aktivitäten besonders auffallen:

Politische Akteure

Desinformation kann einen politischen Hintergrund haben und von staatlichen wie auch nichtstaatlichen Akteuren organisiert werden, die damit die Diskussion über bestimmte politische Führungspersonen und Institutionen manipulieren wollen.

Dank des erheblichen Mitteleinsatzes können diese Kampagnen vielschichtig sein und Originalinhalte generieren, die über staatliche Medien und Dritte in Form von Falschmeldungen verbreitet werden. Es werden auch bezahlte Helfer und Botnetze dafür eingesetzt, Desinformationen auf der Nutzerebene zu verbreiten.

Beispiel:
Advanced Persistent Threat („APT") 28 und APT 29 sind zwei große Akteure der Computerspionage, denen durch US-Geheimdienste eine Beteiligung an einer Desinformationskampagne im Jahr 2016 zur Last gelegt wird. Beide wurden mit dem russischen Geheimdienst in Verbindung gebracht und haben offenbar Methoden angewandt, die den umfangreichen Möglichkeiten nationalstaatlicher Akteure entsprechen.[6]

6| *NCCIC / FBI, GRIZZLY STEPPE - Russian Malicious Cyber Activity, https://www.us-cert.gov/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf.*

Kommerzielle Interessen

Die Kommerzialisierung des Internets durch Werbung stellt auch ein finanzielles Motiv für Desinformation dar, die über das Internet weitgehende Verbreitung erfährt und den Datenverkehr antreibt.

Werbekampagnen zielen darauf ab, möglichst viel Datenverkehr in bestimmten Web-Bereichen zu generieren, verfügen aber nicht über die Möglichkeiten staatlicher Medien, die Erzeugung und Verbreitung ausgearbeiteter Falschmeldungen zu unterstützen. Daher kopieren viele dieser Seiten vornehmlich Inhalte aus anderen Bereichen des Internets oder wandeln sie leicht ab.

Beispiel:
Einige Menschen aus Veles in Mazedonien entdeckten, dass Inhalte über Donald Trump zu erhöhten Besucherzahlen ihrer Webseiten führten und damit zu einem höheren Anzeigenaufkommen für sie. Es wurden allein über 150 Trump-freundliche, auf Einwohner von Veles registrierte Domains gefunden. Beiträge, die den Datenverkehr erhöhen, werden unabhängig von ihrem Nachrichtenwert ausgeschlachtet.[7]

7| *Samanth Subramanian, Inside the Macdonian Fake-News Complex, https://www.wired.com/2017/02/veles-macedonia-fake-news/.*

Trolle

Auch Unterhaltung und Aufmerksamkeit im Internet können Motive für Desinformationskampagnen sein. Das „Trollen" – bewusste Provokationen, die Verärgerung hervorrufen – ist seit langem ein Kennzeichen der Online-Kultur.

Trollkampagnen werden durch informelle, meist anonyme Nutzergruppen online koordiniert und können eine Reihe von Techniken umfassen, von der Erstellung irreführender Dokumente und anderer Informationen bis zu koordinierten, gezielten Versuchen, andere Nutzer online zu ködern und irrezuführen.

Beispiel:
Die Verbreitung rassistischer und frauenfeindlicher Cartoons, die scheinbar Donald Trumps Wahlkampf unterstützen sollte, führte zu zahlreichen Nachforschungen durch die traditionellen Medien. Den Journalisten wurden durch Trolle Berichte untergeschoben, die Empörung hervorrufen sollten, und dann wurden weiteren Journalisten Berichte darüber angeboten, wie die vorherigen hinters Licht geführt worden waren. Die daraus resultierende Reaktion in den Medien steigerte noch die Wirkung der anstößigen Meme, die eigentlich kritisiert werden sollten.[8]

8| *Jesse Singal, How Internet Trolls Won the 2016 Presidential Election, http://nymag.com/selectall/2016/09/how-internet-trolls-won-the-2016-presidential-election.html.*

Diese Gruppen arbeiten nicht immer unabhängig voneinander, und sie sind nicht immer leicht auseinanderzuhalten. Untersuchungen zeigen dabei, dass sich online ein vielschichtiges System von Desinformationsaktivitäten etabliert.

Mögliche Bedrohungen durch neue Techniken

Nachdem Desinformationskampagnen öffentlich gemacht und Maßnahmen ergriffen wurden[9], diese Aktivitäten zu unterbinden, sind die Täter dazu gezwungen, ihre Techniken zu verfeinern. Dabei gibt es einige Trends und Techniken, die den Einfluss dieser anhaltenden Kampagnen voraussichtlich deutlich verstärken werden:

Cyber-Attacken

Desinformationskampagnen bedienen sich zunehmend des Hackens von Rechnern für ihre Zwecke. Damit soll Verwirrung gestiftet und die Fähigkeit von Zielpersonen solcher Angriffe, den Kampagnen zu widerstehen, geschmälert sowie die Glaubwürdigkeit gewisser Kanäle gestärkt werden, die die gestohlenen Informationen verbreiten. Damit eröffnen sich auch Möglichkeiten, Informationen zu enthüllen, die das Opfer einer solchen Kampagne diskreditiert oder in ein schlechtes Licht rückt.

Beispiel:
2017 gelang es Hackern, einige Nachrichtenportale in Katar dazu zu bringen, ein irreführendes Narrativ zu verbreiten, mit dem der Emir des Landes diskreditiert wurde und das zu einer regionalen Isolierung des Landes führte.[10]

9| *Wie zuletzt auch in Deutschland erfolgt, vgl. z.B. http://www.faz.net/aktuell/politik/bundestagswahl/fake-news-im-wahlkampf-erfundene-geschichten-spielen-noch-keine-rolle-15205975.html.*

10| *Patrick Wintour, Russian hackers to blame for sparking Qatar crisis, FBI inquiry finds, https://www.theguardian.com/world/2017/jun/07/russian-hackers-qatar-crisis-fbi-inquiry-saudi-arabia-uae.*

Die Evolution der Künstlichen Intelligenz (KI) und des maschinellen Lernens

Errungenschaften in den Bereichen KI und maschinelles Lernen bringen eine Reihe neuer Methoden hervor, menschliches Verhalten glaubhaft von Maschinen imitieren zu lassen. Diese Methoden werden offen publiziert, und die technischen Instrumente zu ihrem Einsatz sind zunehmend verfügbar, da die Kosten für die entsprechenden Rechnerkapazitäten sinken. Das wird die Vorreiter solcher Aktivitäten wahrscheinlich ermuntern, mit diesen Techniken zu experimentieren, um ihre Desinformation glaubhafter scheinen zu lassen und deren Aufdeckung zu erschweren.

Beispiel:
Face2Face, eine neuere Forschungsarbeit der Universität Stanford, zeigt, dass maschinelles Lernen dazu eingesetzt werden kann, aus dem Bildmaterial realer Personen wie etwa politische Amtsträger und andere Führungspersönlichkeiten[11], glaubhaft erscheinende Videos zu erstellen.

Metadaten

Die Täter profitieren von dem leichten Zugang zu den genauen Messdaten über ihre Falschinformationen, die sie produzieren. Indem sie Technik „von der Stange" nutzen, die zu Marketingzwecken entwickelt wurde, erhalten die Betreiber von Desinformationskampagnen Zugang zu detail-

11| Justus Thies et al., Face2Face: Real-Time Face Capture and Reenactment, http://www.graphics.stanford.edu/~niessner/thies2016face.html.

lierten Informationen über die Nutzer und können nahezu in Echtzeit ihre Strategien für eine noch wirksamere Verbreitung ihrer Desinformation verfeinern.

Durch die Erhebung von Metadaten hat die akademische Forschung auch zunehmend die komplexen Prozesse verstehen gelernt, durch die Inhalte geteilt werden, an Glaubwürdigkeit gewinnen und sich möglicherweise viral in einer Nutzergemeinschaft verbreiten. In künftigen Kampagnen könnte dieses Wissen genutzt werden, um die Verbreitung von Botschaften an einflussreiche Personen innerhalb eines Netzwerks zeitlich abzustimmen und damit eine Lawine von Aktivitäten zu ihren Inhalten auszulösen.

Beispiel:
Ein neueres Papier zeigt detaillierte Modelle, wie falsche Informationen in Wikipedia-Artikeln verbleiben und über das Netz verbreitet werden.[12] Solche Informationen helfen böswilligen Akteuren dabei, Desinformationen zu lancieren, die schwieriger zu entlarven sind und sich wirksamer verbreiten.

12| *Srijan Kumar et al., Disinformation on the Web: Impact, Characteristics, and Detection of Wikipedia Hoaxes, http://dl.acm.org/citation.cfm?id=2883085.*

Empfehlungen für die Politik

Die Politik kann eine Reihe proaktiver Schritte unternehmen, um der Bedrohung durch Desinformationskampagnen zu begegnen und bereits vorhandene Bemühungen zu stärken:

Bessere Instrumente zur Überprüfung von Fakten

Die Schaffung kollaborativer Online-Plattformen für digitale Medien, die der Überprüfung von Fakten dienen, sollte gefördert werden, damit Journalisten und Bürger im Web kursierende Desinformation rascher erkennen und darauf reagieren können.[13]

Sensibilisierung im Bereich Medienkompetenz

Investitionen und Partnerschaften könnten eingerichtet werden, die in Sensibilisierungskampagnen die Bürger über Möglichkeiten aufklären, die Qualität von Online-Informationen zu bewerten, und sie ermuntern, sich aktiv an der Bekämpfung von Desinformation zu beteiligen, wenn sie erkannt wird.

Untersuchung von „Warnhinweisen"

Es sollten Studien in Auftrag gegeben werden, inwieweit „Warnhinweise" wirken könnten, die Nutzer von Online-Plattformen darauf aufmerksam machen, wenn der Wahrheitsgehalt bestimmter Inhalte aus journalistischer Sicht zweifelhaft erscheint.[14] Diese Studien könnten auch untersuchen, ob stabile, maschinenlesbare Signale zur Qualität von Informationen geschaf-

13| Entsprechende Bemühungen umfassen Projekte wie Check. Meedan, Check, https://meedan.com/en/check/ /Der deutsche Rechercheverbund Correctiv, https://correctiv.org/.

14| An Ein Beispiel solcher „strittiger" Hinweise werden probeweise bei Facebook untersucht. Jon Constine, Facebook now flags and down-ranks fake news with help from outside fact checkers, https://techcrunch.com/2016/12/15/facebook-now-flags-and-down-ranks-fake-news-with-help-from-outside-fact-checkers/.

fen werden könnten, die sich in einschlägige Algorithmen und andere Systeme integrieren lassen.

Unterstützung des Journalismus

Der Staat kann die Schaffung von Partnerschaften unterstützen, die eine verlässliche Finanzierung des investigativen Journalismus durch den öffentlichen und den privaten Sektor sicherstellen.

Öffentliche Alarmsysteme

Der Gesetzgeber könnte Online-Plattformen dazu bewegen, Daten zu bedeutsamen Desinformationskampagnen in Echtzeit bereitzustellen. Dies würde bei Forschern, Journalisten und den Nutzern insgesamt das Bewusstsein für diese Aktivitäten und deren Gefahren stärken.[15]

15| *Eine weitere Erörterung dazu, inwieweit eine höhere Transparenz bei der Bekämpfung von Desinformation helfen könnte: Tim Hwang und Sam Woolley, The Most Important Lesson From the Dust-Up Over Trump's Fake Twitter Followers, http://www.slate.com/articles/technology/future_tense/2017/06/the_lesson_of_the_dust_up_over_trump_s_fake_twitter_followers.html.*

ANSPRECHPARTNER

Nico Lange
Leiter des Auslandsbüros Washington D.C.
nico.lange@kas.de

Daphne Wolter
Koordinatorin Medienpolitik
Hauptabteilung Politik und Beratung, Berlin
daphne.wolter@kas.de

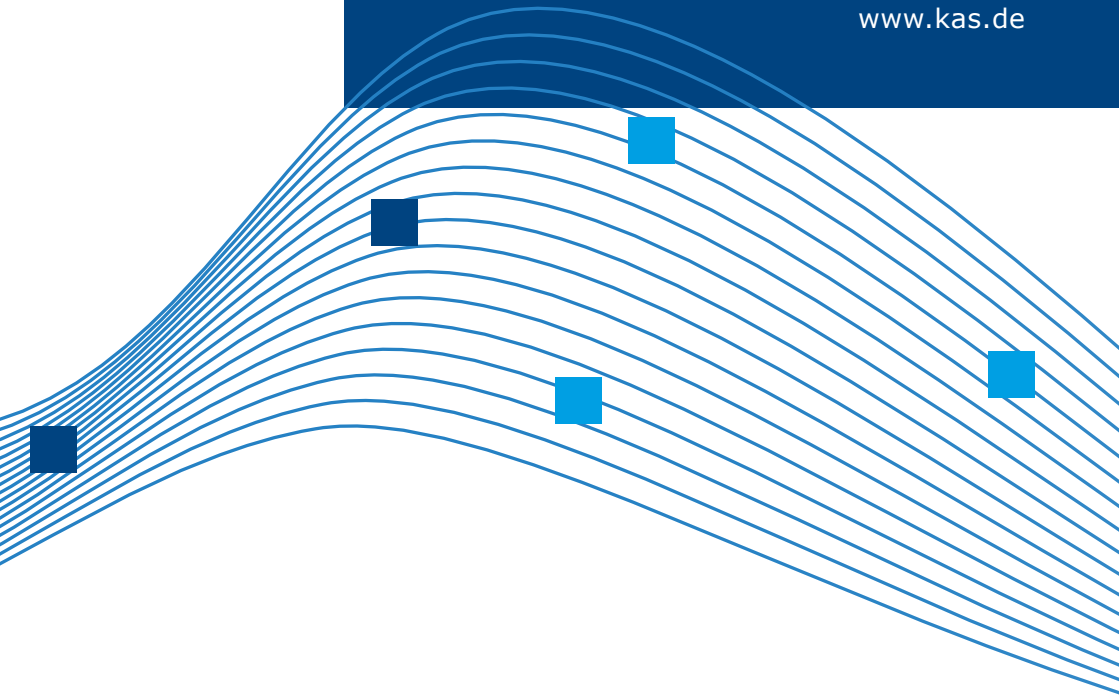
ZUR VERTIEFENDEN LEKTÜRE EMPFEHLEN WIR:

„Die Invasion der Roboter" von Simon Hegelich, abrufbar unter http://www.kas.de/wf/de/33.46486/

„Disruption der Meinungsbildung" von Simon Hegelich und Morteza Shahrezaye, abrufbar unter http://www.kas.de/wf/de/33.49188/

„Künstliche Intelligenz" von Gerhard Lakemeyer, abrufbar unter http://www.kas.de/wf/de/33.49369/

www.kas.de



Konrad
Adenauer
Stiftung