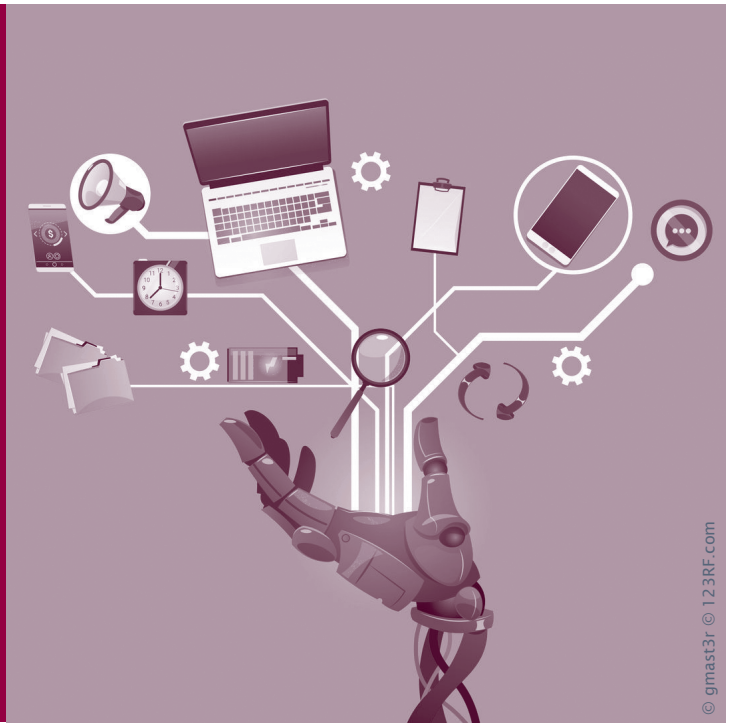
BÜRO FÜR TECHNIKFOLGEN-ABSCHÄTZUNG
BEIM DEUTSCHEN BUNDESTAG

Sonja Kind
Tobias Jetzke
Sebastian Weide
Simone Ehrenberg-Silies
Marc Bovenschulte

Social Bots

TA-Vorstudie

April 2017
Horizon-Scanning Nr. 3



Das Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag (TAB) berät das Parlament und seine Ausschüsse seit 1990 in Fragen des technischen und gesellschaftlichen Wandels. Das TAB ist eine organisatorische Einheit des Instituts für Technikfolgenabschätzung und Systemanalyse (ITAS) im Karlsruher Institut für Technologie (KIT). Zur Erfüllung seiner Aufgaben kooperiert es seit September 2013 mit dem Helmholtz-Zentrum für Umweltforschung GmbH – UFZ, dem IZT – Institut für Zukunftsstudien und Technologiebewertung gGmbH sowie der VDI/VDE Innovation + Technik GmbH.

Sonja Kind
Tobias Jetzke
Sebastian Weide
Simone Ehrenberg-Silies
Marc Bovenschulte

Social Bots

TA-Vorstudie

TAB-Horizon-Scanning Nr. 3

Büro für Technikfolgen-Abschätzung
beim Deutschen Bundestag (TAB)
Neue Schönhauser Straße 10
10178 Berlin

Tel.: +49 30 28491-0
Fax: +49 30 28491-119
buero@tab-beim-bundestag.de
www.tab-beim-bundestag.de

2017

Umschlagbild: gmast3r © 123RF.com

Papier: Circle*offset* Premium White
Druck: Wienands Print + Medien GmbH, Bad Honnef

ISSN-Print: 2199-7101
ISSN-Internet: 2199-711X

Inhalt

Zusammenfassung

Das Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag (TAB) hat durch seinen Konsortialpartner VDI/VDE-IT die vorliegende TA-Vorstudie zur gesellschaftlichen und politischen Relevanz des Themas Social Bots erarbeitet. Im Mittelpunkt stand die Untersuchung von Gefahren durch eine mögliche Manipulation politischer Diskussionen und Trends in sozialen Netzwerken. Grundlage bilden 25 Experteninterviews, die im Zeitraum von Oktober bis Dezember 2016 durchgeführt wurden, sowie eine Literatur- und Quellenanalyse. Auf dieser Basis wurden Thesen erarbeitet, die in einem öffentlichen Fachgespräch am 26. Januar 2017 im Deutschen Bundestag diskutiert und validiert wurden. Die Ergebnisse des Fachgesprächs sowie ein zusätzliches, im Februar 2017 geführtes (schriftliches) Interview mit Facebook flossen in die TA-Vorstudie mit ein.

Das Phänomen Social Bots ist noch recht jung. Wenngleich die Aktivitäten von Social Bots insbesondere auf der Plattform Twitter nachgewiesen werden können, sind die Wirkungszusammenhänge auf die (politische) Willensbildung noch kaum belegt. Dennoch wird den Social Bots ein durchaus schadhaftes bis hin zu gefährliches Einflusspotenzial unterstellt. Social Bots werden momentan im Wesentlichen dafür eingesetzt, Diskussionen inhaltlich zu verzerren sowie die Wichtigkeit von Themen oder die Popularität von Personen und Produkten zu beeinflussen. Nach Experteneinschätzung bergen sie das Potenzial, die politische Debattenkultur im Internet durch die massenhafte Verbreitung von (Falsch-) Nachrichten zu verändern und durch eine »Klimavergiftung« das Vertrauen in die Demokratie zu unterlaufen. Eine wichtige Voraussetzung für den Einfluss von Social Bots auf politische Entscheidungsprozesse sind Kulminationspunkte wie etwa eine knappe Entscheidung bei Wahlen. Über die politische Einflussnahme hinaus bergen Social Bots das Potenzial, das Kunden- und Kaufverhalten Einzelner (über das sogenannte Influencer Marketing) und sogar ganze Märkte (z.B. Börsenhandel) zu manipulieren. Die technischen Möglichkeiten zur Enttarnung von Social Bots sind noch im Entwicklungsstadium und hinken der schnellen Entwicklung von Bots hinterher. Eine der wesentlichen identifizierten Handlungsoptionen gegen Social Bots besteht in der Stärkung der Medien- und informationstechnischen Kompetenz der Kinder und Erwachsenen.

Mögliche Wirkungsbereiche von Social Bots

- qualitative und quantitative Verzerrung von Diskussionen zur Störung der Debattenkultur im Internet bis hin zur Störung des gesellschaftlichen Friedens
- Verunsicherung in Krisensituationen, beispielsweise durch Posten von Falschmeldungen
- Beeinflussung von Themen, die dadurch zu Trending Topics werden können
- Verzerrung von Statistiken bei der Auswertung von Daten in sozialen Medien, wie z.B. der Auswertung der Popularität anhand von Retweets
- Cyber Warfare – hybride Kriegsführung, beispielsweise die Rekrutierung von Teilnehmern für eine Distributed-Denial-of-Service-Attacke (DDoS)
- massenhafter Versand von Schadsoftware an ausgewählte Bevölkerungsgruppen (Automated Spear Phishing)
- persönliche Beleidigung und Belästigung von Personen, indem Einzelpersonen spezifisch mit diskreditierenden Botschaften adressiert werden
- Beeinflussung von Kaufentscheidungen in Bezug auf Produkte und Dienstleistungen
- Wirtschaftskriminalität – gezielte Fehlinformation, die zu Kauf- bzw. Verkaufsentscheidungen führt

Einführung I.

Social Bots sind Computerprogramme, die darauf ausgerichtet sind, in sozialen Netzwerken, beispielsweise auf Facebook oder Twitter, maschinell erstellte Beiträge wie Kommentare, Antworten oder Meinungsäußerungen zu generieren, um Diskurse zu beeinflussen bzw. zu manipulieren.

Fakeaccounts von Social Bots, d.h. gefälschte Nutzerprofile, hinter denen keine authentischen Personen stehen, lassen sich leicht vervielfachen, sodass beispielsweise auf Twitter tausende Benutzerkonten geschaffen werden können, die wiederum zehntausende Tweets pro Tag erzeugen. Es wird vermutet und ist teilweise auch belegt, dass Social Bots sowohl von Staaten als auch von Unternehmen und Interessengruppen gezielt eingesetzt werden. Die Social Bots sind in der Lage, sinnvolle Texte zu erzeugen, die von Menschen geschriebenen Texten ähneln. Für Menschen ist es also selten offensichtlich, dass die Beiträge nicht von einem Menschen, sondern von einer Maschine stammen. Die Menschenähnlichkeit wird auch dadurch suggeriert, dass der Social Bot nicht immer politisch agiert und kommentiert, sondern auch mehr oder weniger Belangloses postet, beispielsweise Kommentare zu Fußballergebnissen, Hinweise auf Serieninhalte etc.

Social Bots agieren durchaus menschenähnlich. Sie können Konversationen führen und greifen dabei auf passende Inhalte aus dem Internet zurück; sie können einflussreiche Personen in sozialen Netzwerken identifizieren bzw. deren Verhalten analysieren, diesen folgen oder durch Anfragen gezielt die Aufmerksamkeit auf sich lenken. Dabei imitieren sie das Verhalten von menschlichen Nutzern, indem sie beispielsweise zu unterschiedlichen Tageszeiten einen unterschiedlichen Grad an Aktivität vortäuschen. Sie stehlen die Identitäten von realen Nutzern, indem sie Nutzernamen annehmen, die realen Nutzernamen ähneln, oder indem sie personenbezogene Informationen wie Bilder oder Links für sich verwenden (Ferrara et al. 2014, S. 4).

Ziele der Untersuchung

Ziel der TA-Vorstudie war, einen Überblick über den aktuellen Stand der Technik von Social Bots (Fähigkeiten der eingesetzten Algorithmen), Anwendungsfelder und Anwender, Verbreitung sowie tatsächliche und angenommene Risiken zu schaffen. Ferner sollten der momentane Kenntnisstand sowie Einschätzungen zum tatsächlichen Ausmaß des Einsatzes von Social Bots sowie deren Wirkungskraft beleuchtet werden. Im Mittelpunkt stand die Untersuchung von potenziellen Gefahren durch eine mögliche Manipulation politischer Diskussionen und Trends in sozialen Netzwerken sowie Einflusspotenziale im Bereich der Wirtschaft.

Die Analyse konzentrierte sich auf drei Fragestellungen:

- Was ist heute machbar, und wie wird der Einfluss von Social Bots nachgewiesen?
- Wofür können Social Bots zukünftig eingesetzt werden?
- Wie lassen sich Social Bots erkennen und verhindern?

Die Untersuchung fand von Oktober bis zum Dezember 2016 statt. Zwischenergebnisse wurden im Rahmen eines öffentlichen Fachgesprächs am 26. Januar 2017 im Deutschen Bundestag vorgestellt und diskutiert. Die zentralen Diskussionslinien des Fachgesprächs zu möglichen Handlungsfeldern wurden in Kapitel VI aufgegriffen und zusammengefasst.

Methodik

Die methodische Herangehensweise der Kurzstudie fußt auf drei Säulen: Es wurden Interviews mit 25 Fachexperten aus sechs Bereichen durchgeführt (Anhang 2): Wissenschaft, Verwaltung, zivilgesellschaftliche Organisationen, Parteien (Social-Media-Beauftragte), Presse/Medien sowie Wirtschaft. Insgesamt wurden 35 Expertinnen und Experten angefragt. In einer systematischen Literatur- und Quellenanalyse wurden wissenschaftliche sowie weitere Veröffentlichungen sondiert, ergänzend wurde eine quantitative Web-of-Science-Analyse vorgenommen (Kap. III.2). Ferner wurde anhand eines Experiments überprüft, ob es mit geringen Programmierkenntnissen gelingen kann, einen eigenen Social Bot zu programmieren (Kap. IV).

Definition und Eigenschaften von Social Bots II.

Social Bots sind Computerprogramme, die eine menschliche Identität vortäuschen und für manipulative Zwecken eingesetzt werden, indem sie wie Menschen im Internet kommunizieren (Bilton 2014; Fuchs 2016a; Voß 2015; Woolley/Howard 2016a u. 2016b). Menschen, die mit Social Bots interagieren, nehmen diese nicht als durch Algorithmen gesteuerte automatische Kommunikation, sondern als menschliche Internetteilnehmer wahr und sind sich der Manipulation nicht bewusst.

Bei Social Bots handelt es sich um Algorithmen, die als (semi)automatisierte Agenten vordefinierte Aufgaben wahrnehmen können (Boshmaf et al. 2011, S. 93; Fredheim 2014; Guilbeault 2016, S. 5003; Murthy et al. 2016, S. 4955; Woolley/Howard 2016b, S. 4885). Im Kern bestehen Social Bots aus drei Elementen: den Benutzerkonten in sozialen Netzwerken, Programmierschnittstellen sowie der in einer beliebigen Programmiersprache verfassten Software mit der Verhaltenslogik des Social Bots (Interviews Hegelich u. Janetzko). Technisch gesehen sind Social Bots mit Blick auf ihre Zielrichtung grundsätzlich neutral. Sie führen lediglich das aus, wozu sie (von Menschen) programmiert worden sind.

Das Wort Bot in Social Bot leitet sich von »robot« (Roboter) ab (Ferrara et al. 2014). Der Ausdruck Social weist darauf hin, dass es sich bei den verwendeten Algorithmen um Programme handelt, die vorzugsweise innerhalb von sozialen Medien ihre Wirkung entfalten (Boshmaf et al. 2011, S. 93).

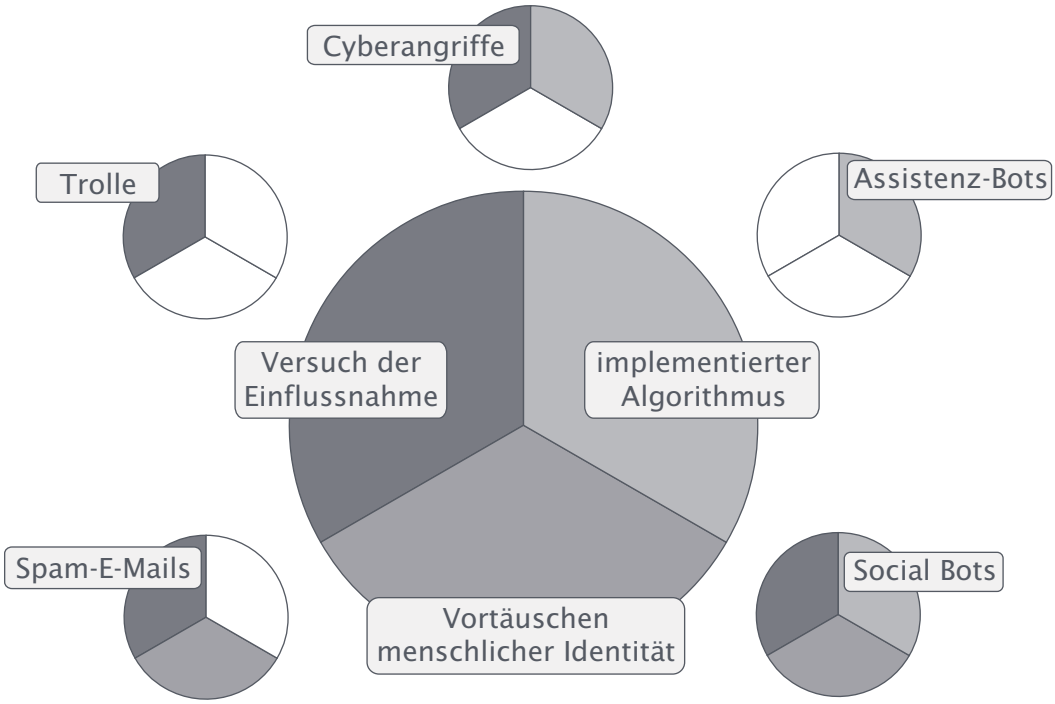
Social Bots imitieren menschliches Verhalten, um ihrem jeweiligen Gegenüber eine menschliche Identität vorzutäuschen (Interview Pfeffer; Bilton 2014; Fischer 2016; Fuchs 2016a; Voß 2015; Woolley/Howard 2016b, S. 4885). Dies erfolgt in der Regel mit der Absicht, ihre Interaktionspartner zu beeinflussen und deren Meinung zu manipulieren (Voß 2015; Weck 2016; Woolley/Howard 2016b, S. 4882).

In Abgrenzung zu anderen Internetphänomenen, wie Assistenz-Bots, Spam-E-Mails, Trollen oder Cyberangriffen, sind Social Bots durch die Kombination dreier zentraler Merkmale charakterisiert (Abb. II.1):

- Es handelt sich bei Social Bots um einen in einer Software implementierten Algorithmus.
- Sie täuschen eine reale Person vor.
- Social Bots versuchen, Einfluss auf die Meinungsbildung zu nehmen.

Der Begriff Social Bots ist nicht immer ganz trennscharf. Teilweise werden Social Bots noch weitergehend differenziert und z. B. als Twitter-Bot bezeichnet, wenn sie primär auf der Plattform Twitter aktiv sind (Dewey 2016; Kollanyi 2016, S. 4932), oder Political Bots genannt, wenn sie maßgeblich dazu eingesetzt werden, die öffentliche Meinung zu beeinflussen (Woolley/Howard 2016b, S. 4882). Sowohl in den Experteninterviews als auch in den analysierten Fach- und Medienartikeln verschwimmen zuweilen die Grenzen zwischen einzelnen Definitionsansätzen.

Abb. II.1 Abgrenzung von Social Bots zu anderen Internetphänomenen



Eigene Darstellung

Social Bots unterscheiden sich von unterstützenden Bots (z. B. Chat-Bots, digitale Assistenten) hinsichtlich ihrer Zielsetzung; ihre technischen Grundlagen sind verwandt.

Die in der Abbildung II.1 aufgeführten Internetphänomene unterscheiden sich von Social Bots dadurch, dass sie nur ein oder zwei der für Social Bots wesentlichen drei Kennzeichen aufweisen.

Insbesondere sind assistierende oder unterstützende Bots von Social Bots abzugrenzen, weil solche Chat- und Bot-Systeme zwar über eine den Social Bots vergleichbare technische Basis verfügen, sich jedoch hinsichtlich ihres Einsatz-

zwecks unterscheiden. Werden Social Bots in der Regel zur Täuschung ihrer Interaktionspartner mit dem Ziel einer Beeinflussung bzw. einer Manipulation eingesetzt (Interview Helbing; Woolley/Howard 2016b, S. 4882), so dienen Chat- und Assistenz-Bots primär der Unterstützung, nutzen aber genauso wie Social Bots semantische Analysen (Markoff 2017; Neff/Nagy 2016, S. 4915 f.).

Der Zweck von Assistenz-Bots besteht beispielsweise darin, automatisierte Meldungen wie Wetternachrichten oder Unwetterwarnungen zu versenden. Zu den Assistenz-Bots zählen auch Chat-Bots oder Messengerdienste, die in den Dialog mit Internetnutzern treten. Beispiele für solche Bots sind die Spracherkennungssoftware Siri von Apple, Cortana von Microsoft oder Watson von IBM. Ein Beispiel für einen Messenger-Bot ist der von Facebook betriebene Bot namens Poncho in der Gestalt einer Comickatze mit gelbem Regencape. Poncho postet Wetternachrichten und beantwortet darüber hinaus auch Fragen im Chat.

Social Bots, Trolle als menschliche Akteure sowie Spam-E-Mails eint die Zielsetzung der Manipulation oder Desinformation. Mit Cyberangriffen eint Social Bots deren technische Basis und ebenfalls die Zielsetzung der Einflussnahme.

Social Bots sind in der Lage, sogenannte Fakenews massenhaft zu verbreiten.

Hinter Trollen verbergen sich Einzelpersonen, die zwar viele Nachrichten aussenden, dies aber nicht automatisiert tun und deshalb in ihrem Wirkungsgrad im Vergleich zu Social Bots begrenzt sind (Interview Janetzko). Allerdings können Trolle und Social Bots gemeinsam wirken, indem Social Bots die von Trollen abgesetzten Botschaften massenhaft verbreiten und dadurch verstärken. Der Einflussbereich von Trollen wird so erweitert (Interviews Hegelich, Janetzko u. Stöcker).

Bei Spam-E-Mails handelt es sich um ein Phänomen, bei dem ebenfalls häufig vorgegeben wird, dass die Nachricht von einem Menschen gesendet wird. Sehr bekannt sind die Spam-E-Mails mit betrügerischen Absichten, in denen eine Person um Mithilfe beim Zugriff auf eine große Erbschaft bittet und dafür eine Teilsumme zur Gratifikation zahlen möchte.

Als ein weiteres Internetphänomen sind Cyberangriffe von Social Bots abzugrenzen, da sie auf das Vortäuschen einer menschlichen Identität gänzlich verzichten. Dies ist auch nicht erforderlich, weil Cyberangriffe direkt auf Hard- oder Software zielen, um ihre schadhafte Wirkung zu entfalten.

Schließlich sind auch noch Fakenews zu erwähnen, die einer anderen Logik als den zuvor beschriebenen Internetphänomenen folgen. Als Fakenews werden Nachrichten bezeichnet, die in der Regel wissentlich gefälscht oder erfunden wurden und mit denen die Öffentlichkeit für politische oder kommerzielle Zwe-

cke manipuliert werden soll. Bei Fakenews handelt es sich um Inhalte, die im Internet oder traditionellen Medien verbreitet werden können. Social Bots können dazu eingesetzt werden, diese gefälschten Nachrichten massenhaft zu transportieren und innerhalb von Bot-Netzwerken zu multiplizieren.

Die Initiatoren und Urheber von Social Bots können bislang bis auf wenige Ausnahmen nicht identifiziert oder rückverfolgt werden (Interviews Welchering u. Wenzel). Dies betrifft sowohl Social Bots zur politischen Propaganda als auch Social Bots für wirtschaftliche Zwecke (Interviews Hegelich u. Kossol). Mutmaßliche Initiatoren politisch motivierter Manipulationen sind Geheimdienste, Terrorgruppen, terroristisch motivierte Einzelpersonen (Lone Wolves), aber auch andere Akteure wie z. B. Unterstützer im Wahlkampf (Interviews Hegelich, Reez u. Welchering).

Social Bots können je nach technischer Entwicklungsstufe eine menschliche Identität unterschiedlich gut vortäuschen. Einfache Social Bots erkennen Schlüsselbegriffe (z. B. Refugees) und reagieren darauf, indem sie z. B. Bilder aus dem Internet posten oder Kommentare retweeten. Komplexere Social Bots können Kommunikationsinhalte analysieren und Dialoge führen. Zurzeit dominieren einfache Social Bots im Internet.

Social Bots existieren in verschiedenen technischen Entwicklungsstufen, die unterschiedliche Funktionen und komplexe Aktivitäten erlauben (Interview Helbing). Als zu programmierende Funktionen sind prinzipiell alle automatisierbaren Aktivitäten in sozialen Medien möglich (Bohacek 2016; Howard/Kollanyi 2016, S. 1), wie z. B. die Veröffentlichung von Inhalten, das Weiterleiten von und Antworten auf Nachrichten oder das Knüpfen sozialer Beziehungen in Form von Freunden oder Followern (Freitas et al. 2015, S. 25).

Bei den derzeit eingesetzten Social Bots handelt es sich um ein Reiz-Reaktions-Modell, dessen Grundfunktionen darin bestehen, äußere Stimuli zu erkennen (z. B. bestimmte Stichwörter) und durch einen programmierten Mechanismus auf diese Reize mit vordefinierten Aktionen zu reagieren (Interview Janetzko). Das Handlungsspektrum von Social Bots kann von einzelnen, einfachen Funktionalitäten bis hin zu verknüpften, komplexen Aktionen reichen.

Einfache Social Bots veröffentlichen vorgegebene Nachrichten oder Links, die auf andere Webinhalte führen, und wiederholen bzw. retweeten von anderen Nutzern veröffentlichte Nachrichten bzw. heben diese durch Favorisierung (liken) hervor (Interview Quandt; Murthy et al. 2016, S. 4956).

Je komplexer Social Bots programmiert werden, desto mehr täuschende Merkmale weisen diese auf. Die Benutzerkonten komplexer Bots sind detailliert und durch charakteristische, personenbezogene Daten gekennzeichnet (z. B. Alter, Geschlecht, Name etc.), sie haben Profilbilder und die Chronik der Akti-

vitäten reicht in die Vergangenheit. Außerdem verfügen sie über Freunde bzw. Follower (Interview Neumann). Auch ihre Aktivitätsmuster wie Tag- und Nachtrhythmus oder die Anzahl gesendeter Nachrichten wirken realistisch und entsprechen weitestgehend denen menschlicher Akteure.

Komplexere Social Bots sind so programmiert, dass sie verschiedene Vorlieben vortäuschen. Die Nutzerkonten der Social Bots folgen diversen Themen, veröffentlichen nur gelegentlich unterschiedliche Inhalte und fügen nur sehr ausgewählte fremde Benutzerkonten zu ihrem eigenen Profil hinzu bzw. folgen selbst nur bestimmten Benutzerkonten (Fischer 2016). Ebenso entnehmen komplexere Social Bots ihre erzeugten und veröffentlichten Inhalte nicht einfach nur einer programmierten Datenbank. Stattdessen sind die Algorithmen in der Lage, Informationen zu sammeln und mittels semantischer Analyse und weiterer Daten in immer wieder neue Texte zu verwandeln (Interview Strohmaier).

Aktuell scheinen einfache Social Bots mit geringem Funktionalitätsspektrum am weitesten verbreitet zu sein (Interviews Helbing u. Stöcker). Einfache Social Bots können allein durch das ständige Wiederholen bestimmter Botschaften dafür sorgen, dass die Gegenbotschaft in der schieren Masse untergeht bzw. in Relevanzrankings nach unten sinkt oder gar nicht mehr auftaucht (sogenannte Brute-Force-Attacken). Umgekehrt können sie als Verstärker für Botschaften agieren und diese im Extremfall sogar zum Trend werden lassen (Interviews Neumann, Quandt u. Strohmaier; Woolley 2016, S. 1).

Ein einfacher Social Bot lässt sich mit nur wenigen Programmierkenntnissen erstellen. Handbücher und Anleitungen dazu finden sich frei verfügbar im Internet. Allerdings wächst der Schwierigkeitsgrad mit der technischen Komplexität der zu programmierenden Bots stark an, wenn diese beispielsweise Sprachanalysen durchführen und Dialoge simulieren sollen.

Die Herstellung von Social Bots kann auch in Auftrag gegeben werden. Hierzu existiert eine Wertschöpfungskette mit global verteilten Produktionsstufen.

Die Schaffung der technischen Voraussetzungen eines Social Bots ist bereits heute mit relativ einfachen und frei zugänglichen Mitteln möglich. Spezielle Programmierkenntnisse sind zumindest für die Erstellung von Social Bots mit geringer Komplexität nicht erforderlich (Interviews Grimme, Pfeffer u. Strohmaier). Es reichen Grundkenntnisse in gängigen Programmiersprachen wie Java, Python etc., um die im Internet verfügbaren Bestandteile der Algorithmen in Form von Baukastensystemen zusammenzusetzen und innerhalb eines Tages zum Einsatz zu bringen (Interview Janetzko; siehe auch Kap. IV). Anleitungen, wie dies zu bewerkstelligen ist, sind im Internet ohne großen Suchaufwand auf-

findbar (Bohacek 2016). Die Programmierung von Bots gegen Entgelt hat sich außerdem bereits zu einem Geschäftsmodell für Einzelpersonen entwickelt (Breithut 2016).

Bei steigender Komplexität der Social Bots lassen sich auch einzelne Entwicklungsschritte an Dienstleister auslagern (Interviews Grimme u. Pfeffer). Dies ist vor allem dann notwendig, wenn die im Einzelfall verfügbaren Rechenkapazitäten nicht mehr für den Betrieb der Social Bots ausreichen oder aber komplexere Programmierkenntnisse erforderlich sind. Dafür können beispielsweise cloudbasierte Datenverarbeitungsdienste eingekauft und spezialisierte Dienstleister beauftragt werden (Interview Janetzko).

Weiterhin werden von einschlägigen Anbietern die notwendigen Daten zur Erstellung von sehr echt wirkenden Benutzerkonten zur Verfügung gestellt, denn je mehr Daten in die Erstellung der Benutzerkonten und die Programmierung der Social Bots einfließen, desto menschlicher wirken und agieren diese. Aus der Vielzahl an möglichen Akteuren, die an der Erstellung und dem Betrieb komplexer Social Bots mitwirken können, hat sich eine weltweit verteilte Wertschöpfungskette entwickelt (Interview Hegelich). Da es sich dabei um einen hochgradig intransparenten Markt handelt, kann dessen Bedeutung jedoch kaum plausibel abgeschätzt werden (Interview Kossol).

In den nächsten Jahren sind erhebliche Entwicklungssprünge im Bereich der Bot-Technologie zu erwarten. Die technologische Reife der Social Bots wird von den fortschreitenden Entwicklungen in den Bereichen künstliche Intelligenz, Machine Learning und Big Data profitieren. Social Bots werden deshalb zukünftig noch menschenähnlicher agieren können und schwieriger zu enttarnen sein.

Bisher hat sich die kurze und einfache Form der Nachrichten, die über soziale Netzwerke ausgetauscht werden, begünstigend auf die technische Entwicklung von Social Bots ausgewirkt. Weil meist keine längeren Dialoge in den sozialen Medien geführt werden, können die Leser nur schwer nachvollziehen, ob Beiträge von einem Menschen oder von einem Bot formuliert wurden. So lässt sich mit sehr einfachen Algorithmen menschliches Kommunikationsverhalten in Kurznachrichten simulieren (Interview Janetzko).

In den kommenden Jahren werden wesentliche Entwicklungssprünge in der Bot-Technologie erwartet (Interviews Grimme, Hegelich u. Pfeffer). Eine maßgebliche Rolle spielt dabei die Weiterentwicklung im Bereich der künstlichen Intelligenz, die bislang nur rudimentär in die Programmierung von Social Bots eingeflossen ist (Guilbeault 2016, S. 5005), in Zukunft aber an Bedeutung gewinnen wird (Fuchs 2016a).

Die Betreiber sozialer Medien setzen selbst verstärkt auf die Anwendung von als solchen gekennzeichneten Bots innerhalb von Messengerdiensten wie den bereits erwähnten Dienst Poncho von Facebook oder Allo von Google, der auf einem Google-Handy benutzt werden soll. Diese Chat-Bots sollen als digitale Assistenten zukünftig intensiv in der Kundenbetreuung und Nutzerunterstützung eigesetzt werden (Interviews Fuchs u. Walter 2016). Die Idee besteht darin, dass der Nutzer innerhalb des sozialen Netzwerks mit dem Bot kommuniziert. Er kann Produkte auswählen und kaufen, ohne dafür den »Kosmos« des sozialen Netzwerks verlassen zu müssen. So können z.B. Hotelzimmer, Flüge, Kinokarten oder Blumen innerhalb des sozialen Netzwerks gebucht werden, ohne dafür auf die jeweilige Website der Anbieter zu wechseln. Dies ermöglicht neue Geschäftsmodelle (Interview Lutter), aber auch Auswirkungen dahingehend haben, wie Menschen noch mehr auf Websites der Anbieter gezogen werden können. Die Entwicklung der technisch anspruchsvollen und intelligenten Bots wird auch die Entwicklung von Social Bots weiter beflügeln, weil sie aufgrund des zunehmend intelligenten Verhaltens zukünftig immer schwerer von Menschen unterschieden werden können (Interviews Fuchs, Hegelich, Walter u. Welchering).

Des Weiteren setzen sich die schon länger zu beobachtenden Entwicklungen fort, die eine einfache Programmierbarkeit von Social Bots ermöglichen. Dazu gehören sinkende Preise für Speicherplatz und Rechenleistung, die Verbreitung von Breitbandanschlüssen und die Verfügbarkeit von Cloudcomputing (Interviews Kondo u. Welchering). Ferner werden Fortschritte im Bereich der Sprachanalyseprogramme eine verbesserte Kommunikationsfähigkeit der Social Bots ermöglichen (Interview Hegelich). Aufgrund der zunehmenden Verbreitung von Big-Data-Analysen und deren Verzahnung mit Sprachanalyseprogrammen wird eine immer bessere und flexiblere sprachliche Ausdrucksfähigkeit von Social Bots erwartet (Interview Janetzko).

Die skizzierten technischen Entwicklungslinien deuten darauf hin, dass Social Bots zukünftig immer besser menschliche Identitäten imitieren können (Interview Neumann) und aufgrund der verschwimmenden Grenzen zwischen realer und künstlicher Intelligenz kaum noch von menschlichen Akteuren in sozialen Netzwerken zu unterscheiden und damit auch immer schwerer zu enttarnen sein werden (Interview Wenzel).

Literatur- und Quellenanalyse zu Social Bots III.

Social Bots in wissenschaftlicher Literatur und Presse 1.

Das Thema Social Bots wird in der Wissenschaft erst seit wenigen Jahren bearbeitet, auch wenn die dahinterliegende Technologie schon bis in die 1960er Jahre zurückreicht, als erste Bots wie beispielsweise ELIZA entwickelt wurden (Weizenbaum 1978). Bei ELIZA handelt es sich um ein von Joseph Weizenbaum im Jahr 1966 entwickeltes Computerprogramm, das mit Menschen kommunizieren konnte, indem es auf eine Sammlung von Textbausteinen zurückgriff. Wie ein Chat-Bot führt ELIZA Gespräche mit den Nutzern und bediente sich dabei einer besonderen Fragetechnik. ELIZA griff das Gesagte auf und formulierte daraus eine Frage mit Synonymen und Oberbegriffen des ursprünglichen Textes oder forderte den Fragenden auf, mehr von sich zu erzählen (Ferrara et al. 2016, S. 96). Ein typischer Dialog wäre: »Ich habe Schwierigkeiten mit meinem Bruder.« ELIZA: »Erzähle mir mehr über Deine Familie.« ELIZA steht somit stellvertretend für einen der ersten funktionsfähigen Chat-Bots.

Boshmaf et al. (2011) publizierten eine erste wissenschaftliche Arbeit zu Social Bots im Jahr 2011. Darin wird ein Experiment beschrieben, bei dem sich Bots als Familienmitglieder ausgeben und versuchen, per Freundschaftsanfragen auf Facebook Informationen von Menschen auszuspähen. Wagner et al. (2012) setzten sich ebenfalls in einem Experiment, diesmal allerdings unter Nutzung des sozialen Netzwerks Twitter, mit der Frage auseinander, inwieweit Menschen mit Social Bots interagieren und z. B. auf Aktivitäten von Bots antworten oder deren Einträge kommentieren, Tweets retweeten oder gar den Bots folgen. Seit etwa 2012/2013 etabliert sich die wissenschaftliche Auseinandersetzung zunehmend (Interviews Janetzko u. Strohmaier). Diese Entwicklung lässt sich auch durch eine in dieser Untersuchung durchgeführte Analyse des Web of Science (Rechercheplattform zu Publikationen aus den Fächern Medizin, Natur-, Geistes-, Sozial- und Wirtschaftswissenschaften) zum Thema Social Bot bestätigen (Kap. III.2).

Noch gibt es nur einen relativ kleinen Kreis nationaler und internationaler Autoren im Forschungsfeld Social Bots. Zum Zeitpunkt Dezember 2016 stammten die meisten wissenschaftlichen Veröffentlichungen aus Forschungsprojekten folgender Wissenschaftler: Emilio Ferrara von der University of Southern California (Bessi/Ferrara 2016; Ferrara et al. 2014; Ferrara et al. 2016), Simon Hegelich von der Hochschule für Politik München (Hegelich 2016; Hegelich/Janetzko 2016), Sam Woolley von der University of Washington (Woolley 2016; Woolley/Howard 2016a u. 2016b) und Philip Howard von der University of Oxford (Howard/Kollanyi 2016).

In Deutschland beschränkt sich die Forschung bis jetzt auf zwei Vorhaben. Seit Sommer 2015 laufen die vom Bundesministerium für Bildung und Forschung (BMBF) geförderten Forschungsprojekte »PropStop« und »Social Media Forensics« (SoMeFo), die sich mit der Erkennung, dem Nachweis und der Bekämpfung von verdeckten Propagandaangriffen über Onlinemedien beschäftigen. Die Koordination des Projekts »PropStop« erfolgt durch Christian Grimme am Institut für Wirtschaftsinformatik an der Universität Münster. Das Projekt »Social Media Forensics« war zunächst an der Universität Siegen angesiedelt und wird nun von Simon Hegelich an der Hochschule für Politik München fortgesetzt. Wissenschaftliche Publikationen aus beiden Projekten liegen aufgrund der kurzen Laufzeit noch nicht vor, erste Zwischenergebnisse sind frühestens im Jahr 2017 zu erwarten (Interview Quandt).

Schwerpunkte in der wissenschaftlichen Literatur und Forschung zu Social Bots sind gesellschaftliche und wirtschaftliche Auswirkungen. Es gibt erste Ansätze zum Effektnachweis von Social Bots auf Entscheidungsprozesse bzw. Diskursverläufe wie etwa die Radikalisierung von Diskursen. Es wird also der Frage nachgegangen, ob Social Bots tatsächlich die Entscheidungsprozesse von Menschen beeinflussen können (Interview Janetzko; Bessi/Ferrara 2016; Woolley/Howard 2016b). In Bezug auf technische Fragestellungen stehen Aspekte wie das Detektieren von Social Bots oder die Programmierung besonders intelligenter Bots im Mittelpunkt (Interviews Grimme u. Hegelich; Howard/Kollanyi 2016; Subrahmanian et al. 2016). Zusammengefasst lässt sich festhalten, dass es bislang nur eine geringe Anzahl von Publikationen mit einem ausschließlichen Fokus auf das Thema Social Bots gibt.

Parallel zur wissenschaftlichen Auseinandersetzung wird das Thema Social Bots auch in den Medien behandelt. Im Jahr 2014 wurde es zunächst in Onlineforen diskutiert (Interview Welchering), seit dem Sommer 2015 ist das Thema auch in Online-, Print- sowie seit einigen Monaten in TV-Medien präsent (Interviews Grimme u. Walter 2016). Besonders in den letzten Wochen des Jahres 2016 und rund um das öffentliche Fachgespräch des Ausschusses für Bildung, Forschung und Technikfolgenabschätzung am 26. Januar 2017 im Deutschen Bundestag zu Social Bots war eine große mediale Präsenz des Themas zu beobachten. Die Berichterstattung in den Medien fokussierte bis Ende 2016 überwiegend auf einzelne Ereignisse bzw. Teilaspekte, wie z.B. auf die Aktivitäten von Social Bots in Partnervermittlungsbörsen (Lobo 2016; Newitz 2015; ZEIT ONLINE 2016). Anfang des Jahres 2017, nach Veröffentlichung des Thesenpapiers zu dieser TA-Vorstudie und nach dem Fachgespräch im Bundestag, wurden Social Bots vor allem in Zusammenhang mit ihrer möglichen Verwendung im Bundestagswahlkampf, ihrem Einsatz zur Verbreitung von Fakenews sowie den Möglichkeiten zu ihrer Erkennung und Eindämmung diskutiert (Beuth 2017; Endt 2017; Kerl 2017; Krause 2017; Tutt 2017).

Web-of-Science-Analyse 2.

Als Ergänzung zur Literatur- und Quellenanalyse wurde eine semiquantitative Web-of-Science-Analyse von Publikationsdaten durchgeführt.

Die Forschungsdatenbank »Web of Science« deckt gegenwärtig eine große Vielfalt an wissenschaftlichen Publikationen mit rund 50.000 Büchern, 12.000 Journalen und 160.000 Conference Proceedings aus den Bereichen Natur-, Geistes- und Sozialwissenschaften ab. Suchergebnisse enthalten reichhaltige Metadaten wie Schlagwörter, Jahr der Veröffentlichung, Veröffentlichungsort, Forschungsgebiet, Adressen der Autoren, Anzahl der Zitationen etc. Bei der quantitativen Auswertung der Web-of-Science-Daten standen diese Metainformationen der Publikationen im Fokus. Die Auswertung hatte zum Ziel, wissenschaftliche Publikationen mithilfe ihrer Metadaten zu kategorisieren und miteinander in Bezug zu setzen. Für eine Visualisierung wurden die Daten mithilfe einer Software für Netzwerkanalyse grafisch aufbereitet.

Auswahl der Literatur

Für die Auswahl der relevanten wissenschaftlichen Artikel war eine Suchanfrage mit geeigneten Begriffen erforderlich, um das Themengebiet möglichst trennscharf zu erfassen. Die Gespräche mit den Experten und die qualitative Literaturanalyse hatten ergeben, dass das Thema derzeit nur mit einer relativ großen Anzahl von Begriffen verschlagwortet werden kann. Die Suchanfrage im Web of Science erfolgte deshalb mit folgenden Bezeichnungen, die mit einem ODER-Operator verknüpft wurden: social bot, political bot, propaganda bot, public relations bot, like bot, push bot, influence bot, marketing bot.

Die Suche nach wissenschaftlichen Veröffentlichungen zum Thema Social Bots, die mindestens einen der zuvor genannten Begriffe enthielten, lieferte ca. 500 Treffer. Im nächsten Schritt wurden die Treffer auf ihre Relevanz bzw. Passung untersucht und nichtrelevante Artikel manuell aussortiert. Nach dieser Selektion ergab sich eine Artikelzahl von lediglich 59 Publikationen. Der Grund hierfür lag darin, dass Suchergebnisse aus dem Jahr 2011 und früher kaum Bezug zum Thema Social Bots hatten und deshalb die meisten Treffer der initialen Suche aussortiert werden mussten. Dies lag vor allem daran, dass viele der Suchergebnisse mit dem Akronym »bot« für Borderline Ovarian Tumor verschlagwortet waren und aus dem Medizinbereich stammten.

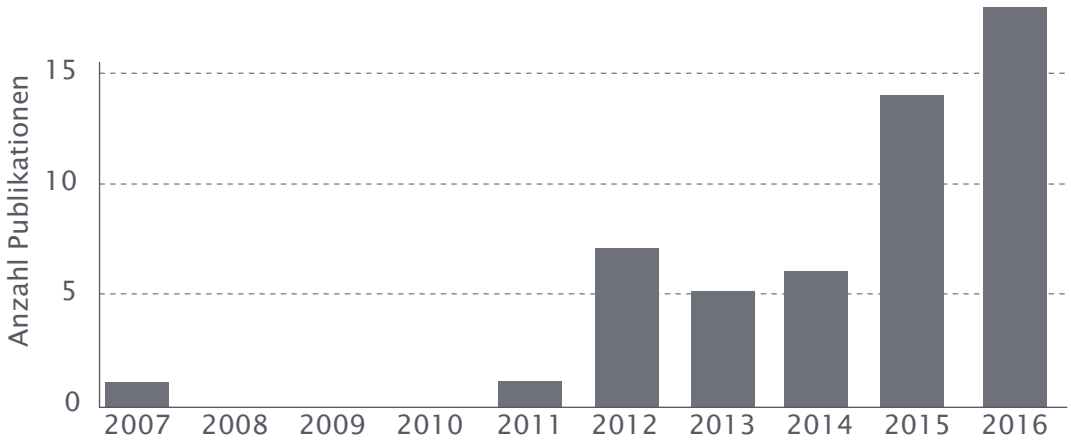
Die Interpretation der Daten bezieht sich demzufolge auf eine recht geringe Anzahl an Veröffentlichungen. Zudem deckt das Web of Science viele, aber bei Weitem nicht alle Fachveröffentlichungen ab. Die Registrierung im Web of Science erfolgt erst bei Veröffentlichungsentscheidung und daher immer mit einer gewissen zeitlichen Verzögerung – in jungen, hoch dynamischen Gebieten

wie der Social-Bot-Forschung (und der Informatik insgesamt) spiegeln sie daher nicht die neuesten Forschungsaktivitäten wider, weshalb die Ergebnisse entsprechend vorsichtig interpretiert werden sollten.

Noch vergleichsweise geringe Anzahl wissenschaftlicher Publikationen zu Social Bots

Abbildung III.1 zeigt, dass zu diesem Thema erst seit ein paar Jahren veröffentlicht wird und die Zahl der Publikationen noch vergleichsweise gering ist; seit 2015 ist jedoch ein Aufwärtstrend bei den Publikationen zu verzeichnen.

Abb. III.1 Anzahl der Publikationen zum Thema Social Bots im Web of Science



Eigene Darstellung

Erforschung von Social Bots an der Schnittstelle von Informatik und Sozialwissenschaften

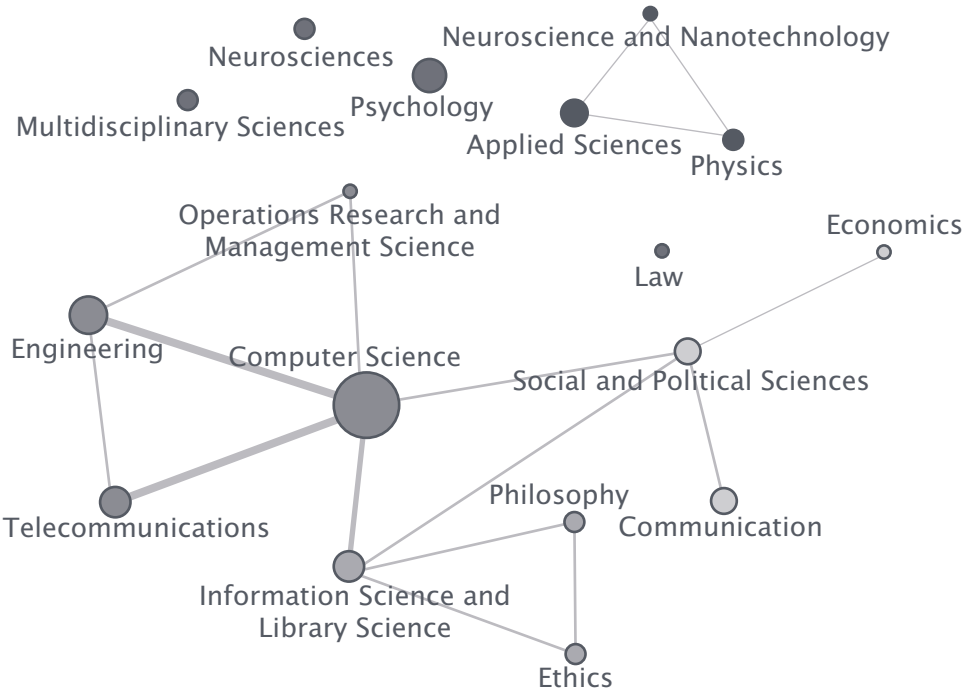
Im nächsten Schritt wurde untersucht, welche Fachrichtungen sich mit dem Thema Social Bots beschäftigen. In der Abbildung III.2 repräsentiert die Größe der farbigen Kreise die Anzahl der Publikationen, die in diesem Forschungsgebiet erschienen sind. Die Verbindungen zwischen den Kreisen zeigen, ob in den Publikationen Themen aus mehreren Forschungsgebieten adressiert werden. Die Linienstärke beschreibt, wie häufig die Forschungsgebiete in den Publikationen gemeinsam adressiert wurden (je dicker, desto häufiger).

Die Erforschung von Social Bots findet an der Schnittstelle von Sozialwissenschaften und Informatik statt. Ferner sind Fachgebiete wie Kommunikationsforschung, Informationswissenschaften, Psychologie oder Soziologie maßgeblich

beteiligt. Der Schwerpunkt der Forschung liegt im Bereich der Informatik. Der entsprechende Kreis repräsentiert mit 30 Publikationen das größte Feld. Eine stärkere wissenschaftliche Kooperation ist anhand der dicken Linien zu den Fachrichtungen Telekommunikation und Ingenieurwissenschaften zu erkennen.

Ende 2016 gab es einige Fachrichtungen, wie Recht, mit lediglich einer Publikation, die zudem nicht vernetzt waren. Im Fachbereich Psychologie wird sich etwas intensiver mit dem Thema beschäftig, dieser ist jedoch ebenfalls nicht interdisziplinär verknüpft. Es kann hieraus geschlussfolgert werden, dass Forschungen in verschiedenen Fachbereichen zu Social Bots angestoßen wurden, sich Vernetzungen zu anderen Fachrichtungen vermutlich aber erst noch etablieren werden.

Abb. III.2 Vernetzung der verschiedenen Fachrichtungen



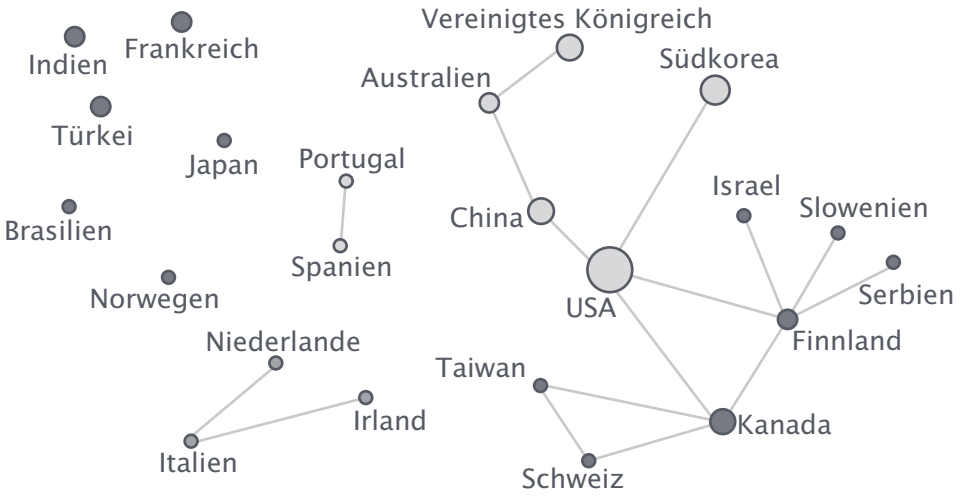
Begriffserläuterungen:
Neurosciences = Neurowissenschaften; Neuroscience and Nanotechnology = Neurowissenschaften und Nanotechnologie; Psychology = Psychologie; Multidisciplinary Sciences = interdisziplinäre Forschung; Applied Sciences = angewandte Forschung; Physics = Physik; Economics = Volkswirtschaftslehre; Operations Research and Management Science = Unternehmensforschung und Betriebswissenschaft; Law = Recht; Engineering = Ingenieurwissenschaften; Computer Science = Informatik; Social and Political Sciences = Soziologie und Politikwissenschaften; Telecommunications = Telekommunikation; Philosophy = Philosophie; Communication = Kommunikationsforschung; Information Science and Library Science = Informations- und Bibliothekswissenschaft; Ethics = Ethik

Eigene Darstellung

Geografischer Forschungsschwerpunkt ist die USA

Die Frage nach geografischen Schwerpunkten der Forschung zu Social Bots und internationalen Forschungskooperationen ist relativ eindeutig zu beantworten. Abbildung III.3 zeigt den stärksten Forschungsschwerpunkt in den USA, die mit wissenschaftlichen Partnern in Kanada, Südkorea, China und Finnland kooperieren. Die Tatsache, dass Deutschland in der Abbildung nicht erscheint, ist einerseits damit zu begründen, dass das Web of Science nur englischsprachige Literatur listet und somit deutschsprachige Texte ausschließt. Andererseits sind die beiden expliziten Forschungsprojekte zu Social Bots in Deutschland noch sehr jung und Publikationen stehen noch aus.

Abb. III.3 Geografische Forschungsschwerpunkte und Kooperationen

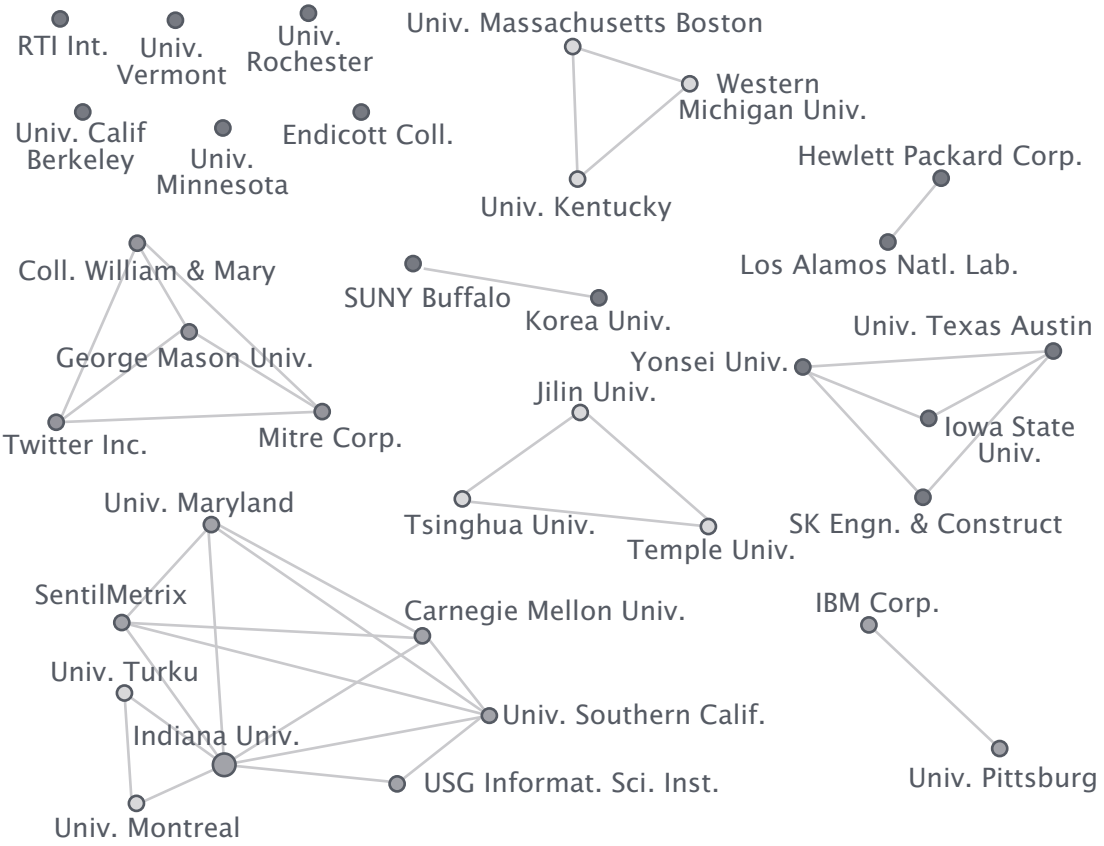


Eigene Darstellung

Mehrere Forschungscluster in den USA

Eine Betrachtung der Forschungskooperationen von Institutionen innerhalb der USA in Abbildung III.4 zeigt, dass sich mehrere kleinere Kooperationscluster aus wissenschaftlichen Institutionen gebildet haben und diese primär national kooperieren. In den meisten Fällen spiegeln die Forschungscluster die Zusammenarbeit an lediglich einer Veröffentlichung wider. Etwas aus dieser Menge heraus sticht die Indiana University mit der Forschungsgruppe um Emilio Ferrara, die sowohl national als auch international am stärksten vernetzt ist. Interessant ist, dass an einigen Publikationen auch Privatunternehmen, wie Twitter, Hewlett Packard und IBM, beteiligt waren.

Abb. III.4 Institutionen in den USA und Kooperationspartner



Eigene Darstellung

Die Analyse der Publikationsdaten des Web of Science hat gezeigt, dass

- die Anzahl wissenschaftlicher Publikationen zu Social Bots noch recht gering ist,
- das Thema erst seit weniger als 5 Jahren in der Forschung an Bedeutung gewinnt,
- das Thema besonders in den Disziplinen Informatik und Sozialwissenschaften beforscht wird und
- es bisher nur wenige internationale Forschungskooperationen gibt.

Social Bots Insights IV.

In einem Experiment sollte überprüft werden, ob es gelingen kann, einen eigenen, funktionsfähigen Social Bot zu erstellen. Angenommen wurde, dass nur geringe Programmierkenntnisse nötig sind und der erforderliche Programmcode im Internet leicht zu finden ist.

Ziel war es, mit diesem Social Bot auf Twitter versandte Nachrichten weiterzuleiten (retweeten). Zu diesem Zweck wurde im Internet nach verfügbaren Programmcodes für Bots gesucht, die auf der für Programmierer einschlägigen Website namens GitHub schnell gefunden werden konnten. Auf Basis eines ausgewählten Codes wurde ein einfacher Bot programmiert, der nach dem Hashtag »#bundestag« suchen sollte und per Zufall eines der Suchergebnisse von Tweets mit »#bundestag« retweetet. Die Funktionsweise des programmierten Bots wird im Anhang 1 erläutert.

Für die Anbindung des Bots an Twitter musste ein Twitteraccount eingerichtet werden. Ursprünglich war es geplant, den Bot mindestens einen Monat lang laufen zu lassen. Da der Betrieb von Bots jedoch gegen die allgemeinen Geschäftsbedingungen (AGB) von Twitter verstößt, wurde der Testzeitraum auf wenige Minuten verkürzt und lediglich erprobt, ob der Bot grundsätzlich lauffähig ist. Nachdem die Funktionsfähigkeit bestätigt werden konnte, wurde der Account sofort wieder deaktiviert.

Dieses kleine Experiment konnte zeigen, dass der Einsatz eines einfachen Twitter-Bots selbst für Laien mit wenigen Programmierkenntnissen mit nur geringem Aufwand auf dem eigenen Computer (mit entsprechender Entwicklungsumgebung) möglich ist. Der Zeiteinsatz zur erfolgreichen Implementierung des Twitter-Bots mithilfe von im Internet verfügbaren Codezeilen (node) und Tutorials (Shiffman 2015) betrug nur wenige Stunden. Spezielle Kenntnisse zur Syntax oder zu den grundlegenden Funktionen einer Kommandozeile waren nicht erforderlich.

Die sozialen Fähigkeiten des hier programmierten Bots waren auf sehr grundlegende Funktionen beschränkt. Bots dieser Kategorie generieren zwar keine Inhalte selbst, könnten aber durch Retweeten oder Liken theoretisch dazu missbraucht werden, bestimmte Hashtags wichtiger erscheinen zu lassen, als es sich aus den menschlichen Aktivitäten bei Twitter ergäbe.

Es ist anzunehmen, dass Webfachleute in kürzester Zeit weitaus komplexere Bots implementieren könnten. Die Skalierung der Bots würde allein durch die Zugangsmöglichkeiten der Application-Programming-Interface-Token (API-Token) beschränkt, die zur Authentifizierung und Anmeldung eingesetzt werden. Bot-Codebeispiele existieren in großer Zahl in verschiedenen Programmiersprachen auf GitHub, sodass ein breites Feld der Programmierergemeinschaft angesprochen werden kann. Die Einstiegshürden sind entsprechend niedrig.

Thesen V.

1. Es gibt lediglich eine begrenzte Anzahl prominenter Beispiele der Einflussnahme durch Social Bots, auf die sowohl in der Presse als auch in wissenschaftlichen Artikeln immer wieder Bezug genommen wird. Der in den Artikeln beschriebene Wirkungsraum ist an erster Stelle Twitter und seltener Facebook. Das Ausmaß der tatsächlichen Einflussnahme ist allerdings kaum belegt.
2. Social Bots werden momentan im Wesentlichen dafür eingesetzt, Diskussionen inhaltlich zu verzerren sowie die Wichtigkeit von Themen oder die Popularität von Personen und Produkten in die Höhe zu treiben. Darüber hinaus werden Personen auch diskreditiert, beleidigt oder zum Kauf von entgeltpflichtigen Diensten im Internet verführt.
3. Social Bots können nur unter bestimmten Voraussetzungen Ergebnisse politischer Entscheidungsprozesse beeinflussen. Eine Voraussetzung ist beispielsweise ein politischer Kulminationspunkt wie eine knappe Entscheidung bei Wahlen. Diese Voraussetzungen können sie selbst nicht schaffen.
4. Social Bots tragen zur Veränderung der politischen Debattenkultur im Internet bei und können durch die massenweise Verbreitung von (Falsch-)Nachrichten zu einer Desinformation und »Klimavergiftung« im öffentlichen Diskurs führen. Social Bots bergen das Potenzial, das Vertrauen in die Demokratie zu unterlaufen.
5. Social Bots haben das Potenzial, das Kunden- und Kaufverhalten Einzelner (über das sogenannte Influencer Marketing) und sogar ganze Märkte (z. B Börsenhandel) zu manipulieren.
6. Social Bots können eine Gefahr für die IT-Sicherheit darstellen. Sie greifen nicht direkt die Hard- oder Software von IT-Systemen an, wie dies bei Hackerangriffen der Fall ist, sondern nehmen den Menschen als potenzielle Schwachstelle der IT-Sicherheit ins Visier und können diesen für Angriffe instrumentalisieren (z. B. durch Links, über die Schadsoftware installiert wird).
7. Social Bots stellen langfristig eine Bedrohung für das Geschäftsmodell von sozialen Netzwerken dar. Ein Teil der Nutzer könnte sich abwenden, weil sie das Vertrauen in die Echtheit der Beiträge verlieren. Investoren verlieren das Interesse, weil sich die Plattformen durch Werbeeinnahmen oder den Verkauf von Nutzerdaten finanzieren, aber nur Menschen Kaufentscheidungen treffen.
8. Social Bots und ähnliche Internetphänomene können auf Dauer dazu führen, dass die Anonymität der Urheber von Algorithmen im Internet

aufgegeben wird, ein Diskurs zur Ethik von Algorithmen angestoßen und ggf. die Entstehung eines kostenpflichtigen und geschützteren Second Internet befördert wird.

9. Der Einsatz von Social Bots muss nicht per se mit negativen Absichten verbunden sein. Es gibt künstlerisch-kreative Beispiele für den Einsatz von Social Bots sowie Ansätze, diese als Lockvogel oder als Gegenmaßnahme zur Bekämpfung von Falschnachrichten einzusetzen. Ferner könnten Sie für ein Nudging, im Sinne einer positiven Beeinflussung menschlichen Verhaltens, eingesetzt werden.
10. Die technischen Möglichkeiten zur Enttarnung von Social Bots sind noch im Entwicklungsstadium. Die Enttarnung hinkt der schnellen Entwicklung von Bots hinterher.

Diese zehn Thesen wurden auf Basis der Literatur- und Quellenanalyse sowie der Interviews mit den Fachexperten formuliert. Sie fassen die wesentlichen Ergebnisse der TA-Vorstudie zusammen. Die Ableitung der einzelnen Thesen wird im Folgenden erläutert.

1. Einfluss und Wirksamkeit von Social Bots

1.1 Beispiele für den Einsatz von Social Bots und deren Wirksamkeit

1. Es gibt lediglich eine begrenzte Anzahl prominenter Beispiele der Einflussnahme durch Social Bots, auf die sowohl in der Presse als auch in wissenschaftlichen Artikeln immer wieder Bezug genommen wird. Der in den Artikeln beschriebene Wirkungsraum ist an erster Stelle Twitter und seltener Facebook. Das Ausmaß der tatsächlichen Einflussnahme ist allerdings kaum belegt.

Bis heute gibt es nur eine überschaubare Anzahl von Beispielen in der wissenschaftlichen Literatur, bei denen der politisch motivierte Einsatz von Social Bots nachgewiesen werden konnte. Die drei am häufigsten in den Experteninterviews, in der wissenschaftlichen Literatur sowie in der Presse genannten Beispiele sind die Social-Bot-Einsätze während der Protestbewegungen in der Ukraine, im Verlauf der Brexit-Kampagnen sowie im US-Präsidentschaftswahlkampf 2016 (Bond et al. 2012; Hegelich 2016; Howard 2016; Howard/Kollanyi 2016; Kollanyi et al. 2016).

Tab. V.1 Prominente Beispiele für den Einsatz von und versuchte Einflussnahme durch Social Bots

Land	politischer Aktionsraum	Jahr	Ersticken von Bewegungen durch Informationsflutung	Propaganda und Meinungsmache	künstliches Aufblähen der Social-Media-Follower
Ägypten	*Protestbewegung* Demonstrationen auf dem Tahir-Platz und Verbreitung von Falschnachrichten über Twitter	2011	X	X	
Mexiko	*Präsidentschaftswahl* sogenannte Peña-Bots, die über Twitter Nachrichten mutmaßlich im Auftrag des Präsidentschaftskandidaten Enrique Peña Nieto verbreiteten	2012	X	X	X
Südkorea	*Präsidentschaftswahl* Aktionen gegen die Gegenkandidaten der Präsidentin Park Geun Hye	2013	X	X	
Syrien*	*Protestbewegung* Eine syrische Nachrichtenagentur flutete den Hashtag der Aufständischen auf Twitter #Syria mit Nachrichten zugunsten der syrischen Regierung	2013	X	X	
Großbritannien	*Brexit-Kampagne* im Vorfeld des Votums zum Verbleib Großbritanniens in der EU, Fluten der Hashtags #StrongerIn und #Brexit mit Nachrichten	2016	X	X	
Ukraine*	*Protestbewegung* 15.000 gesteuerte Twitterbenutzerkonten (Maidan-Krise)	2014	X	X	
USA	*Präsidentschaftswahlen* Kampagnen über Hashtags der Kandidaten	2008 2012 2016		X	X

* vermuteter Einsatz zusammen mit Trollen

Eigene Darstellung basierend auf den Interviews sowie Bilton 2014; Hegelich 2016, S. 5; Howard/Kollanyi 2016, S. 1 f.; Markoff 2017; Murthy et al. 2016, S. 4956; Woolley 2016, S. 5; Woolley/Howard 2016a

Alle diese Social-Bot-Einsätze wurden auf Twitter nachgewiesen. Tabelle V.1 gibt einen Überblick zu weiteren häufig genannten Beispielen von Social-Bot-Aktivitäten. Das Ausmaß scheint jedoch größer zu sein. Die Forscher Howard und Woolley konnten mithilfe ihrer Rechercheplattform politicalbots.org bereits für 18 Länder nachweisen – von Australien über die USA bis Venezuela –, dass dort in den letzten 5 Jahren Social Bots in politischen Prozessen, meist für Wahlkämpfe, betrieben worden sind (Woolley 2016, S. 7).

Nicht immer ist geklärt, ob zusätzlich zu den Social Bots auch Trolle zum Einsatz kamen, was zumindest für das Ukrainebeispiel und Syrien vermutet wird (Interviews Hegelich u. Walter; Elliott 2014).

Das Aufkommen der Bot-Kommunikation zu bestimmten Themen auf Twitter ist dabei durchaus beachtlich. Howard hat nachgewiesen, dass ca. 1,7 Mio. Tweets in einer der TV-Debatten der Kandidaten von Bots generiert wurden (Kelion/Shiroma 2016). Und in einer weiteren Studie konnte gezeigt werden, dass fast 20 % der Tweets auf Twitter im US-Präsidentschaftswahlkampf durch Social Bots verbreitet wurden. Hierbei produzierten ca. 400.000 Social Bots rund 3,8 Mio. Tweets (Bessi/Ferrara 2016). Im weiteren belegten Fall von Social-Bot-Aktivitäten im Ukrainekonflikt wurden von 15.000 Profilen 60.000 Tweets pro Tag abgesetzt (Hegelich 2016, S. 5).

Aus den genannten Beispielen und Forschungsarbeiten leitet sich ab, dass der primäre Wirkungsraum für Social-Bot-Aktivitäten – zumindest momentan – Twitter zu sein scheint. Wirkräume für Social Bots ergeben sich aber grundsätzlich in allen sozialen Netzwerken, die nutzerfreundliche und hürdenfrei zugängliche APIs besitzen, was neben Twitter besonders auf Instagram und Google+ zutrifft (Interviews Hegelich u. Wenzel).

Twitter ist aufgrund seiner sehr geringen technischen Hürden eine von Social Bots hoch frequentierte Plattform, da sie eine leichtere Datenzugänglichkeit im Vergleich zu anderen Plattformen bietet. Hierdurch ergibt sich eine gewisse Schwerpunktsetzung der Forschung auf Twitter, die letztlich aber nicht unbedingt den tatsächlichen Fokus der Social-Bot-Aktivitäten im Internet widerspiegeln muss (Interview Hegelich).

Die Daten von Twitter sind laut den interviewten Wissenschaftlern vergleichsweise leicht zu extrahieren, doch ihre Güte für valide und aussagekräftige Experimente wird durchaus kritisch bewertet. Es wird von Twitter nicht eindeutig dokumentiert, welche und wie viele Daten tatsächlich bei Datenabfragen zur Verfügung gestellt werden (Morstatter et al. 2013, S. 1). Die Forscher merkten zu den Forschungsarbeiten in sozialen Netzwerken ferner an, dass diese zumindest mit Blick auf Experimente – wie etwa den probeweisen Betrieb von Social Bots auf Twitter – rechtlich erschwert sind, weil die allgemeinen Geschäftsbedingungen (AGB) der sozialen Netzwerkanbieter dies untersagen und sie für wissenschaftliche Zwecke auch keine Ausnahmen erlauben (Interview Strohmaier).

Es wird angenommen, dass sich die Unternehmen diesbezüglich nur wenig kooperativ zeigen, weil sie die Forschungsergebnisse als potenziell geschäftsschädigend einschätzen (Interview Pfeffer).

Im Gegensatz zu Twitter sind Social-Bot-Aktivitäten auf Foren von Onlinemedien, wie z.B. SPIEGEL ONLINE, Welt oder Bild, noch weitgehend unbekannt (Interview Walter). Der Nachweis, dass auch hier Social Bots vorkommen, ist ein Ziel des Forschungsprojekts »PropStop« (Interviews Grimme u. Stöcker). Lediglich ein Fall im WDR-Blog wird angeführt, bei dem Einträge über IP-Adressen zu einer Propagandaplattform der Terrorvereinigung Islamischer Staat (IS) zurückverfolgt werden konnten (Interview Welchering). Bis heute scheinen Foren aufgrund der technischen Hürden, wie z.B. die fehlende API und durch Captcha-Abfragen (completely automated public Turing test to tell computers and humans apart), noch besser als soziale Netzwerke vor dem Einschleusen von Social Bots geschützt zu sein (Interview Fuchs). Dies mag auch der Grund dafür zu sein, dass auf den Webseiten der großen Verlage in den Kommentierungen zu Artikeln eher Trolle als Social Bots aktiv sind (Interview Walter).

Der überwiegende Tenor in den Interviews mit den wissenschaftlichen Experten war, dass von den Social Bots eine Gefahr ausgeht, es bisher jedoch keine wissenschaftlichen Studien gibt bzw. nur sehr wenige Hinweise vorliegen, dass die Beeinflussung von großen gesellschaftlichen Gruppen durch Social Bots tatsächlich gelingt (Interviews Grimme, Hegelich, Janetzko u. Strohmaier).

Einsatzgebiete 1.2

2. Social Bots werden momentan im Wesentlichen dafür eingesetzt, Diskussionen inhaltlich zu verzerren sowie die Wichtigkeit von Themen oder die Popularität von Personen und Produkten in die Höhe zu treiben. Darüber hinaus werden Personen auch diskreditiert, beleidigt oder zum Kauf von entgeltpflichtigen Diensten im Internet verführt.

Wesentliche Einsatzgebiete für Social Bots waren bislang Wahlkämpfe, Proteste oder der Versuch, politische Strömungen zu beeinflussen. Dabei werden die Social Bots bis jetzt für drei Ziele eingesetzt: erstens für das Ersticken oppositioneller Gegenmeinungen durch das Fluten von Hashtags mit ablenkenden, polarisierenden oder banalen Nachrichten, zweitens die Verbreitung von Propaganda und Meinungsmache sowie drittens das künstliche Erzeugen hoher Followerzahlen auf Twitter zum Unterstreichen der eigenen Position (Woolley 2016, S. 7).

In den Foren der deutschen Parteien scheinen Social Bots – im Vergleich zu den USA – noch keine gewichtige Rolle zu spielen. Dennoch gibt es seit

2012/2013 Beobachtungen zu Unregelmäßigkeiten der Twitterbenutzerkonten einzelner Politiker. So kam es vereinzelt zu massiven Anstiegen von Followern bei Spitzenpolitikern, deren Ursprung sich nicht erklären ließ (Hauck 2012; Heinrich 2016; Thomas 2013; Voß 2013). Beim Twitterbenutzerkonto von Bündnis 90/Die Grünen wurden im Jahr 2015 ebenfalls sprunghafte Anstiege verzeichnet. Dies wurde an Twitter gemeldet und die neuen Follower daraufhin gelöscht. Laut Interviewpartner hat sich das Prozedere zur Kontaktaufnahme mit Twitter seitdem jedoch deutlich erschwert, weil das Unternehmen in Deutschland keine Kontaktperson mehr stellt (Heinrich 2016). Zudem konnten Social-Bot-Aktivitäten auf den Websites der Parteien während der Flüchtlingswelle 2015, insbesondere bei der damit verbundenen Debatte in der CSU beobachtet werden (Interviews Dudzak u. Wenzel). Die Erfahrungen der Parteien mit Social Bots führten dazu, dass die redaktionelle Überwachung der Foren/Kommentarbereiche demnächst zumindest in einigen Fraktionen auch softwaregestützt durchgeführt werden soll.

Aktuell sind die anlassbezogenen Aktivitäten von Social Bots in sozialen Medien die augenfälligste Form der Beeinflussung (Interview Welchering). Damit verbundene Gefahren bestehen in der bereits zuvor beschriebenen direkten Einflussnahme auf politische Debatten. Gegenwärtige Risiken durch Social Bots ergeben sich ferner im Bereich Cybermobbing, indem Einzelpersonen per Bots mit diskreditierenden Botschaften persönlich beleidigt und belästigt werden (Interview Neumann).

Neben Risiken für politische Prozesse sind auch Gefahren für wirtschaftliche Abläufe ins Auge zu fassen. Hierfür gibt es bis heute nur wenige belegte Beispiele: In einem vielpublizierten Fall wurde im Jahr 2014 der Börsenkurs des Technologieunternehmens Cynk durch Social Bots künstlich per Tweets in die Höhe getrieben. Automatisierte Tradingalgorithmen nahmen die über Twitter verbreiteten Gerüchte auf und investierten in Cynk, bis der Marktwert um das 200-Fache auf rund 6 Mrd. US-Dollar stieg. Nach der Entdeckung wurde der Börsenhandel der Aktie ausgesetzt und es kam zu realen Verlusten für die Käufer (Ferrara et al. 2014, S. 99; Fiegerman 2014). Laut einem Interviewpartner berichtet auch das Bonner FinTech-Unternehmen Stockpulse GmbH von wiederholten Versuchen, bei denen Börsenvorgänge mittels der Verbreitung von Nachrichten über Social Bots manipuliert wurden. Stockpulse analysiert Daten aus sozialen Medien, bereitet diese auf und verkauft diese an Anleger zur Beurteilung von Wertpapieren und hat somit einen guten Einblick in die Vorgänge sozialer Medien (Interview Janetzko).

Ein zweiter vielpublizierter Fall behandelt Fakeprofile auf der US-amerikanischen Onlinedatingplattform Ashley Madison. Im Jahr 2015 berichtete die Bloggerin Annalee Newitz davon, dass sie über 70.000 gefälschte Profile auf der Plattform identifizieren konnte. Diese Social Bots gaben vor, Frauen zu sein und

verwickelten Männer in kostenpflichtige Chatgespräche (Newitz 2015). Der kanadische Betreiber Avid Life Media bestätigte, tatsächlich Social Bots verwendet zu haben, doch er verkündete auch, dass er diese Vorgehensweise auf all seinen international betriebenen Plattformen mittlerweile wieder eingestellt hätte (ZEIT ONLINE 2016).

Sowohl Bitkom e.V. als auch der Bundesverband Digitale Wirtschaft (BVDW) e.V. konnten keine Aussagen dazu machen, ob ihre Verbandsmitglieder von Social-Bot-Angriffen schon betroffen waren oder diese Social Bots gezielt selbst nutzen, beispielsweise um eigene Produkte in Kommentaren zu bewerben (Interviews Kossol u. Lutter). Letztlich war keinem der Interviewpartner eine Einschätzung zur allgemeinen Schadenshöhe – bis auf das dokumentierte Beispiel Cynk – möglich.

Die interviewten Experten bestätigten, dass Social Bots in den sozialen Netzwerken sehr weitverbreitet sind, wenngleich nur grobe Schätzungen vorliegen, wie viele Bots auf Onlineportalen tatsächlich aktiv sind. Die Angaben der Experten und in der Literatur variieren: Der Social-Bot-Forscher Simon Hegelich geht davon aus, dass es weltweit 100 Mio. aktive Social Bots gibt. Weiteren Expertenschätzungen zufolge könnten ca. 30 bis 35 Mio. Benutzerkonten auf Facebook Social Bots sein (ca. 1,8 bis 2,1 %) sowie 62 bis 80 Mio. der Twitterprofile (ca. 20 bis 25 %) (Interviews Fuchs, Helbing, Pfeffer, Sander u. Welchering; Statista GmbH 2016b, S. 29). Haustein et al. (2016, S. 233) sind bei ihrer Studie über Twitter von 10 bis 16 % ausgegangen, und Breithut (2016) zitiert in einem Bericht Zahlen von Facebook, wonach es rund 15 Mio. Bot-Benutzerkonten gibt, wobei sich darunter auch unterstützende Bots befinden, die etwa Wetterberichte und Lokalnachrichten versenden. Auf die Frage, wie groß der Anteil von Social Bots an den Nutzern ist, antwortete Facebook, dass die Aktivitäten mit betrügerischen Absichten im Vergleich zu den Gesamtaktivitäten sehr gering ausfallen (»Fraudulent activity has always been a tiny fraction of overall activity on Facebook.«) (Interview Facebook).

Unklar ist dabei, wie hoch der Anteil der Social Bots am gesamten Bot-Aufkommen ist. Einen Anhaltspunkt zu generellen Bot-Aktivitäten im gesamten Internetverkehr bietet eine Untersuchung des US-amerikanischen IT-Sicherheitsunternehmens Imperva, das nach eigenen Angaben mittlerweile im fünften Jahr das Vorkommen von Bots im Internet analysiert. Zu Bots zählen sowohl gute (z.B. Suchmaschinen und Webcrawler) als auch schlechte Bots, die unerlaubt Daten sammeln, Spams versenden oder automatisiert Identitätsüberprüfungen umgehen und für DDoS-Attacken eingesetzt werden (Impersonator).

Imperva wertete dazu im vergangenen Jahr gemäß den Angaben auf ihrer Website 16,7 Mrd. Anfragen auf 100.000 zufällig ausgewählte Internetdomänen »aus dem Incapsula Netzwerk« (genauere Angaben hierzu fehlen) aus und kam zu dem Ergebnis, dass über 50 % des Onlineverkehrs von Bots bestritten wer-

den. Davon stammten rund 23 % von guten und 29 % von schlechten Bots. Das Verhältnis von guten zu schlechten Bots hat sich entsprechend der Untersuchungsergebnisse seit 5 Jahren kaum verändert, jedoch leicht zugunsten der guten Bots verschoben (Zeifman 2017). Daraus folgt, dass das Bot-Aufkommen im Internet vergleichsweise hoch ist, genaue Aussagen zum Anteil der Social Bots unter den schlechten Bots lassen sich hieraus jedoch nicht ableiten.

Auch wenn die Schätzungen und Angaben zum Ausmaß der Bots und insbesondere Social Bots auseinandergehen, so sind sich die Forscher einig, dass schon heute die technischen Voraussetzungen für den großflächigen Einsatz von Social Bots in Form von Bot-Armeen gegeben sind, was auf ihr mögliches Gefahrenpotenzial schließen lässt (Interviews Hegelich, Neumann u. Strohmaier).

Prämissen für die Beeinflussung politischer Entscheidungsprozesse 1.3

3. Social Bots können nur unter bestimmten Voraussetzungen Ergebnisse politischer Entscheidungsprozesse beeinflussen. Eine Voraussetzung ist beispielsweise ein politischer Kulminationspunkt wie eine knappe Entscheidung bei Wahlen. Diese Voraussetzungen können sie selbst nicht schaffen.

Es bedarf eines politischen Kulminationspunktes oder starker Trends

Social Bots setzen in politischen Diskussionen im Internet in der Regel keine eigenen Trends, sondern erkennen vorhandene Trends und nutzen diese als Vehikel zur Verbreitung von Meinungen (Interviews Neumann u. Pfeffer). Potenziell einflussreich scheinen sie im Zusammenhang mit politischen Kulminationspunkten zu sein, wenn es in politischen Entscheidungsprozessen um knappe Mehrheiten geht, so, wie dies im Wahlkampf zwischen Clinton und Trump oder der Brexit-Kampagne zu beobachten war. Fernsehduelle im Wahlkampf bieten einen Anlass, um währenddessen oder kurz im Anschluss der Sendungen per Social Bots Meinungen zu verbreiten (Bessi/Ferrara 2016).

Bestimmte soziale Gruppen schenken sozialen Medien mehr Vertrauen als traditionellen Informationsquellen

Ob Social Bots wirken können und bei wem, hängt auch davon ab, mithilfe welcher Medien eine Meinungsbildung erfolgt. Diese scheint zunehmend über soziale Medien stattzufinden (Interview Fuchs). Dies wird vom Hans-Bredow-

Institut in einer Studie zur Nutzung digitaler Nachrichten bestätigt (Hölig/Hasebrink 2016). Unter den befragten Internetnutzern zeigte sich im Jahr 2016 eine zunehmende Medien- und Nachrichtenskepsis. Immerhin vertraut ca. ein Fünftel der Befragten den Nachrichten nicht, wobei jüngere Altersgruppen noch skeptischer als ältere sind (allerdings verweisen die Autoren auf einen möglichen Einfluss der Ereignisse im Befragungszeitraum Anfang 2016). Nachrichten werden weniger langfristig als anlassbezogen rezipiert, und das Nachrichteninteresse sinkt insgesamt. Besonders in der Gruppe der 18- bis 24-Jährigen ist die Nachrichtennutzung im Vergleich zur Vorjahresbefragung zurückgegangen. Fernsehen und Radio sind dennoch nach wie vor die mit Abstand am meisten genutzten Quellen für Nachrichten. Allerdings haben soziale Netzwerke mit einem Plus an 6 Prozentpunkten innerhalb eines Jahres auf 31 % (Anteil der Befragten, die das Medium regelmäßig als Nachrichtenquelle verwenden) erstmalig Zeitungen mit 29 % überholt. Unter den sozialen Netzwerken wird Facebook mit Abstand am häufigsten für Nachrichten genutzt und liegt mit 27 % der Befragten deutlich vor Twitter mit 4 %. Die Ergebnisse zeigen, dass Nachrichtennutzung nach wie vor über eine Vielzahl an Kanälen erfolgt, soziale Medien aber eine immer wichtigere Rolle für die Meinungsbildung spielen und sich hierdurch ein Einfallstor für technisch-basierte Manipulationen ergeben kann (Fuchs 2016a).

Um der Frage nachzugehen, von wem soziale Medien genutzt werden, hat die OECD deren Gebrauch in Abhängigkeit vom Bildungsgrad ermittelt. In allen Ländern Europas werden soziale Medien überwiegend von höheren Bildungsschichten genutzt – überraschenderweise ist allein in Deutschland das Verhältnis umgekehrt (OECD 2015, S. 146), was auf eine grundsätzliche Skepsis der Bildungseliten in Deutschland gegenüber soziale Medien hindeuten könnte.

Es gibt Hinweise darauf, dass Twitter vor allem Eliten und Entscheidungsträgern gefällt (Bennet 2012) und die Nutzer bei Twitter im Vergleich zu Facebook, Instagram oder LinkedIn über einen höheren Bildungsgrad verfügen (Greenwood et al. 2016). Ob das auch für Deutschland zutrifft, kann nicht genau beantwortet werden, da hierzu bislang widersprüchliche Zahlen vorliegen (Statista GmbH 2009 u. 2016b, S. 32).

Unabhängig von den Zahlen zum Bildungsgrad ließ sich in den vergangenen Jahren beobachten, dass soziale Netzwerke vermehrt von Politikern, Journalisten und seit ca. 1 bis 2 Jahren von der Polizei genutzt werden (Interview Walter; Laufersweiler 2015). Die Bundespolizei ist allein mit zehn Benutzerkonten, verschiedene Bundesländer sind mit mehr als einem Twitterkonto der Polizei vertreten, z.B. Nordrhein-Westfalen mit neun, Rheinlandpfalz mit sieben und Mecklenburg-Vorpommern mit sechs Twitterkonten (Statista GmbH 2016b, S. 44).

Insbesondere Politiker nutzen das Medium Twitter vermehrt für die Darstellung eigener Positionen und Anmerkungen (Fuchs 2016b; Seibt 2015). Im Ranking der Politiker 2016 stand Peter Altmaier an erster Stelle mit rund 128.000 Followern, gefolgt von Sarah Wagenknecht, Dr. Gregor Gysi, Dr. Peter Tauber sowie Sigmar Gabriel mit jeweils rund 100.000 Followern (Statista GmbH 2016b, S. 40). Wenngleich der potenzielle Wirkungsraum von Twitter auf der einen Seite relativ begrenzt ist, weil Twitter in Deutschland mit rund 5,08 Mio. aktiven Nutzern im Jahr 2015 von einem vergleichsweise kleinen Kreis genutzt wird (Statista GmbH 2016b, S. 29), scheinen auf der anderen Seite das Risiko der Manipulation von Meinungsbildnern und das damit verbundene Multiplikatorpotenzial umso größer, wenn diese Plattform primär von Entscheidungsträgern frequentiert wird (Interview Walter).

Medien oder andere Institutionen leisten einen Beitrag zur Verbreitung und Validierung der Nachrichten aus sozialen Netzwerken

Eine Meinungsmanipulation kommt vor allem dann zum Tragen, wenn Falschnachrichten von Journalisten oder anderen öffentlichen Personen und Institutionen verbreitet und durch deren Berichterstattung in traditionellen Medien als glaubwürdig ausgewiesen werden (Interview Grimme; Laufersweiler 2015). Die in den sozialen Medien in Trending Topics diskutierten Themen werden durch Journalisten und Politiker oftmals aufgegriffen und schaffen es dann, als wahrgenommene Empörungswellen, in die Medien und somit in den Fokus öffentlicher Debatten zu kommen (Interview Fuchs; Weck 2016). Befördert wird diese Entwicklung dadurch, dass das Internet zu einer der wichtigsten und auch kostengünstigsten Recherchequellen für den Journalismus geworden ist.

Die offene Programmierschnittstelle Application Programming Interface der sozialen Netzwerke ermöglicht erst den Zugang von Social Bots

Eine weitere Prämisse für die Verbreitung von Social Bots sind die Programmierschnittstellen, die den Bots den Zugang zu sozialen Netzwerken erleichtern. Die Application Programming Interface (API) eines sozialen Netzwerks bietet über einen Programmcode einen Zugang zu den Funktionen dieses Netzwerks (beispielsweise Posten, Liken, Folgen, Suchen etc.). Das Verhalten des Social Bots wird in einer geeigneten Programmiersprache, beispielsweise JavaScript, Python oder Ruby, implementiert. Der Social Bot wird somit außerhalb des so-

zialen Netzwerks ausgeführt und interagiert mit diesem über die Programmierschnittstelle (Interview Hegelich).

Die Betreiber sozialer Netzwerke haben ein Interesse daran, diese Programmierschnittstellen möglichst einfach zugänglich zu machen, um für Applikationsentwickler attraktiv zu sein. Je einfacher die Registrierung von neuen Nutzern ist, desto attraktiver wird das soziale Netzwerk für Applikationsentwickler und damit auch für den Einsatz von Social Bots.

Die Erstellung von Social Bots ist legal, bestimmte Anwendungen sind es nicht

Die Erstellung von Social Bots (Programmierung, massenweises Erstellen von Benutzerkonten, Verbreitung von Botschaften) ist nach deutschem und US-amerikanischem Recht legal. Einzelne Aktionen von Social Bots, beispielsweise das Posten oder Retweeten eines einzelnen Tweets, stellen keinen Straftatbestand dar. Der Betrieb der Social Bots auf den Plattformen der sozialen Netzwerke hingegen verstößt gegen die AGB dieser Unternehmen (Interviews Heinrich, Neumann u. Facebook).

Durch die Anwendung von Social Bots ausgelöste Straftatbestände liegen mutmaßlich vor allem im Bereich der Wirtschaftskriminalität wie Betrug, unlauterer Wettbewerb sowie unerwünschte Werbung/Spams (Interviews Kriegeskorte, Pfeffer u. Sachweh). Darüber hinaus könnten weitere Straftatbestände berührt sein, wie z.B. Volksverhetzung, Verletzung der Privatsphäre, Identitätsdiebstahl oder Vortäuschung falscher Fakten (Interview Helbing; Fuchs 2013).

Verbreitung und Reichweite der Social Bots sind eng an die Popularität der sozialen Netzwerke geknüpft

In Nordamerika sind Twitter und Facebook für den Einsatz von Social Bots aufgrund der im Vergleich zu Deutschland höheren Marktdurchdringung und Nachfrage sehr attraktiv, im russischsprachigen Raum erfolgt der Einsatz von Social Bots oft über das dort sehr populäre Netzwerk VKontakte.

Twitter könnte zukünftig jedoch an Bedeutung verlieren. Das Unternehmen erzielte nicht die erwünschten Wachstumsraten, meldete bereits Anfang des Jahres 2016 Verluste, und das erst 2012 eröffnete und im Januar 2016 erweiterte Berliner Büro wurde im Oktober 2016 wieder geschlossen (morgenpost.de 2016). Der Börsenkurs von Twitter verlief in den vergangenen Jahren rückläufig, auch die potenziellen Übernahmen von Twitter durch Microsoft, Google und Disney sind im Jahr 2016 gescheitert (SPIEGEL ONLINE 2016). Als ein möglicher Grund wird das vergleichsweise hohe Aufkommen von Hasskommentaren

auf Twitter vermutet, die zwar nicht ausschließlich von Social Bots verbreitet werden, aber zumindest dazu beitragen (Damm 2016). Es wäre nicht völlig ausgeschlossen, dass Twitter mittelfristig sogar aus dem Markt wieder ausscheidet.

Zukünftige Einflusspotenziale und Einsatzmöglichkeiten von Social Bots 2.

In Kapitel V.1 wurden die aktuell belegten Beispiele für den Einsatz von Social Bots beschrieben. In diesem Kapitel V.2 liegt der Schwerpunkt darauf, welche Einsatzmöglichkeiten und Einflusspotenziale von Social Bots zukünftig erwartet werden.

Einflusspotenzial auf politische Prozesse 2.1

4. Social Bots tragen zur Veränderung der politischen Debattenkultur im Internet bei und können durch die massenweise Verbreitung von (Falsch-) Nachrichten zu einer Desinformation und »Klimavergiftung« im öffentlichen Diskurs führen. Social Bots bergen das Potenzial, das Vertrauen in die Demokratie zu unterlaufen.

Das zukünftige von Social Bots ausgehende Einflusspotenzial wird von den Experten unterschiedlich bewertet. Die Einschätzungen reichen von eher marginal über hoch bis hin zu das Internet und die demokratische Gesellschaft zersetzend.

Der Sprecher des Chaos Computer Clubs schätzt das zukünftige Einflusspotenzial eher gering ein, weil Social Bots und deren Botschaften gleichgesetzt werden könnten mit Telefonanrufen im Wahlkampf oder Spams und Phishingnachrichten per E-Mail. Hier bedürfe es lediglich eines sensibleren Umgangs mit Informationen (Interview Neumann).

Die Mehrzahl der interviewten Experten bewertet das mögliche Einflusspotenzial auf politische und auch wirtschaftliche Prozesse hingegen als deutlich höher. Ein Interviewpartner drückt seine Sorge aus, dass die Gefahr der Meinungsbeeinflussung durch Social Bots bislang eher noch verharmlost wird (Interview Sachweh). Die interviewten Experten sehen im Wesentlichen die folgenden vier Einflusspotenziale (Bessi/Ferrara 2016, S. 6; Ferrara et al. 2016, S. 96 f., 2016, S. 1 f.; Hegelich 2016, S. 3 f.; Woolley 2016, S. 3).

Verbreitung von Nachrichten zur Manipulation von Trends

Die in den sozialen Netzwerken gesammelten Daten werden zunehmend kommerziell analysiert, um daraus Trendaussagen zum Verhalten der Nutzer und deren Vorlieben abzuleiten oder um Hinweise zur Popularität der eigenen Person oder von Firmenprodukten zu bekommen. Wenn massenhaft Nachrichten mit manipulierenden Botschaften verbreitet oder Follower auf Twitter bzw. Friends auf Facebook sowie Retweets und Likes vorgetäuscht werden, können Trends entstehen, die aufgrund der manipulierten Datenlage zu Fehlinterpretationen führen.

Zum Beispiel werden Nachrichten durch das massenhafte und manipulative Like-Setzen anderen Nutzern in der Timeline verfügbar gemacht, weil diese durch den Algorithmus von Facebook als für Dritte interessant bewertet werden. Zudem könnten künstlich sogenannte Trending Topics auf Twitter erzeugt werden oder eine Popularität von Benutzerkonten vortäuschen (Ford et al. 2016, S. 4892).

Diese Form der Manipulation funktioniert laut Expertenmeinung besonders in Deutschland aufgrund der gegenüber den USA geringeren Nutzerzahlen auf Twitter und Facebook sehr gut. Es könnten somit Themen in die öffentliche Debatte rücken, die ohne Social Bots keine oder nur wenig Relevanz hätten.

Hinzu kommt, dass nur wenige Social Bots ausreichen, um das Spektrum der gezeigten Nachrichten in sozialen Netzwerken zu verändern. Simon Hegelich konnte in Zusammenarbeit mit Benedikt Walter nachweisen, dass nur vier Social Bots durch das Liken von Kommentaren genügen, gezielt Botschaften zum Trend werden zu lassen, die dadurch verstärkt in den Nachrichtenstreams anderer Nutzer erscheinen. Es handelte sich dabei um Nachrichten auf Facebook, die Pegida- und AfD-affine Themen umfassten. Nutzer, die ohnehin schon eine Nähe zu flüchtlings- und europafeindlichen Themen haben, kommen auf diese subtile Art und Weise verstärkt mit fremdenfeindlichen Meinungen in Berührung, die ihre eigenen Meinungstendenzen verstärken können (Interview Walter).

Manipulation und Polarisierung von politischen Debatten und Diskursen

Der politische Diskurs, der früher ausschließlich in traditionellen Medien (Radio, TV, Zeitungen) stattfand, wird heutzutage durch einen Diskurs in den sozialen Medien, besonders durch Twitter, als ein neues Instrument der politischen Kommunikation ergänzt (Ford et al. 2016, S. 4892; Seibt 2015). Die interviewten Experten befürchten, dass Social Bots die Informationslage in den sozialen Medien und indirekt auch in den traditionellen Medien verfälschen (Interviews Pfeffer, Quandt u. Strohmaier).

Die Manipulation und Beeinflussung politischer Debatten könnten langfristig zur Unterminierung des Vertrauens in die Demokratie und demokratischer Prozesse führen und zu einer Gefahr für die innere Sicherheit werden (Interviews Fuchs u. Quandt). Daher sei es wichtig, dass insbesondere Behörden und politische Verantwortungsträger Falschmeldungen nicht dafür verwenden, um ihre Autorität und Glaubwürdigkeit zu behalten (Interview Pfeffer). Es könnten sich verstärkt manipulierte Nachrichten über die sozialen Medien verbreiten, die nationalen Interessen widersprechen bzw. nicht mehr unter dem Einfluss der Medien oder Regierungsinstitutionen stehen (Interview Strohmaier).

Mit Blick auf die Bundestagswahl 2017 müsste deshalb berücksichtigt werden, dass wichtige und unter Umständen wahlentscheidende Debatten online geführt werden und dadurch verstärkt der Beeinflussung durch Social Bots ausgesetzt sein könnten (Interview Dudzak). Darüber hinaus könnten anlassbezogene politische Diskurse durch ein massenhaftes Auftreten von Social Bots zum Erliegen kommen, wenn Hashtags gekapert oder Kommentarspalten mit nicht zur Diskussion gehörenden Spams geflutet würden. Dies könnte potenzielle Leser und Kommentatoren abschrecken, sich weiterhin an den Diskursen zu beteiligen (Interview Fuchs).

Social-Bot-Aktivitäten könnten ferner zu einer Radikalisierung beitragen, da sie wie Katalysatoren den Boden für extreme Meinungen bereiten, indem sie gemäßigte Meinungen aus den Debatten verdrängten und radikalen Gruppierungen ein Gefühl der Mehrheit gäben, aus dem diese eine Legitimation ableiteten (Interview Sander). Extremmeinungen könnten betont, gemäßigte Meinungen marginalisiert werden (Interview Heinrich). Außerdem könnten sie zur Bildung von Filterblasen und dadurch zu einer Fragmentierung gesellschaftlicher Gruppen und damit der öffentlichen Meinung beitragen (Interview Quandt). Beispielsweise würden in den AfD- und Pegida-Netzwerken bei Facebook Gerüchte und Meinungen gestreut, welche die Gefühlslage der Leser beeinflussten. Hierdurch würden laut Experten vorhandene Frustration und Wut der Nutzer geschürt. Diese bewegten sich zunehmend in einer isolierten Meinungsblase, zu der Social Bots Botschaften beitrügen. Wenngleich Social Bots nicht die alleinigen Auslöser für fremdenfeindliche Einstellungen und für daraus resultierendes Verhalten sind und es auch eher unwahrscheinlich ist, dass Menschen ihre Wahlentscheidungen allein nach einem Meinungsbild auf Twitter ausrichten, könnten sie zumindest dazu beitragen (Interview Walter; Amann et al. 2016, S. 45).

Verbreitung von Falschinformationen und Gerüchten in Krisensituationen

Die Gesellschaft könnte durch die Nutzung von Social Bots in Krisensituationen destabilisiert und verunsichert werden. Es besteht die realistische Gefahr, dass in

akuten Krisensituationen gezielt Verwirrung gestiftet wird oder Social Bots für Rekrutierungsprozesse und die Verbreitung von religiöser Propaganda genutzt werden (Interview Quandt). Ein Beispiel, wie Verwirrung und Unruhe gestiftet werden können, ist der Vermissten- und angebliche Missbrauchsfall des russlanddeutschen Mädchens Lisa im Januar 2016, der zu diplomatischen Spannungen zwischen Russland und Deutschland führte (Amann et al. 2016, S. 45). Allerdings ist in diesem Beispiel eine Beteiligung von Social Bots nicht nachgewiesen worden.

Die Verbreitung von massenhaften Falschnachrichten wäre auch deshalb problematisch, weil psychologisch bedingt ein größerer Glaube an den Wahrheitsgehalt einer Nachricht entsteht, je häufiger die gleiche Botschaft zu lesen ist (Interview Stöcker). Besonders terroristische Gruppierungen wären in der Lage, dieses Potenzial auszunutzen (Interview Hegelich) Die Gefahren für die innere Sicherheit könnten an den belegten Auswirkungen von Falschmeldungen auf Twitter im Kontext des Münchener Attentats im Juli 2016 auf dem Gelände des Olympia-Einkaufszentrums abgelesen werden. Es kursierten zahlreiche Falschmeldungen (z. B. »Schüsse am Stachus«, »Schüsse am Marienplatz«, »Schüsse am Isartor«), die von den Medien aufgegriffen und über Twitter weiterverbreitet wurden, wodurch Verunsicherung entstand.

In kritischen Situationen steigt das Informationsbedürfnis, gleichzeitig sind Zeitfenster für Reaktionen sehr klein. Dies begünstige die Verbreitung von Fehl- und Falschmeldungen und beeinträchtige im ungünstigen Fall das Sicherheitsgefühl in der Gesellschaft (Interviews Hegelich u. Janetzko).

Schaffen künstlicher Anlässe

Neben der kurzfristigen, anlassbezogenen Einflussnahme scheint vor allem die langfristige Beeinflussung der öffentlichen Meinung ein Gefahrenpotenzial darzustellen. Ziel von Social Bots in diesem Sinne wäre die dauerhafte verdeckte Beeinflussung der öffentlichen Meinung im Internet (Hegelich 2016, S. 4). Es wird ferner angenommen, dass künstlich Anlässe geschaffen werden könnten, um dadurch Trends in den sozialen Medien zu erzeugen, um diese als Foren für die Verbreitung von Propaganda auszunutzen (Interview Welchering).

Ein Beispiel dafür, wie künstlich Anlässe geschaffen werden können, ist die in den sozialen Medien entfachte Diskussion über Angela Merkels im letzten Wahlkampf in einem Fernsehduell getragene Halskette mit den Farben Schwarz-Rot-Gold, die als »Deutschlandkette« bezeichnet wurde. Das Thema wurde auch von traditionellen Medien aufgegriffen und schien zuweilen wichtige Themen des Wahlkampfs zu überlagern. Auch wenn hinter diesem Hype mutmaßlich Menschen und keine Social Bots standen (Interview Anonym).

Einflusspotenzial auf wirtschaftliche Prozesse 2.2

5. Social Bots haben das Potenzial, das Kunden- und Kaufverhalten Einzelner (über das sogenannte Influencer Marketing) und sogar ganze Märkte (z. B. Börsenhandel) zu manipulieren.

Ein weiteres potenzielles Anwendungsfeld für Social Bots besteht im Bereich des Influencer Marketings, bei dem kommerzielle Agenturen damit beauftragt werden, Tweets und Kommentare zu posten bzw. Likes zu setzen (Interviews Sander u. Walter; Schieb 2016). Zwar ist der Einsatz von Social Bots im Bereich Influencer Marketing noch unbekannt, doch dessen Automatisierung ist durchaus realistisch (Interview Kossol) und aufgrund der Umsatzstärke dieses Bereichs attraktiv (Interview Stöcker). Beim Influencer Marketing handelt es sich um gezielte Marketingmaßnahmen im Internet, um Nutzer in ihrer Kaufentscheidung positiv zu beeinflussen und für ein Produkt oder eine Marke einzunehmen. Eine Strategie dabei ist, gezielt Influencer zu einem Thema zu identifizieren, wie z. B. Blogger, Social-Media-Meinungsführer oder Journalisten. Diese prägen dann über ihre Beiträge in den sozialen Medien die Meinungen oder wirken als Markenbotschafter und Multiplikatoren. Speziell die Social-Media-Meinungsführer üben in den sozialen Medien wie Twitter, Facebook, Instagram oder YouTube in Form von eigenen Beiträgen, Kommentaren, Meinungen oder Weiterleitung von Postings einen Einfluss aus. Sie zeichnen sich durch eine große Anzahl von Followern aus und erhalten meist viel Resonanz in Form von Likes, Shares und Kommentaren auf ihre Beiträge. Sogenannte Blogger-Relations-Manager stellen den Kontakt zu Influencern her.

Wird der Begriff etwas weiter gefasst, zählen dazu auch Personen ohne nachgewiesenen großen Einfluss, die im Internet, beispielsweise auf Amazon, Bewertungen zu einem Produkt abgeben und damit die Kaufentscheidung anderer beeinflussen können. Das Influencer Marketing wird seit ca. 10 Jahren durchgeführt und ist mittlerweile eine etablierte Marketingmaßnahme (Interview Kossol). Unternehmen könnten Social Bots zu Werbezwecken im Rahmen von Produktlaunches einsetzen, beispielsweise um die Markteinführung eines neuen Autos auf verschiedenen Kanälen zu bewerben. Diese Vorgehensweise wäre möglicherweise verdeckte Werbung, da für den Nutzer sich diese kaum von Nachrichten unterscheiden würden (Interview Quandt).

Social Bots könnten zudem mit wirtschaftskriminellen Absichten eingesetzt werden. Dies beträfe insbesondere die Manipulation von börsennotierten Finanzprodukten im Sinne einer Marktmanipulation (Interviews Kriegeskorte u. Wenzel). Die Störung von Finanzmärkten hätte vielfältige Auswirkungen auf die verschiedenen Bereiche der Wirtschaft; der Schutz des Vertrauens in die Integrität der Finanzmärkte würde gestört. Das Bundeskriminalamt hat im

Interview für den Bereich Wirtschaftskriminalität drei mögliche Szenarien definiert:

- *Social Bots könnten den Aktienwert gezielt durch Falschmeldungen nach oben treiben, in der Regel aber eher nach unten sinken lassen.* Hierzu werden Unternehmen durch Falschmeldungen in Misskredit gezogen (bzw. hoch gelobt). Wenn Falschmeldungen gehäuft im Internet kursieren, werden diese mit größerer Wahrscheinlichkeit von Privatanlegern gelesen oder von Multiplikatoren aufgegriffen und weiterverbreitet. Die potenziellen Anleger treffen auf dieser Basis eine Investmententscheidung. Die Einnahmen werden beispielsweise durch abgeschlossene Optionen auf den Verlauf des Börsenkurses realisiert, die dann eingelöst werden, wenn sich der Kurs in die gewünschte Richtung bewegt. Sobald das Geld eingelöst ist, können die Aktivitäten der Social Bots wieder eingestellt werden. Eine von einer solchen Aktion betroffene Firma hat als einzelner Akteur nur wenige Möglichkeiten, gegen massenhafte Falschmeldungen mit Gegenmeldungen vorzugehen.
- *Es werden künstliche, nichtexistente Märkte geschaffen, die zu Anlagen in nichtexistente Produkte verleiten.* Mittels Social Bots und der Verbreitung von Meldungen wäre es möglich, über Geschäftsoptionen zu berichten, beispielsweise dass es ein vielversprechendes Geschäft mit knappen Ressourcen gibt. Die Social Bots verbreiten massenweise Informationen dazu, und wenn interessierte Anleger nach diesem Thema im Internet suchen, finden sie Nachrichten zu einem lukrativen Geschäft. Diese Aktivitäten können kriminell ausgenutzt werden, indem ein passendes Finanzprodukt geschaffen wird, in das die Anleger investieren.
- *Social Bots infiltrieren klassische Vertriebs- und Beratungsmodelle für Investments mit Falschnachrichten.* Die Verbreitung von Informationen per Social Bots in sozialen Netzwerken/Onlineforen kann den Börsen- bzw. Marktpreis eines Finanzinstrumentes massiv beeinflussen, da den potenziellen Anlegern ein reges Interesse des Kapitalmarktes am Finanzprodukt vorgetäuscht wird.

Einflusspotenzial auf die IT-Sicherheit 2.3

6. Social Bots können eine Gefahr für die IT-Sicherheit darstellen. Sie greifen primär nicht die Hard- oder Software von IT-Systemen an, wie dies bei Hackerangriffen der Fall ist, sondern nehmen den Menschen als potenzielle Schwachstelle der IT-Sicherheit ins Visier und können diesen für Angriffe instrumentalisieren (z. B. durch Links, über die Schadsoftware installiert wird).

Aktuell scheinen die Gefahren von Social Bots mit Blick auf Industrie 4.0, das Internet of Things und die damit verbundene Zunahme an vernetzten Geräten noch unwahrscheinlich, weil Social Bots Hard- oder Software von IT-Systemen nicht direkt angreifen. Vor dem Hintergrund der rasanten Entwicklungen und der immer intelligenter werdenden Geräte einerseits und der zunehmenden Fähigkeiten von (Social) Bots andererseits ist ein zukünftiges Risiko, wie z. B. das Kapern von Geräten für schadhafte Zwecke, nur schwer abzuschätzen (Interview Kossol).

Im Oktober 2016 sorgte eine DDoS-Attacke auf DNS-Servern dafür, dass zahlreiche Websites nicht mehr erreichbar waren. Mutmaßlich reichten nur 50.000 vernetzte Geräte dafür aus, um diese massiven Störungen auszulösen. Dieser Angriff ging von einem Bot-Netz aus, das von den Social Bots abzugrenzen ist, weil es direkt die Hard- oder Software adressiert und sich nicht wie Social Bots an Menschen wendet.

Ein potenziell schädlicher Einsatz von Social Bots zur Schädigung von IT-Systemen und IT-Infrastrukturen könnte über ein Automatic Spear Phishing realisiert werden. Beim Phishing werden fingierte und vertrauenerweckende Nachrichten an potenzielle Opfer versandt, um diese dazu zu bewegen, auf Links zu klicken oder sich auf Websites mit deren Passwortdaten einzuloggen. Das Spear Phishing hebt sich dadurch ab, dass Nachrichten nicht breit gestreut werden, sondern dass sich der Angriff auf eine bestimmte Zielgruppe, beispielsweise die Angestellten eines Unternehmens, konzentriert und diese mit persönlichen und individualisierten Botschaften angesprochen werden. Diese Art Angriff ist mithilfe von Social Bots möglich und wird durch die leichte Skalierbarkeit umso schädlicher. Das Spear Phishing ist sehr effizient, und es werden Klickraten der adressierten Nutzer von ca. 50 % gegenüber 2 % bei herkömmlichen Phishingnachrichten erreicht. Über das Spear-Phishing-Verfahren könnte per Mausklick Schadsoftware bei den Nutzern installiert werden, die Viren verbreitet oder in der Struktur von trojanischen Pferden die Fernsteuerbarkeit der IT-Systeme ermöglicht, sodass die installierte Software unbemerkt im Hintergrund ihre schädliche Wirkung entfalten kann. Über diese Vorgehensweise ließen sich Social Bots auch zur Organisation von DDoS-Attacken einsetzen (Interview Hegelich; Hegelich 2016, S. 4). Social-Bot-Angriffe mit Spear Phishing auf die Mitarbeiter von Unternehmen oder Betreiber von Infrastrukturen wie Telekommunikation, Energieversorger oder Wasserwerke könnten eine große Gefahr darstellen.

Einflusspotenzial auf Geschäftsmodelle von sozialen Netzwerken 2.4

7. Social Bots stellen langfristig eine Bedrohung für das Geschäftsmodell von sozialen Netzwerken dar. Ein Teil der Nutzer könnte sich abwenden, weil sie das Vertrauen in die Echtheit der Beiträge verlieren. Investoren verlieren das Interesse, weil sich die Plattformen durch Werbeeinnahmen oder den Verkauf von Nutzerdaten finanzieren, aber nur Menschen Kaufentscheidungen treffen.

Die Geschäftsmodelle sozialer Netzwerke basieren überwiegend auf dem Verkauf von Werbung und/oder Nutzerdaten (Falch et al. 2009, S. 3 ff.). Facebook erzielte 2016 rund 97 % seiner Umsätze (27,6 Mrd. US-Dollar) aus Werbeeinnahmen (Statista GmbH 2016a, S. 31).

Plattformen wie Facebook und Twitter unterrichten deshalb regelmäßig ihre Investoren und Werbekunden über die Anzahl ihrer Nutzer und deren Verweildauer auf ihren Plattformen. Die Höhe der Werbeeinnahmen sowie der Verkauf der Nutzerdaten generieren die Umsätze, die wiederum den Börsenwert der Unternehmen bestimmen. Werbung kann aber nur dann erfolgreich wirken, wenn sich diese an Menschen richtet, da nur Menschen eine Kaufentscheidung treffen und Produkte kaufen. Wenn die Ansprache von Menschen den Werbeanbietern nicht garantiert werden kann, verlieren die Investoren das Interesse (Interview Kondo). Gleiches gilt auch gegenüber Kunden der sozialen Netzwerke, die auf Basis der gekauften Nutzerdaten Trendanalysen erstellen, denen eine valide Datenlage zugesichert werden muss. Ferner erleiden die Plattformen einen Reputationsverlust bei ihren Nutzern, wenn sich Social Bots zu stark verbreiten. Die Nutzer zweifeln an der Echtheit der Beiträge oder fühlen sich durch extreme Meinungen und Hate Speeches so stark gestört, dass sie sich von diesem Medium abwenden.

Dass ein Bot-Verkehr grundsätzlich im Internet zu hohen Verlusten bei den Werbeeinnahmen führen kann, wurde in einer Untersuchung der US-amerikanischen Association of National Advertisers und White Ops, einem IT-Sicherheitsunternehmen mit Produkten zum Schutz gegen Missbrauch im Bereich digitaler Werbung (z. B. gefälschte Klickraten von Videos), abgeschätzt. Die Ergebnisse der Studie zeigen, dass den Werbeanbietern im Internet im Jahr 2016 rund 7 Mrd. US-Dollar durch Bot-Aktivitäten verloren gingen (ANA/White Ops 2016).

Die Gefährdung der Geschäftsmodelle hängt auch von strukturellen und technischen Faktoren ab: Die sozialen Netzwerke sind aufgrund der Art, wie Kontakte geknüpft werden, unterschiedlich stark durch Social Bots gefährdet. Bei Facebook und Snapchat werden Kontakte über das sogenannte Invitemodell

geknüpft, d. h., dass die Nutzer ihre potenziellen Kontakte selbst auffordern, ins Kontaktnetzwerk aufgenommen zu werden bzw. bestätigt werden müssen. Umgekehrt findet die Verknüpfung bei Twitter nach dem Followermodell statt, d. h., eine Verbindung kann allein durch den Follower zustande kommen und muss vom Gefolgten nicht aktiv akzeptiert werden (Interview Kossol). Eine Ausnahme bilden geschützte Benutzerkonten.

Soziale Netzwerke, die mit dem Invitemodell arbeiten, sind aufgrund des Bestätigungsvorgangs tendenziell besser vor Social Bots geschützt (Interviews Janetzko, Kossol u. Strohmaier).

Ein technischer Faktor, der den Zugang von Social Bots erleichtert, ist die offene Programmierschnittstelle. Facebook hat im Vergleich zu Twitter eine weniger offene API, wodurch die Wahrscheinlichkeit von Social Bots auf Facebook gegenüber Twitter sinkt.

Facebook (Interview Facebook) berichtete davon, dass schon seit vielen Jahren gegen einen betrügerischen Missbrauch auf seiner Plattform vorgegangen wird. Facebook stellt sich entschieden gegen Fakeaccounts oder Social Bots, weil es in seinem eigenen Interesse ist, dies zu verhindern. Facebook zielt auf die Schaffung eines vertrauenswürdigen Umfelds für seine Nutzer, um eine glaubhafte Kommunikation zwischen Menschen und Wirtschaftsakteuren auf ihrer Plattform zu gewährleisten. Das Einrichten von Fakeaccounts oder der Einsatz von betrügerischen Bots widerspricht den Geschäftsbedingungen von Facebook. Fakeaccounts oder Social Bots werden deshalb sofort nach ihrer Entdeckung entfernt. Um Fakeaccounts zu verhindern, verlangt Facebook ferner schon seit einigen Jahren die Eingabe von Klarnamen bei der Registrierung. Weitere konkrete Maßnahmen bestehen darin, die Rückmeldungen von Nutzern zu Fakeaccounts auszuwerten sowie technische Systeme für das Aufspüren von Fakeaccounts und automatisierten Aktivitäten zu entwickeln und einzusetzen. Die technischen Maßnahmen setzen an verschiedenen Stellen an, um Social Bots einerseits schon bei der Registrierung möglichst zu verhindern und andererseits diese auch noch zu einem späteren Zeitpunkt aufzuspüren. Hierzu werden Erkennungssysteme genutzt, etwa um verdächtige Muster bei Likes zu identifizieren, die mithilfe von Machine-Learning-Technologien kontinuierlich auf dem neuesten Stand gehalten werden (Interview Facebook).

Wie die anderen sozialen Netzwerke damit umgehen, ist weitgehend intransparent. So pflegt beispielsweise Twitter keine offene Kommunikation dazu, wie das Unternehmen zum Thema Social Bots steht oder welche Gegenaktivitäten beabsichtigt sind. Ein möglicher Grund kann darin liegen, dass die Unternehmen schlechte Public Relations vermeiden möchten (Interview Hegelich).

Inwieweit Social Bots die Geschäftsmodelle sozialer Netzwerke bereits real geschädigt haben, kann nicht beantwortet werden. Die zuletzt gescheiterten Versuche, Twitter zu verkaufen, könnten jedoch ein Indikator dafür sein, dass

Zweifel am Potenzial des Geschäftsmodells und an der Validität der Daten bestehen (Interview Fuchs). Ein kausaler Zusammenhang zwischen dem misslungenen Firmenverkauf und dem Vorhandensein von Social Bots kann jedoch nicht belegt werden.

Es führt die sozialen Netzwerke auch vor ein Dilemma. Entweder sie gehen dagegen vor und müssen sich möglicherweise dem Vorwurf der Willkür und Zensur stellen, oder sie bleiben inaktiv und unterstützen damit Beeinflussungsprozesse (Interview Quandt).

2.5 Einflusspotenzial von Social Bots auf das Internet insgesamt

8. Social Bots und ähnliche Internetphänomene können auf Dauer dazu führen, dass die Anonymität der Urheber von Algorithmen im Internet aufgegeben wird, ein Diskurs zur Ethik von Algorithmen angestoßen und ggf. die Entstehung eines kostenpflichtigen und geschützteren Second Internet befördert wird.

Social Bots werden auch als Treiber in der Debatte um das postfaktische Zeitalter beschrieben: Lügen und Fakten sind immer schwerer voneinander zu unterscheiden, Unwahrheiten werden zunehmend in der Gesellschaft hingenommen und akzeptiert. Postfaktische Politik basiert nicht mehr auf belegten Evidenzen, sondern auf Meinungen und Gerüchten. Social Bots tragen als eine Art technisches Propagandamittel zur Informationsflutung und -verstopfung des Internets bei (Interview Reez). Falschmeldungen verbreiten sich immer schneller im Netz und prägen die Meinungsbildung. Der Erfolg von Populisten wird hierdurch und durch die nichttransparenten Filtermechanismen der sozialen Netzwerke erst möglich (Steppat 2016). Einige der interviewten Experten vermuten deshalb, dass die durch Social Bots angetriebene Entwicklung zum Postfaktischen zur Entstehung eines parallelen Internets beitragen könnte, das im Wesentlich von und für Eliten bestimmt wäre (Interview Wetzel). So könnte einerseits das aktuelle weitgehend kostenfreie Netz bestehen bleiben, in dem Werbung, Hate Speeches, Shitstorms und eben auch Social Bots vorzufinden sind, und andererseits könnte ein kostenpflichtiges Internet entstehen, das frei von diesen Phänomenen ist (Interview Welchering). Dies wäre der Gegenentwurf zu dem bereits bestehenden als Deep- oder Darknet bezeichneten Internet, in dem Drogen, Waffen und sonstige kriminelle Angebote gehandelt oder getauscht werden und in dem man vollkommen anonym bleibt. Wer die Initiatoren sein könnten und wer das parallele Internet betreiben könnte, ist offen. Ansätze zu geschlossenen Interneträumen gibt es aber schon heute. So existieren einige Chaträume

und Foren, zu denen der Zutritt nur auf Empfehlung oder Einladung möglich ist (beispielsweise spezifische Chats auf quakenet).

Ein weiterer Aspekt, der im Zusammenhang von Social Bots und der Zukunft des Internets von den Experten angemerkt wurde, sind Anonymität und Ethik von Algorithmen (Reichert 2012; Sandvig et al. 2016). Für Algorithmen gibt es keinen Ausweiszwang, keine Besteuerung und nur wenige Gesetze. Die Urheber von Algorithmen sind unbekannt, sodass diese intransparent und anonym agieren. Dies führt dazu, dass Algorithmen nicht rückverfolgt oder die Urheber verantwortlich gemacht werden können und die ausgelösten Schäden folgenlos für die Verursacher bleiben (Interview Helbing; Angwin 2016). Die Urheber von Algorithmen sollten daher einer Rechenschaftspflicht nachkommen (Angwin 2016; Mittelstadt 2016). Algorithmen könnten markiert werden, u. a. um Herkunft und Identität eines sozialschädlichen Bots nachweisen zu können. Hierbei stellen sich nach Meinung der Experten neben der Frage der praktischen Umsetzbarkeit einer Markierungspflicht eine Fülle von rechtlichen Fragestellungen für Hersteller und Programmierer. Mit Blick auf die Ethik von Algorithmen wird die Idee einer »Sozialverträglichkeitsprüfung von Algorithmen« vorgeschlagen – vergleichbar mit einer Umweltverträglichkeitsprüfung als ein politisches Instrument der Umweltvorsorge mit dem Ziel, umweltrelevante Vorhaben vor ihrer Zulassung auf mögliche Umweltauswirkungen hin zu überprüfen. Die Hersteller von Social Bots müssten demzufolge einen ähnlichen Prozess durchlaufen, um die Sozialverträglichkeit eines Algorithmus nachzuweisen. Das heißt, bevor ein Algorithmus auf den Markt käme, müsste eine Sozialprognose für die Anwendung abgegeben werden. Im Zuge der Prüfung müsste die Frage beantwortet werden, was der Algorithmus im sozialen Handlungsraum konkret bewirken würde (z. B. politische Einflussnahme oder Beeinflussung von Märkten, auch Falschbewertungen zu Produkten). Wie bei der Umweltverträglichkeitsprüfung müssten auch bei der Sozialverträglichkeitsprüfung Grenzwerte der Gefährlichkeit definiert werden. Dies beträfe sowohl die Aspekte der Meinungsbildung als auch die Einflussnahme im Bereich von Marketing (Interview Reez).

Die Beschäftigung mit Social Bots sowie mit der zu erwartenden zunehmenden Interaktion von Internetnutzern mit einer künstlichen Intelligenz berührt zudem aus der Sicht einiger Experten Fragen nach dem Selbstverständnis des Menschen und seiner Menschenwürde. Menschen sollten ein Recht darauf haben, zu wissen, ob sie mit einer künstlichen Intelligenz oder mit einem Menschen interagieren (Interviews Hegelich u. Reez).

Positive Einsatzmöglichkeiten von Social Bots 2.6

9. Der Einsatz von Social Bots muss nicht per se mit negativen Absichten verbunden sein. Es gibt künstlerisch-kreative Beispiele für den Einsatz von Social Bots sowie Ansätze, diese als Lockvogel oder als Gegenmaßnahme zur Bekämpfung von Falschnachrichten einzusetzen. Ferner könnten Sie für ein Nudging, im Sinne einer positiven Beeinflussung menschlichen Verhaltens, eingesetzt werden.

Neben den ausschließlich negativen und schadhaften Einsatzmöglichkeiten der Social Bots wurden von den Interviewpartnern auch einige potenziell positive Nutzungsmöglichkeiten erwähnt, wenngleich diese strengen ethischen Kriterien unterliegen müssten. Mithilfe von Social Bots könnten Counter-Speech-Kampagnen als Instrument zur Auflösung von Falschinformationen betrieben (Interviews Janetzko, Lutter u. Strohmaier 2016) oder Köder-Bots zur Identifizierung von bösartigen Social Bots eingesetzt werden (Interview Grimme).

Laut den Experten wird in einigen Forschungsprojekten aktuell die Nutzung von Social Bots für das Nudging, also zur positiven Beeinflussung von Menschen bezüglich eines die Gesundheit fördernden Verhaltens, untersucht, z. B. um mit dem Rauchen aufzuhören (Interviews Helbing u. Strohmaier). Diese Art Nutzung wirft jedoch ethische Fragen auf (Interviews Grimme u. Hegelich), weil auch in diesen Fällen manipuliert wird. Ethisch unbedenklich wäre dies allenfalls, wenn die Prinzipien der informationellen Selbstbestimmung berücksichtigt würden (Interview Helbing).

Des Weiteren existieren bereits künstlerisch-kreativ inspirierte Bots bzw. Bots, die gutartige und harmlose Nachrichten verbreiten. Der Bot »Pfannkuchenpolizei« (@PfannKPolizei) z. B. ist auf Twitter aktiv und reagiert sofort auf das Wort »Berliner« in Tweets etwa mit Hinweisen darauf, dass »dit Pfannkuchen heißt!«

Ein weiteres Beispiel für ein (bislang) harmloses, allerdings sehr großes Bot-Netzwerk ist das jüngst von den britischen Forschern des Londoner University College, Dr. Shi Zhou und Juan Echeverria Guzman, eher zufällig entdeckte Twitter-Bot-Netzwerk mit ca. 350.000 Benutzerkonten, das im Zeitraum von Juni bis Juli 2013 tausendfach zufällig ausgewählte Textzitate aus den elf Star-Wars-Büchern twitterte und deshalb »Star Wars Botnet« getauft wurde. Die eigentliche Zielstellung dieses Bot-Netzwerks ist unbekannt. Es wird spekuliert, dass es sich um ein Experiment eines Amateurs gehandelt haben könnte (Baraniuk 2017).

3. Enttarnungssysteme und Eindämmungsmöglichkeiten von Social Bots

10. Die technischen Möglichkeiten zur Enttarnung von Social Bots sind noch im Entwicklungsstadium. Die Enttarnung hinkt der schnellen Entwicklung von Bots hinterher.

So groß die Bestrebungen der Entwickler und Initiatoren von Social-Bot-Technologien sind, menschliche Identitäten vorzutäuschen, so extensiv werden auch Bestrebungen vorangetrieben, diese zu enttarnen. Zum Nachteil der Entwickler von Enttarnungsmechanismen gilt analog zur Antivirussoftware, dass eine Bot-Technologie erst einmal aktiv und vor allen Dingen bekannt werden muss, um Gegenmaßnahmen entwickeln und einleiten zu können. Die Enttarnung hinkt der Bot-Entwicklung folglich immer einen Schritt hinterher. Zur Enttarnung werden Verhaltensmuster, Eigenschaften und Verflechtungen in sozialen Netzwerken untersucht, die Bots als solche kennzeichnen und von Menschen bzw. menschlichem Verhalten unterscheiden. Dazu zählt beispielsweise das Alter des Benutzerkontos, das Interaktionsverhalten, die Anzahl der Tweets pro Tag, der Inhalt der Beiträge, die Anzahl von Freunden und Followern oder die Nachvollziehbarkeit des Profils mit plausibler Timeline (Ferrara et al. 2016, S. 101).

Eine einfache, nichttechnische Möglichkeit zur Enttarnung ist die Überprüfung der verdächtigen Benutzerkonten durch Menschen, die zumeist schnell erkennen können, ob sich hinter einem Profil eine menschliche oder maschinelle Identität verbirgt (Wang et al. 2013, S. 1). Diese Art der Enttarnung gerät aber schnell an ihre Grenzen, sobald größere soziale Netzwerke mit mehreren Millionen oder gar Milliarden Nutzern untersucht werden sollen.

An dieser Stelle setzen Big-Data-Verfahren an, die Profilinformationen aus den sozialen Netzwerken auswerten. Auffälligkeiten, wie beispielsweise das Veröffentlichen von Posts in identischen Intervallen, deuten auf den Einsatz von Social Bots hin. Der von Davis et al. (2016) für die Enttarnung entwickelte Service »BotOrNot?« erreicht dabei Treffsicherheiten von 95 %. Allerdings steht die Entwicklung trickreicher Tarnmechanismen wie beispielsweise Benutzerkonten, die sowohl von Menschen als auch von Bots gesteuert werden, nicht still, sodass auch Enttarnungsmechanismen dieser Art ausgehebelt werden können (Ferrara et al. 2016, S. 102).

Seit 2016 gibt es das Pilotprojekt »Botswatch«, das zum Ziel hat, Aktivitäten von Social Bots im Politikumfeld transparent zu machen. Botswatch wird von einer Gruppe von Webentwicklern sowie Datenanalytikern betrieben und fokussiert seine Analysen momentan auf Twitter.

Eine weitere Möglichkeit zur Enttarnung sind Algorithmen, die über die Verbindung von Profilen in sozialen Netzwerken stark vernetzte Gemeinschaf-

ten und damit Bot-Netzwerke identifizieren können. Social Bots sind oft untereinander vernetzt, um ein menschliches Freundenetzwerk vorzutäuschen (Hegelich/Janetzko 2016, S. 579). Die Chance, dass sich in einer Gemeinschaft von Bots ein menschlicher Nutzer aufhält, ist relativ gering. So kann davon ausgegangen werden, dass ab einer bestimmten Durchsetzung von Bots nahezu auch alle restlichen Benutzerkonten von Bots gesteuert werden (Boshmaf et al. 2013, S. 574). Die Methode setzt die Annahme voraus, dass menschliche Communities von Bot-Communities weitgehend getrennt existieren.

Schaffen es allerdings von Bots gesteuerte Benutzerkonten, sich mit menschlichen Nutzern zu verbinden, etwa durch eine bestätigte Freundschaftsanfrage, wird die Identifikation von isolierten Bot-Netzwerken erschwert. Ferrara et al. (2016) konnten zeigen, dass viele Facebooknutzer Freundschaftsanfragen von Bots akzeptieren, wodurch sich die Netzwerke von Menschen mit Bots durchmischen und dadurch Social Bots schwerer zu detektieren sind.

Denkbar wäre, dass zukünftig Dienste vergleichbar mit Klout (ein Bewertungsdienst für Social-Media-Profile) eine größere Bedeutung bekommen. Mittels eines verwandten Dienstes wäre es möglich, sowohl die eigene Reputation in den sozialen Medien als auch die anderer anhand eines Scoringwertes zu überprüfen. Ein solcher Scoringwert könnte die Bestätigung dafür sein, dass es sich bei dem Nutzer um einen Menschen handelt. Diese Art des Reputationsdienstes könnte auch in Plattformen sozialer Netzwerke integriert werden. Hierbei handelt es sich zwar nicht um ein Enttarnungssystem im eigentlichen Sinne, aber die Glaubwürdigkeit und die Echtheit des Nutzers können auf einen Blick erkannt werden.

Eine Hürde haben Entwickler von Enttarnungssystemen und Bots gleichermaßen zu nehmen: Die APIs der sozialen Plattformen ermöglichen bzw. beschränken sowohl den Zugang von Bots als auch von Big-Data-Analysen. Die Betreiber von sozialen Netzwerken können somit einen entscheidenden Einfluss auf die Abwehr von Bot-Armeen haben, indem sie beispielsweise Entwicklern von Enttarnungsmechanismen höhere API-Bandbreiten zur Verfügung stellen.

Aufgrund der Komplexität der verschiedenen Plattformsysteme und der Spezifität einzelner Bot-Technologien ist es wahrscheinlich, dass nur eine Mischung aus verschiedenen Enttarnungsmechanismen Social Bots zuverlässig identifizieren kann (Ferrara et al. 2016, S. 102 f.).

Öffentliches Fachgespräch im Bundestag VI.

Am 26. Januar 2017 wurde ein öffentliches Fachgespräch zur Diskussion und Validierung der Zwischenergebnisse der TA-Vorstudie Social Bots im Deutschen Bundestag durchgeführt.

Ziel des Fachgesprächs war, den Stand der zu diesem Zeitpunkt noch laufenden Untersuchung zu diskutieren, die zentralen Zwischenergebnisse zu überprüfen und Ansatzpunkte für politisches Handeln zu reflektieren. Da das Thema bereits im Vorfeld auf ein großes mediales und politisches Interesse traf, diente das Fachgespräch auch zur Bestimmung der Bedeutung des Phänomens Social Bots.

Als Input für das Fachgespräch diente ein Thesenpapier, in welchem die bis Dezember 2016 gewonnenen zentralen Erkenntnisse aus der Literatur- und Quellenanalyse sowie den bis dahin bereits vollständig abgeschlossenen Experteninterviews zusammengefasst wurden.

Liste der Sachverständigen 1.

Die teilnehmenden 19 Sachverständigen rekrutierten sich aus dem Kreis der für die TA-Vorstudie interviewten Personen bzw. Institutionen:

- Dr. Stephan Arlt, Bundesamt für Sicherheit in der Informationstechnik
- Martin Fuchs, Hamburger Wahlbeobachter/politik-kommunikation.de
- Dr. Christian Grimme, Westfälische Wilhelms-Universität Münster
- Prof. Dr. Simon Hegelich, Hochschule für Politik München an der Technischen Universität München
- Prof. Dr. Dirk Helbing, Eidgenössische Technische Hochschule Zürich
- Prof. Dr. Dr. Dietmar Janetzko, CBS Cologne Business School GmbH
- Ulf-Jost Kossol, T-Systems Multimedia Solutions GmbH/Bundesverband Digitale Wirtschaft (BVDW) e. V
- Holger Kriegeskorte, Bundeskriminalamt
- Linus Neumann, Chaos Computer Club
- Prof. Dr. Jürgen Pfeffer, Hochschule für Politik München an der Technischen Universität München
- Prof. Dr. Thorsten Quandt, Westfälische Wilhelms-Universität Münster
- Dr. Norbert Reez, Bundesakademie für Sicherheitspolitik
- Stephan Sachweh, Pallas GmbH
- Alexander Sander, Digitale Gesellschaft e. V.
- Prof. Dr. Christian Holger Georg Stöcker, Hochschule für Angewandte Wissenschaften Hamburg (ehemals tätig für SPIEGEL ONLINE)

- Prof. Dr. Markus Bernhard Strohmaier, GESIS – Leibniz-Institut für Sozialwissenschaften/Universität Koblenz • Landau
- Benedikt Walter, freier Journalist
- Marie-Teresa Weber, Bitkom e. V. (Arbeitskreis Medienpolitik)
- Dr. Steffen Wenzel, politik-digital.de

Zentrale Diskussionsergebnisse 2.

In dem Fachgespräch wurde zu Beginn in die Ausgangslage eingeführt und danach das Thema entlang dreier Fragestellungen diskutiert (entsprechend dem Aufbau von Kap. V):

1. Einfluss und Wirksamkeit von Social Bots: Was ist heute machbar und wie wird der Einfluss nachgewiesen?
2. Zukünftige Einflusspotenziale und Einsatzmöglichkeiten von Social Bots: Wofür können Social Bots zukünftig eingesetzt werden?
3. Enttarnungssysteme und Eindämmungsmöglichkeiten: Wie lassen sich Social Bots erkennen und verhindern?

Einfluss und Wirksamkeit von Social Bots 2.1

Versachlichung der Diskussion

Zu Beginn wurde von den Diskutanten die Bedeutung einer Versachlichung der Diskussion begrüßt. So sei das Thema schon seit 2015 in den Medien sehr präsent und pendele seitdem zwischen Panikmache einerseits und Verharmlosung anderseits hin und her. Es sei deshalb positiv, dass die Diskussion um Social Bots mit der TA-Vorstudie und dem Fachgespräch eine Versachlichung erfahre.

Das Phänomen Social Bots ist gut nachzuweisen; die Wirkung nicht

In der Diskussion waren sich die Sachverständigen einig, dass Social Bots ein empirisch gut nachweisbares Phänomen seien, deren Wirkung bis jetzt jedoch noch nicht eindeutig belegt werden konnte.

Über die Wirkung von Social Bots wurde ausgiebig und kontrovers diskutiert. Der zugrundeliegende Tenor war, dass trotz der schweren Nachweisbarkeit der Auswirkungen von Social Bots ein Zusammenhang zwischen deren Einsatz und einer Einflussnahme auf Debatten zu vermuten ist. So teilten die Sachverständigen überwiegend die Einschätzung, dass Social Bots politische Diskurse und Debatten beeinflussen können, indem sie Menschen manipulieren. Es

gebe eine umfassende empirische Grundlage für den Nachweis von Social Bots und Manipulationsversuchen von Trends, Informationen, Likes etc. Es wurde aber auch zu bedenken gegeben, dass man allein von dem gehäuften Auftreten der Bots nicht unbedingt auf deren Wirksamkeit schließen könne, denn der Aufwand und die Kosten für die Herstellung von tausenden Bots seien sehr gering. Ob und inwieweit Social Bots tatsächlich die politische Willensbildung beeinflussen, könne momentan noch nicht abschließend beantwortet werden. Generell sei der Nachweis von solchen Wirkungszusammenhängen nur schwer bis kaum möglich.

Social Bots sind ein möglicherweise überschätztes Phänomen

Allein der Vertreter des Chaos Computer Club, Linus Neumann, zweifelte die Wirksamkeit von Social Bots deutlich an und stellte sie als generell überschätztes Phänomen infrage. Die Bedeutung von Social Bots werde stark überzogen und aufgebauscht. Linus Neumann verglich Social Bots in ihrer Wirkung mit Spams, mit denen schon jeder in den verschiedenen Varianten postalisch, per E-Mail, Flugblätter oder per Telefonanruf in Kontakt gekommen sei. Social Bots könnten nicht mehr oder weniger bewirken als andere Medien auch. Fremdenfeindlichkeit würde durch Social Bots nicht erzeugt, lediglich könnten bereits vorhandene Tendenzen verstärkt werden. Die Politik lenke mit der Diskussion um Social Bots davon ab, dass es einen allgemeinen Vertrauensverlust der Bürger in die Politik gebe. Auch die Medien hätten sich die wachsende Nachrichtenskepsis letztlich selbst zuzuschreiben. Schließlich seien Social Bots eher als Symptom denn als Ursache dieser gesellschaftlichen Entwicklungen zu werten.

Der Wirkungsraum von Twitter ist klein, besitzt aber besonderes Multiplikatorpotenzial

Ein Rechenexempel zeigte, dass die potenzielle Anzahl von Wählerinnen und Wählern, die durch Social-Bot-Aktivitäten auf Twitter beeinflusst werden könnten, vergleichsweise gering wäre. Wenn es gelänge, 5 % der rund 4 Mio. deutschen Twitternutzer (bezogen auf 2014, für das Jahr 2016 wurden 5,67 Mio. aktive Nutzer prognostiziert) (Statista GmbH 2016b, S. 29) in ihrer Wahlentscheidung zu manipulieren, beträfe dies weniger als 1 % der Bevölkerung und bewegten sich damit auf einem vernachlässigbaren Niveau. Doch auch wenn der Wirkungsraum gemessen an der Nutzerzahl in Deutschland nicht sehr groß sei, wurde dem in der anschließenden Diskussion gegenübergestellt, dass sich auf Twitter eine große Zahl von Meinungsführern, wie Politiker, Journalisten oder auch die Polizei, bewegte und Twitter dadurch ein hohes Multiplikatorpotenzial habe.

Social Bots sind ein soziales, kein technisches Problem

Des Weiteren wurde kritisiert, dass die Diskussion um Social Bots suggeriere, dass diese autonom handelnde Subjekte seien. Hinter den Social Bots stünden aber ganz normale Menschen, welche die Social Bots lediglich als Werkzeug für die Manipulation benutzten. Damit handele es sich bei dem Thema auch weniger um eine technische als um eine gesellschaftliche Herausforderung, für die eher soziale denn technische Lösungen gefragt seien.

Abgrenzung von Social Bots zu anderen Internetphänomenen

In der Diskussion wurde positiv angemerkt, dass sich Social Bots mittlerweile von anderen, wie z. B. Assistenz-Bots, besser abgrenzen lassen. Social Bots, Fakeaccounts und Fakenews werden oftmals in einem Atemzug genannt, sodass in der Debatte besser darauf geachtet werden sollte, worüber genau gesprochen werde. Fakenews stünden mit Social Bots vor allem deshalb in Verbindung, weil sie u. a. über diese verbreitet würden. Mit Blick auf Fakeaccounts sei zu differenzieren, dass diese sowohl von Personen als auch von Social Bots betrieben werden.

Zukünftige Einflusspotenziale und Einsatzmöglichkeiten von Social Bots 2.2

Eingeleitet wurde der zweite Themenblock mit dem Hinweis, dass selbst, wenn heute noch nicht alle Fragen zur Wirksamkeit von Social Bots beantwortet werden könnten, es bei der Technikfolgenabschätzung gerade darum gehe, die zukünftigen Potenziale zu beschreiben, um daraus eventuelle Handlungsbedarfe abzuleiten. Daher stand beim zweiten Diskussionspunkt die Potenzialität der Social Bots im Mittelpunkt und die Frage danach, wozu diese zukünftig in der Lage sein könnten und welche Einflusspotenziale mit ihnen verbunden wären.

Im Verlauf der Diskussion wurde erörtert, dass Social Bots nicht nur im politischen, sondern auch im wirtschaftlichen Bereich das Potenzial haben, Schaden anzurichten, wenn ablenkende oder falsche Nachrichten die öffentliche Wahrnehmung und Meinung beeinflussen.

Mensch und Maschine werden immer schwerer zu unterscheiden sein

Vor dem Hintergrund der zunehmenden technologischen Reife künstlicher Intelligenz wäre es für die Nutzer zukünftig nicht mehr unterscheidbar, so die Sachverständigen, ob sie mit einem Menschen oder einer Maschine kommuni-

zierten. Von den Diskutanten wurde dazu überwiegend die Meinung vertreten, dass dieser Unterschied für Menschen aber erkennbar sein sollte.

Social Bots könnten trotz Selbstverpflichtungen der Parteien im Wahlkampf eingesetzt werden

Auch wenn sich die etablierten Parteien gegen den Einsatz von Social Bots im Wahlkampf ausgesprochen hätten, sei es nicht ausgeschlossen, dass andere sich der Social Bots im Wahlkampf bedienten. Hier forderten die Sachverständigen dazu auf, eine gewisse Vorsicht walten zu lassen und potenzielle Aktivitäten im Blick zu behalten. In diesem Zusammenhang wurde ein Recherchebeispiel von Simon Hegelich und Benedikt Walter vorgestellt, um zu verdeutlichen, dass die Anzahl der Social Bots allein nicht über deren Wirksamkeit entscheidet. Sie konnten innerhalb eines Pegida- und AfD-nahen Netzwerks auf Facebook nachweisen, dass nur vier Social Bots ausreichten, um eine Filterblase im Nachrichtenstream dieser Netzwerke zu erzeugen.

Social Bots nutzen die Funktionsweisen der Algorithmen von sozialen Netzwerken

Die Sachverständigen erläuterten, wie Social Bots bzw. die Algorithmen der sozialen Netzwerke funktionierten, und leiteten das Potenzial daraus ab, dass Social Bots zu einer Verzerrung der Nachrichtenwahrnehmung beitragen könnten. Technisch betrachtet sei dabei nicht der Algorithmus der Bots maßgeblich, sondern der Filtermechanismus der sozialen Netzwerke. Social Bots könnten in der Regel keine eigenen Trends in den sozialen Netzwerken erzeugen, sondern nutzten vielmehr die Funktionsweisen der Algorithmen aus, indem sie beispielsweise Hashtags mit Nachrichten überschwemmten oder Likes setzten. Hierdurch könnte es zu Verzerrungen in der Wahrnehmung und der Entstehung von Filterblasen kommen, weil Nachrichten zum Trending Topic würden oder in Timelines der Nutzer auftauchten.

Social Bots suggerieren Mehrheitsmeinungen, an denen sich Menschen orientieren

Von einem Sachverständigen wurde das Phänomen der Schweigespirale in die Diskussion um Social Bots eingebracht. Social Bots würden sich dieses Mechanismus bedienen, weil sie durch die massenhafte Verbreitung von Nachrichten eine Mehrheitsmeinung suggerierten. Die Theorie der Schweigespirale besagt, dass Menschen auf Basis wahrgenommener Mehrheiten agieren. Je stärker die

in Massenmedien verbreitete öffentliche Meinung als Mehrheitsmeinung wahrgenommen wird, desto schwerer wird es für den Einzelnen, sich andersartig zu äußern. Je mehr also die eigene Meinung der Mehrheitsmeinung widerspricht, desto größer sind die Hemmungen, sich zu äußern, wodurch die sich verstärkende Schweigespirale entsteht. Social Bots machten sich diesen Mechanismus zunutze und könnten somit zu einer Polarisierung in der Gesellschaft beitragen.

Wirtschaftlicher Schaden durch Börsenmanipulation und Fehlinformationen

Social Bots haben laut Holger Kriegeskorte das Potenzial, Börsenkurse zu manipulieren. Wenn sich Kursverläufe plötzlich ändern und Gewinne bei Einzelpersonen beobachtet werden, liege der Verdacht der Manipulation nahe. Noch falle die Verfolgung solcher virtuellen Taten schwer. Es sei noch unklar, wer eigentlich zur Verantwortung gezogen werden müsse, der Programmierer des Algorithmus oder der Auftraggeber. Sicher sei, dass die möglichen Mechanismen zur Verbreitung von Informationen für wirtschaftskriminelle Absichten ausgenutzt werden und dadurch ein hoher wirtschaftlicher Schaden entstehe. Auch wenn der Zusammenhang oft nicht nachweisbar sei, müsse man diesen kriminellen Ereignissen nachgehen.

Social Bots als Teil einer größeren Manipulationsmöglichkeit im Internet

Dirk Helbing nahm in der Diskussion um die Potenzialität der Social Bots eine besonders kritische Position ein. Er sehe einen generellen Trend der Zunahme von Manipulationsmöglichkeiten im Internet. Zudem sei es unstrittig, dass soziale Medien eine verstärkende Wirkung auf Debatten haben würden, denn Massenmedien seien schon immer für Propaganda eingesetzt worden. Social Bots hätten das Potenzial, zu einem sozialen Klimawandel beizutragen. Er verglich Social Bots mit Doping. Auch Doping sei nur schwer nachzuweisen und entfalte eine Wirkung, die ebenfalls nur schwer gemessen werden könne.

Die Entwicklung von Social Bots müsse in dem größeren Kontext der Entwicklungen von künstlicher Intelligenz, Big Data und Nudging eingeordnet werden. Es gehe im Internet zunehmend um eine subliminale, also unterschwellige Beeinflussung unter Ausnutzung der beim Internetsurfen hinterlassenen Datenspuren. Dirk Helbing argumentierte, dass sich die sozialen Netzwerke durch Werbeeinnahmen finanzieren und damit ein Interesse an einer auf Individuen ausgerichteten, personalisierten Werbung hätten. Einen Schritt weiter gedacht, könne dieses Prinzip auch auf Nachrichten übertragen werden, indem

den Internetnutzern auf ihr persönliches Profil hin maßgeschneiderte Artikel verfügbar gemacht werden. Diese Form von individualisierten Nachrichten sei gefährlich für die Gesellschaft, weil sie ihr die gemeinsame Informationsgrundlage und Faktenbasis raube. Wünschenswert sei stattdessen eine pluralistische Sicht auf die Welt, die nicht von den Algorithmen der großen Internetkonzerne wie Google und Facebook bestimmt werden solle.

Enttarnungssysteme und Eindämmungsmöglichkeiten von Social Bots 2.3

Medien- und Technikkompetenz der Kinder, Jugendlichen und Erwachsenen stärken

Das Kommunikationsverhalten und die Rezeption von Nachrichten haben sich durch das Internet insgesamt verändert. Es handelt sich um einen disruptiven Wandel, vergleichbar mit der Einführung des Buchdrucks oder der Einführung des Fernsehens. Dieser Wandel ist zwar schon länger im Gange, stellt aber nach wie vor völlig neue, bisher noch ungelöste Anforderungen an die Gesellschaft.

Es herrschte Konsens darüber, die mediale Aufklärung und auch Technikkompetenz der Internetnutzer im Sinne einer Digital Literacy zu stärken. Dies müsse bereits in der Schule beginnen, wenngleich auch Erwachsene gefordert seien, das System Internet noch besser zu verstehen. Viele Internetnutzer seien mit den grundlegenden Mechanismen im Internet wie der Logik der Verstärkung über Klicks oder der Finanzierung über Werbung und Daten noch wenig vertraut, weshalb sie oftmals sehr unreflektiert damit umgingen.

Es wurde für eine informationstechnische Grundbildung plädiert und die Idee eingebracht, Informatik in den Bildungskanon mit aufzunehmen. So wie Grundzüge von naturwissenschaftlichen Phänomenen gelehrt werden, sei auch ein grundlegendes Verständnis informationstechnischer Funktionsweisen und Zusammenhänge sinnvoll. Eine einfache und schnelle Aufklärung könne bereits an beispielhaften Demonstrationen der technischen Möglichkeiten und Logiken von Algorithmen gelingen.

Doch Bildung allein sei nicht ausreichend, um dem Phänomen Social Bots zu begegnen, vielmehr sei auch eine Persönlichkeitsbildung erforderlich. Kinder und Jugendliche müssten in der Lage sein, die Angebote und Möglichkeiten des Internets kritisch zu bewerten, um auf verantwortliche Weise damit umgehen zu können.

Medienkompetenz der Journalisten und Medien stärken

Ferner waren sich die Sachverständigen einig, dass sich auch Journalisten bzw. die Medien stärker mit den Funktionsweisen der Algorithmen von sozialen Medien auseinandersetzen sollen, und appellierten, vorsichtiger bei der Verbreitung von Nachrichten zu sein. Journalisten sollen stärker hinterfragen und besser nachvollziehen können, wie eine Nachricht zum Trend werde oder die Popularität eines Benutzerkontos entstehe. Typische Indikatoren, wie z.B. die Anzahl der Tweets, Likes, Retweets oder Followern, seien leicht zu manipulieren. Es empfehle sich deshalb für die Medien, sich bei der Bewertung von Nachrichten nicht allein auf diese Indikatoren zu stützen.

Kennzeichnungspflicht wurde kontrovers diskutiert

Die Handlungsoption einer möglichen Kennzeichnungspflicht für Social Bots wurde von den Sachverständigen kontrovers diskutiert.

Zunächst wurde erörtert, dass eine Kennzeichnung von Bots allein durch die sozialen Netzwerke erfolgen könne und müsse. Schließlich könne nicht davon ausgegangen werden, dass die Betreiber von Social Bots ihre Benutzerkonten selbst als Bots ausweisen, weil deren primäres Interesse ja gerade in der Täuschung liege und darin, im Verborgenen zu agieren.

Eine Kennzeichnungspflicht sei bisher auch technisch noch nicht umsetzbar. Social Bots würden noch nicht zuverlässig erkannt. Es bestehe damit die Gefahr, dass eine Sicherheit suggeriert werde, die letztlich so nicht existiere, weil vermutlich nicht alle Bots erfasst und gekennzeichnet werden könnten. Eine Kennzeichnung und Verbote würden ferner auch Ausweichbewegungen auf andere Plattformen befördern.

Daneben wurde kritisch hinterfragt, wie eine Kontrolle und eine Sanktionierung gegen Verstöße einer Kennzeichnungspflicht erfolgen könnten. Es wurde ein Vergleich mit der Klarnamenpflicht bei Facebook herangezogen, die nicht funktioniere, weil eine Identität des Nutzers nicht wirklich überprüft werde und Verstöße keinerlei Sanktion unterworfen seien.

Ein weiterer Aspekt, der in diesem Zusammenhang aufgebracht wurde, war ein möglicher Zielkonflikt zwischen der durch den Datenschutz gedeckten Anonymität der Nutzer einerseits und der Detektion von Bots andererseits, wenn Internetnutzer zum Zwecke der Enttarnung von Social Bots beobachtet werden.

Einige Sachverständige setzten deshalb auf die Selbstregulation durch die sozialen Netzwerke. Weil das Geschäftsmodell der sozialen Netzwerke primär aus Werbeinnahmen bestehe, müsse es ein Eigeninteresse daran geben, den Betrieb von Social Bots auf ihren Plattformen zu unterbinden.

Ethik und Identitätsnachweis von Algorithmen

Neben der Kennzeichnungspflicht für Social Bots gab es auch eine Empfehlung für den generellen Identitäts- und Herkunftsnachweis von Algorithmen, vergleichbar mit einer Ausweispflicht.

Programme und Roboter agieren immer menschenähnlicher, sodass auch über ähnliche Rechte und Pflichten nachgedacht werden muss, wie sie die Rechtsordnung für natürliche Personen vorsieht. Aktuell wird dies vom EU-Parlament diskutiert. Es soll eine Rechtecharta für Roboter und Systeme mit künstlicher Intelligenz entwickelt werden, die ethische Grundprinzipien berücksichtigt und auch Haftungsfragen mit einschließt (Europäische Kommission 2016; Nevejans 2016).

Zu dem im Thesenpapier erwähnten Aspekt einer Sozialverträglichkeitsprüfung von Algorithmen wurde kritisch angemerkt, dass noch ungeklärt sei, wie die Ethik von Algorithmen eingeschätzt werde und wer über die Grenzwerte von Gefährlichkeit entscheiden könne. Mit Blick auf eine Ausweispflicht von Algorithmen wurde zudem angemerkt, dass dies, wenn überhaupt, nur international reguliert werden könne.

Territoriale Reichweite von Gesetzen und Regulierungen

Bei der Umsetzung einer Gerichtsbarkeit müsse auf die territoriale Reichweite geachtet werden. Dadurch, dass es sich bei den sozialen Netzwerken um internationale Konzerne handele, seien nationale Vorschriften und Gesetze ohnehin wirkungslos. Hierfür bedürfe es weltweiter gemeinsamer Initiativen, die Akteure aus Wirtschaft und Politik gleichermaßen einschlössen.

Forschungsbedarf

Die Sachverständigen waren sich ebenfalls einig, dass es im sehr jungen Forschungsfeld Social Bots weiterer Untersuchungen bedürfe, um zu gesicherten Erkenntnissen zu gelangen.

Zwar sei über das Phänomen auf Twitter schon recht viel bekannt, doch vermutlich betreffe es auch andere soziale Netzwerke wie Snapchat oder Instagram. Der Wirkungsraum gehe also vermutlich über Twitter weit hinaus. In den technisch stärker geschlossenen Systemen seien Social Bots aber kaum erforscht.

Problematisch für die Forschung sei es, dass der Datenzugang für wissenschaftliche Arbeiten bei den sozialen Plattformen erschwert sei, denn der experimentelle Betrieb von Social Bots verstoße gegen deren AGB. Demzufolge seien gesetzliche Regelungen wünschenswert, die einen besseren Datenzugang erlaub-

ten. Eine weitere Einschränkung bestehe im internationalen Wettbewerb um Kooperationsmöglichkeiten mit den vorwiegend US-amerikanischen Plattformbetreibern. Facebook gewähre bis heute nur einigen amerikanischen Forschern Zugang zu seinen Daten, sodass europäische Wissenschaftler im Hintertreffen seien.

Handlungsoptionen VII.

Mit Blick auf den in dieser TA-Vorstudie abgebildeten Erkenntnisstand und die sich daraus ergebenden Konsequenzen stellen Social Bots ein neues, sich dynamisch entwickelndes Phänomen dar. Social Bots kommen in der Praxis für manipulative Anwendungen zum Einsatz. Selbst bei möglichen positiven Anwendungsszenarien von Social Bots, z. B. im Bereich des gesundheitsfördernden Nudging, ist das Ziel ihres Einsatzes eine Einflussnahme auf Verhalten.

Da der Grad der Durchdringung der Meinungsbildung und damit die Wirksamkeit bzw. Wirkmächtigkeit von Social Bots in Bezug auf die Wahrnehmung von Sachverhalten, den öffentlichen Diskurs oder auch auf demokratische Prozesse generell noch nicht abschließend geklärt sind, können auch die sich daraus ergebenden Handlungsfelder nur vorläufiger Natur sein. Unstrittig scheint gegenwärtig jedoch, dass der Umgang mit Social Bots eine Kombination aus ordnungspolitischen und rechtlichen, technischen und aufklärerisch-edukativen Aktivitäten erfordert.

Medien- und informationstechnische Kompetenz in Zeiten von Social Bots und Fakenews stärken

Wie in der einleitenden Definition von Social Bots deutlich wird, reihen sich die automatisierten Meinungsmacher ein in eine ganze Reihe ähnlicher und sich darum herum gruppierender Phänomene. Da Social Bots gezielt dazu eingesetzt werden, Propagandanachrichten zu verbreiten, schlagen sie eine unmittelbare Brücke zu den sogenannten Fakenews, also der Verbreitung von Lügenmeldungen und Gerüchten, bzw. zur postfaktischen Gesellschaft ganz allgemein.

Die bisher vorliegenden Erkenntnisse legen nahe, dass für einen souveränen Umgang mit Propaganda- oder Falschmeldungen das Wissen um die Qualität und Zuverlässigkeit von Quellen einerseits sowie Grundkenntnisse informationstechnischer Zusammenhänge andererseits entscheidend sind. Kinder, Jugendliche und auch Erwachsene sollten in ihrer Medienkompetenz im Sinne einer Digital Literacy gestärkt werden. Ein grundlegendes Verständnis informationstechnischer Funktionsweisen und Zusammenhänge – etwa dazu, wie Nachrichten zum Trend werden – sollte unbedingt in der schulischen Ausbildung vermittelt werden.

Solange sich die Medienrezipienten nicht bereits in einer Echoblase aus einseitigen, als wahr angenommenen und sich selbstverstärkenden Nachrichten befinden, ist eine ausgeprägte Medienkompetenz zur Bewertung und Einschätzung von Quellen und Nachrichtentypen ein wirksames Mittel, um die Nichtbeeinflussbarkeit gegenüber Fakenews und dem Wirken von Social Bots zu er-

höhen. Doch scheint aktuell die Unterscheidungsfähigkeit zwischen der Seriosität einer Twittermeldung – dem momentan für den Einsatz von Social Bots bevorzugten sozialen Medium – und einem Artikel in einem etablierten Medium nicht mehr durchweg gegeben zu sein. Ob das Thema Social Bots in einem größeren Rahmen zur *richtigen* Nutzung vernetzt-digitaler und sozialer Medien edukativ behandelt werden kann oder spezifisch adressiert werden muss, wäre zu klären.

Verbesserte Standards im Journalismus

Da auch etablierte Medien zunehmend auf Inhalte aus sozialen Medien zurückgreifen (aus Gründen der Aktualität und prinzipiell auch der Authentizität) und so unter Umständen eine Multiplikation und eine Legitimierung von Botgenerierten Inhalten erfolgen können, ist die Verifizierung derartiger Quellen auch durch den professionellen Journalismus notwendig. Ähnlich wie die Herkunft von Bildmaterial auf Glaubwürdigkeit und Echtheit hin überprüft wird, muss dies auch für Twittermeldungen und andere potenziell automatisch generierte Inhalte gelten.

Zudem sollte sich die Bewertung der Relevanz von Nachrichten oder der Popularität von Themen oder Personen aufgrund der leichten Manipulierbarkeit nicht allein auf die in sozialen Medien typischen Indikatoren, wie z.B. die Anzahl der Retweets oder Follower stützen. Aufgrund der Arbeitsverdichtung und der von Onlinemedien getriebenen Aktualitätserwartungen wird es für den professionellen Journalismus jedoch immer herausfordernder, die notwendigen Qualitätsansprüche zu erfüllen. Hier wären Mechanismen zu implementieren, die als Mindeststandards zur Verifikation verbindlich angewendet werden.

Dass in den klassischen Medien zunehmend ein Bewusstsein für die Problematik von Social Bots und Fakenews allgemein besteht, verdeutlichte die Berichterstattung zum Anschlag auf einen Berliner Weihnachtsmarkt am 19. Dezember 2016: Hier wurden neue Ermittlungserkenntnisse nur vorsichtig aufgegriffen, immer wieder relativiert und betont, dass es auch darum gehe, keine Gerüchte zu verbreiten.

Social Bots verstoßen (noch) nicht gegen geltendes Recht

Neben einem aufgeklärten Umgang mit von Social Bots generierten und/oder massiv verbreiteten (Falsch-)Meldungen und deren Entlarvung erfahren die Eindämmung und die Bekämpfung des Phänomens eine hohe Aufmerksamkeit. Der bestehende Rechtsrahmen bietet nach übereinstimmender Einschätzung jedoch keine Handhabe, um Social Bots und deren manipulativen Einsatz zu

unterbinden. Anders als noch im Herbst 2016 hat sich gegen Ende des Jahres 2016 in der öffentlichen, aber insbesondere der politischen Diskussion die Wahrnehmung von Social Bots deutlich erhöht.

Eine Kennzeichnungspflicht von Bots zum jetzigen Zeitpunkt wirft Probleme auf, u. a. aufgrund der Schwierigkeiten bei der zuverlässigen Detektion von Bots, mangelnder Sanktionierungsmöglichkeiten sowie von Konflikten mit dem Datenschutz. Alternativ gilt es zu erwägen, bei den Anbietern sozialer Medien auf wirksame Selbstverpflichtungen sowie Maßnahmen gegen die Verbreitung von Social Bots auf ihren Plattformen hinzuwirken. Aufgrund der nur punktuellen Offenlegung von Fallzahlen und Geschäftspraktiken inklusive Abwehrmaßnahmen von Social Bots und verwandten Phänomenen durch die Betreiber sozialer Medien kann kaum eingeschätzt werden, in welchem Umfang diese aktiv sind und welche Konsequenzen sich daraus ableiten.

Bei rechtswidrigen Praktiken durch Social Bots wäre zu erwägen, die Auftraggeber oder Programmierer strafrechtlich zu belangen. Dies wäre der Fall, wenn mit dem Bot-Einsatz der Aufruf zum Begehen von Straftaten, Angriffe auf die freiheitlich demokratische Grundordnung verbunden oder andere schädliche Auswirkungen für die Gesellschaft zu erwarten sind (z.B. Wirtschaftskriminalität, Täuschung bei Produktbewertungen).

Da aber nur in Ausnahmefällen damit zu rechnen sein dürfte, die international und von Drittländern aus agierenden Initiatoren von Social Bots zu identifizieren und rechtlich belangen zu können, stellt die Ausübung von rechtlichen Druckmitteln gegenüber den Betreibern von Social-Media-Plattformen ggf. eine weit wirksamere Lösung dar. Dabei muss gewährleistet sein, dass es (technisch) möglich ist, Social Bots sicher zu identifizieren. Prinzipiell ist denkbar, die Plattform-Betreiber mit in die Verantwortung der durch sie verbreiteten Inhalte zu nehmen, wenngleich hier noch viele Fragen offen bleiben, insbesondere, wer über den Wahrheitsgehalt einer Nachricht und deren Löschung letztlich entscheiden kann, ohne dabei das Grundrecht der Meinungsfreiheit zu gefährden. Dennoch muss mit Blick auf Falschnachrichten und sogenannte Hate Speeches eine Diskussion geführt werden, wo die Grenzen der Toleranz liegen. Soziale Medien sollten weiterhin für die freie Meinungsäußerung genutzt werden können, ohne grundsätzlich infrage gestellt zu werden.

Auch ohne Änderung des Rechtsrahmens scheint es angesichts der jüngsten Erfahrungen mit der automatisierten Erzeugung/Verbreitung von (Falsch-)Meldungen möglich, durch Selbstverpflichtungen von Unternehmen und zivilgesellschaftlichen Organisationen zumindest einer weiteren Verbreitung von Social Bots Einhalt zu gebieten. Die Ankündigung aller im Deutschen Bundestag vertretenden Parteien, im Wahlkampf auf den Einsatz von Social Bots zu verzichten, weist hier in eine richtige Richtung, wobei abzuwarten ist, wie lange

ein solcher Verzicht Bestand haben oder von anderen politischen Gruppierungen missachtet wird.

Enttarnung und Bekämpfung von Social Bots

Social Bots profitieren von den drei großen Treibern der Digitalisierung – Ausbau der Daten- und Kommunikationsnetze, Verfügbarkeit preiswerter Speicher, Zugang zu leistungsfähigen Rechenkapazitäten. Demzufolge ist zu erwarten, dass sich ein dynamisches Gleichgewicht zwischen der Entwicklung von Social Bots und entsprechenden Enttarnungssystemen ergeben wird. Wenngleich die Entwicklung von Enttarnungssystemen unerlässlich ist, ist gegenwärtig keine definitive technische Lösung des Problems in Sicht. Da Social Bots zum weit überwiegenden Teil beim Kurznachrichtendienst Twitter eingesetzt werden, der sich neben der auch maschinell gut generierbaren Nachrichtenstruktur durch eine einfach ansteuerbare Schnittstelle (API) auszeichnet, stellt diese einen möglichen Abwehrmechanismus gegen Social Bots dar. So gibt es Überlegungen, dass an der API eine Identifikation des zugreifenden Algorithmus erfolgt. Auf diese Weise könnte ermittelt werden, wie der Algorithmus funktioniert, was er bewirkt etc. Durch eine derartige Maßnahme würde nur erwünschten Algorithmen der Zugang gewährt, während unerwünschte Algorithmen, wie sie in Social Bots verwendet werden, abgeblockt werden könnten. Ob ein solcher Mechanismus jedoch tatsächlich wirksam sein kann und eine Chance auf Realisierung hat, wird auch in Expertenkreisen angezweifelt. Das Phänomen Social Bots könnte weiterhin eine Entwicklung hin zu einer möglichen Zweiteilung des Internets befördern, mit einem allgemeinen und einem unkontrollierten Teil und einem lauteren, von Gatekeepern kontrollierten Teil. Da die Diskussion gegenwärtig noch keine einheitliche Perspektive und technologische Machbarkeit erkennen lässt, ist es notwendig, durch wissenschaftliche Projekte eine belastbare Grundlage zu den Möglichkeiten und Grenzen einer technischen Eindämmung von Social Bots sowie zu deren weitergefassten Konsequenzen zu schaffen.

Forschungsbedarf zu Social Bots

Die vorliegende TA-Vorstudie zeigt, dass die Beschäftigung mit dem noch recht jungen Phänomen Social Bots gegenwärtig noch viele Fragen offen lässt. In den seltensten (und stets immer wieder angeführten) Fällen konnte die direkte Wirkung der Social Bots und ihrer Meldungen nachgewiesen werden. Zudem gibt es nur wenige verlässliche Zahlen, um die Dimension einschätzen zu können. Ferner werden nicht unerhebliche Ressourcen in die Entwicklung und den Einsatz von Social Bots gesteckt, die nahelegen, dass sie einen (ggf. erst mittelfristig

erkennbaren) Effekt haben. Um eine umfassende Klärung und Einschätzung des Gefährdungspotenzials sowie der technischen und rechtlichen Herausforderungen zu ermöglichen, sind weitere Forschungen und investigative Ermittlungen nötig. Auch Dunkelfeldforschungen zur Social-Bot-Szene wären vorstellbar, um sich ein Bild über das tatsächliche Ausmaß (Quantität und Qualität) machen zu können. Mittels Befragungen von Tätern und Opfern könnte versucht werden, das Phänomen besser zu erfassen. Nur mit einer erweiterten Wissensbasis kann die Frage beantwortet werden, ob Social Bots potenziell demokratiegefährdend oder nur eine lästige Randerscheinung sind.

Die Betreiber von sozialen Netzwerken könnten die Forscher unterstützen, indem sie Entwicklern von Enttarnungsmechanismen höhere API-Bandbreiten zur Verfügung stellten und Kooperationen mit Wissenschaftlern eingehen, damit der Datenzugang erleichtert und die Forscher bei ihren Untersuchungen nicht gegen die AGB der Plattformbetreiber verstoßen müssen.

Social Bots sind nur ein Teil potenzieller Manipulationsmöglichkeiten im Internet – öffentlicher Diskurs und Etablierung von Gremien für einen internationalen Umgang mit der Digitalisierung erforderlich

Social Bots sind zwar ein potenzieller Faktor für die mögliche Verbreitung von Falschnachrichten zur Manipulation, sie sind jedoch gleichzeitig nur eine von vielen Manipulationsmechanismen, die im Kontext künstlicher Intelligenz, Big Data und personalisierter Ansprache neu entstehen. Die diesen Entwicklungen zugrundeliegende Thematik einer potenziell unterbewusst laufenden Manipulation auf Basis von im Internet hinterlassenen Datenspuren, die Verbreitung von subjektivierten Nachrichten und die damit verbundene Gefahr des Verlusts einer gemeinsamen objektiven Informationsbasis in der Gesellschaft können nur in einem größeren Kontext diskutiert werden und gehen über die Problemstellung Social Bots weit hinaus.

Dies trifft auch zu auf die in der TA-Vorstudie aufgeworfenen Fragen der Experten nach der sozialen Verträglichkeit, Ethik und Ausweispflicht von Algorithmen sowie den Rechten und Pflichten von künstlicher Intelligenz. Social Bots sind hier ebenfalls als Teil eines größeren Ganzen – und zwar der Entwicklung von Digitalisierung, Robotik und künstlicher Intelligenz – zu betrachten. Es geht um nichts weniger als die Frage, wie die Gesellschaft in einer global digitalisierten Welt leben möchte.

Die Auseinandersetzung mit diesen Fragestellungen würde die Einrichtung von Gremien und Institutionen erfordern, die Akteure von Wirtschaft sowie Wissenschaft und Gesellschaft gleichermaßen mit einbeziehen. Eine solche Umsetzung ist durchaus schwierig, weil die Digitalisierung international ist, die Rechtsordnungen aber national sind. Denkbar wären international abgestimmte

Konventionen und Standards innerhalb von global agierenden Gremien zum Thema Digitalisierung (vergleichbar etwa mit der Klimarahmenkonvention der Vereinten Nationen), die einen Rahmen zum Umgang mit der Digitalisierung vorgeben und die nationalen Regulierungsbemühungen flankieren. Das Ziel, sich international auf gemeinsame Richtlinien zu verständigen, würde große Bemühungen der internationalen Staatengemeinschaft unter Einbindung der global agierenden Konzerne erfordern.

Unabhängig von einer institutionellen Lösung ist der öffentliche Diskurs über die digitale Gesellschaft einerseits bzw. Social Bots andererseits ein erster Schritt. Ausgehend von einer Diskussion über Social Bots könnte ein genereller Diskurs angeregt werden über die Frage, wie wir in Zukunft miteinander und mit künstlicher Intelligenz leben wollen.

Literatur

Amann, M.; Knaup; H.; Müller, A.-K.; Rosenbach, M.; Wiedemann-Schmidt, W. (2016): Digitale Dreckschleudern. In: Der Spiegel (43), S. 44–45

ANA (Association of National Advertisers), White Ops (2016): White ops study reveals bot fraud will cost marketers more than $7 Billion in 2016. www.ana.net/content/show/id/38432 (14.2.2017)

Angwin, J. (2016): Make algorithms accountable. www.nytimes.com/2016/08/01/opinion/make-algorithms-accountable.html?_r=1 (2.11.2016)

Baraniuk, C. (2017): Army of 350,000 Star Wars bots found lurking on Twitter. www.newscientist.com/article/2117811-army-of-350000-star-wars-bots-found-lurking-on-twitter/ (30.1.2017)

Bennet, S. (2012): The smartest people prefer Twitter to LinkedIn and Facebook. Research Shows [STUDY]. www.adweek.com/socialtimes/smart-twitter-users/471525 (12.12.2016)

Bessi, A.; Ferrara, E. (2016): Social bots distort the 2016 U.S. presidential election online discussion. http://firstmonday.org/ojs/index.php/fm/article/view/7090/5653 (30.1.2017)

Beuth, P. (2017): Social Bots: Furcht vor den neuen Wahlkampfmaschinen. www.zeit.de/digital/internet/2017-01/social-bots-bundestagswahl-twitter-studie/komplettansicht?print (24.1.2017)

Bilton, N. (2014): Friends, and influence, for sale online: There are several services that allow social media users to buy bots, which can make celebrities appear more popular and even influence political agendas. http://bits.blogs.nytimes.com/2014/04/20/friends-and-influence-for-sale-online/?_r= (20.11.2016)

Bohacek, S. (2016): How to make a Twitter bot with node.js and host it for free with OpenShift. https://botwiki.org/tutorials/make-an-image-posting-twitter-bot/ (2.2.2017)

Bond, R.M.; Fariss, C.J.; Jones, J.J.; Kramer, A.D.I.; Marlow, C.; Settle, J.E.; Fowler, J.H. (2012): A 61-million-person experiment in social influence and political mobilization. In: Nature (489), S. 295–98

Boshmaf, Y.; Muslukhov, I.; Beznosov, K.; Ripeanu, M. (2011): The Socialbot Network. When bots socialize for fame and money. In: Proceedings of the 27th Annual Computer Security Applications Conference, S. 93–102

Boshmaf, Y.; Muslukhov, I.; Beznosov, K.; Ripeanu, M. (2013): Design and analysis of a social botnet. In: COMPUTER NETWORKS 57(2), S. 556–78

Breithut, J. (2016): Wie Social Bots uns manipulieren, wer daran verdient und wie die Fakes auffliegen. www.bento.de/gadgets/social-bots-manipulieren-facebook-und-twitter-einige-verdienen-damit-geld-258770/ (15.1.2016)

Damm, C. (2016): Alles ganz anders: Das ist der wahre Grund, warum niemand Twitter kaufen möchte. www.businessinsider.de/alles-ganz-anders-das-ist-der-wahre-grund-warum-niemand-twitter-kaufen-moechte-2016-10 (6.2.2017)

Davis, C.A.; Varol, O.; Ferrara, E.; Flammini, A.; Menczer, F. (2016): BotOrNot. A system to evaluate Social Bots. In: Proceedings of the 25th International Conference Companion on World Wide Web. International World Wide Web Conferences Steering Committee, S. 273–74

Dewey, C. (2016): One in four debate tweets comes from a bot. Here's how to spot them. www.washingtonpost.com/news/the-intersect/wp/2016/10/19/one-in-four-debate-tweets-comes-from-a-bot-heres-how-to-spot-them/ (26.10.2016)
Elliott, C. (2014): The readers' editor on… pro-Russia trolling below the line on Ukraine stories. www.theguardian.com/commentisfree/2014/may/04/pro-russia-trolls-ukraine-guardian-online (1.11.2016)
Endt, C. (2017): Social Bots – Die Angst vor den Automaten. www.sueddeutsche.de/politik/social-bots-die-angst-vor-den-automaten-1.3356302 (1.2.2017)
Europäische Kommission (2016): Draft report with recommendations to the Commission on Civil Law Rules on Robotics. www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML%2BCOMPARL%2BPE-582.443%2B01%2BDOC%2BPDF%2BV0//EN (8.2.2017)
Falch, M.; Henten, A.; Tadayoni, R.; Windekilde, I.M. (2009): Business models in social networking. http://vbn.aau.dk/en/publications/business-models-in-social-networking(12ed9200-04e7-11df-9046-000ea68e967b).html (13.12.2016)
Ferrara, E.; Varol, O.; Davis, C.; Menczer, F.; Flammini, A. (2016): The rise of Social Bots. In: Communications of the ACM 59(7), S. 96–104
Ferrara, E.; Varol, O.; Davis, C.A.; Menczer, F.; Flammini, A. (2014): The rise of Social Bots. In: arXiv preprint arXiv:1407.5225
Fiegerman, S. (2014): The curious case of Cynk, an abandoned tech company now Worth $5 Billion. http://mashable.com/2014/07/10/cynk/#CvEuP_Dbskqn (7.12.2016)
Fischer, F. (2016): Twitter-Bots. Ferngesteuerte Meinungsmache. www.zeit.de/digital/internet/2013-05/twitter-social-bots (9.6.2016)
Ford, H.; Dubois, E.; Puschmann, C. (2016): Keeping Ottawa honest – One Tweet at a time? Politicians, journalists, wikipedians, and their Twitter Bots. In: International Journal of Communication 10, S. 4891–914
Fredheim, R. (2014): Putin's bot army – part one: a bit about bots. http://blog.rolffredheim.com/2013/06/putins-bots-part-one-bit-about-bots.html (1.11.2016)
Freitas, C.; Benevenuto, F.; Ghosh, S.; Veloso, A. (2015): Reverse engineering Socialbot infiltration strategies in Twitter. 2015. https://socialnetworks.mpi-sws.org/papers/TwitterBots_ASONAM15.pdf (27.10.2016)
Fuchs, J.G. (2013): Internet-Infrastruktur: So sieht es wirklich aus mit unserem Netz [Analyse]. http://t3n.de/news/internet-infrastruktur-sieht-465368/ (5.4.2016).
Fuchs, M. (2016a): Automatisierte Trolle. Warum Social Bots unsere Demokratie gefährden. www.nzz.ch/digital/automatisierte-trolle-warum-social-bots-unsere-demokratie-gefaehrden-ld.116166 (8.11.2016)
Fuchs, M. (2016b): Wie viral sind Bundesregierung & Bundesminister in Social Media? 9.11. www.hamburger-wahlbeobachter.de/2016/11/wie-viral-sind-bundesregierung.html (14.11.2016)
Greenwood, S.; Perrin, A.; Duggan, M. (2016): Social Media Update 2016. http://assets.pewresearch.org/wp-content/uploads/sites/14/2016/11/10132827/PI_2016.11.11_Social-Media-Update_FINAL.pdf (3.2.2017)
Guilbeault, D. (2016): Growing bot security: An ecological view of bot agency. In: International Journal of Communication 10, S. 5003–21
Hauck, M. (2012): Die wundersame Follower-Vermehrung der CDU. www.sueddeutsche.de/digital/twitter-die-wundersame-follower-vermehrung-der-cdu-1.1411578

Haustein, S.; Bowman, T.D.; Holmberg, K.; Tsou, A.; Sugimoto, C.R.; Lariviere, V. (2016): Tweets as impact indicators: Examining the implications of automated »bot« accounts on Twitter. In: JOURNAL OF THE ASSOCIATION FOR INFORMATION SCIENCE AND TECHNOLOGY 67(1), S. 232–38.

Hegelich, S. (2016): Invasion der Meinungs-Roboter. Konrad-Adenauer-Stiftung.

Hegelich, S.; Janetzko, D. (2016): Are Social Bots on Twitter political actors? Empirical evidence from a Ukrainian Social Botnet. In: Strohmaier, M.; Gummadi, K.P.; Lindner, D.; Weller, K.; Gilbert, E.; Macy, M.; Wagner, C. (Hg.): Proceedings of the Tenth International AAAI Conference on web and social media, S. 579–82.

Hölig, S.; Hasebrink, U. (2016): Reuters Institute Digital News Survey 2016 – Ergebnisse für Deutschland. Hamburg

Howard, P.N. (2016): Pro-Clinton bots ›fought back but outnumbered in second debate‹. http://philhoward.org/pro-clinton-bots-fought-back-but-outnumbered-in-second-debate/ (6.12.2016)

Howard, P.N.; Kollanyi, B. (2016): #Strongerin, and #Brexit: Computational propaganda during the UK-EU referendum. https://ssrn.com/abstract=2798311 (17.10.2016).

Kelion, L.; Shiroma, S. (2016): Pro-Clinton bots ›fought back but outnumbered in second debate‹. www.bbc.com/news/technology-37703565 (6.12.2016)

Kerl, C. (2017): Darum sind »Social Bots« eine Gefahr für die Demokratie. www.morgenpost.de/politik/article209347449/Darum-sind-Social-Bots-eine-Gefahr-fuer-die-Demokratie.html (24.1.2017).

Kollanyi, B. (2016): Where do bots come from? An analysis of bot codes shared on GitHub. In: International Journal of Communication (10), S. 4932–51

Kollanyi, B.; Howard, P.N.; Woolley, S.C. (2016): Bots and automation over Twitter during the third U.S. presidential debate. http://politicalbots.org/wp-content/uploads/2016/10/Data-Memo-Third-Presidential-Debate.pdf (6.12.2016)

Krause, S. (2017): Gute Bots, schlechte Bots. www.tagesspiegel.de/medien/pro-und-contra-meinungsroboter-gute-bots-schlechte-bots/19314790.html (1.2.2017)

Laufersweiler, T. (2015): Twitter und Journalismus – wer profitiert? www.ard.de/home/ard/Twitter_und_Journalismus___wer_profitiert_/2392846/index.html (3.2.2017)

Lobo, S. (2016): Nach dem Trump-Sieg. Wie soziale Medien Wahlen beeinflussen. www.spiegel.de/netzwelt/web/fuenf-arten-wie-soziale-medien-wahlen-beeinflussen-kolumne-a-1121577.html (18.11.2016).

Markoff, J. (2017): Automated pro-Trump bots overwhelmed pro-Clinton messages, researchers say. www.nytimes.com/2016/11/18/technology/automated-pro-trump-bots-overwhelmed-pro-clinton-messages-researchers-say.html?_r=1 (18.11.2016)

Mittelstadt, B. (2016): Auditing for transparency in content personalization systems. In: International Journal of Communication 10, S. 4991–5002

morgenpost.de (2016): Twitter Deutschland will offenbar Büro in Berlin schließen. www.morgenpost.de/wirtschaft/article208553097/Twitter-Deutschland-will-offenbar-Buero-in-Berlin-schliessen.html (12.12.2016)

Morstatter, F.; Pfeffer, J.; Liu, H.; Carley, K.M. (2013): Is the sample good enough? Comparing data from Twitter's streaming API with Twitter's firehose. https://arxiv.org/pdf/1306.5204v1.pdf (28.10.2016)

Murthy, D.; Powell, A.B.; Tinati, R.; Anstead, N.; Carr, L.; Halford, S.J.; Weal, M. (2016): Bots and political influence: A sociotechnical investigation of social network Capital. In: International Journal of Communication 10, S. 4952–71

Neff, G.; Nagy, P. (2016): Talking to Bots: Symbiotic agency and the case of Tay. In: International Journal of Communication 10, S. 4915–31
Nevejans, N. (2016): European Civil Law Rules in Robotics. www.europarl.europa.eu/RegData/etudes/STUD/2016/571379/IPOL_STU(2016)571379_EN.pdf (8.2.2017)
Newitz, A. (2015): Ashley Madison code shows more women, and more Bots. http://gizmodo.com/ashley-madison-code-shows-more-women-and-more-bots-1727613924 (13.5.2016)
node: www.node.js. https://nodejs.org/en/ (8.12.2016)
OECD (Organisation for Economic Co-operation and Development) (2015): Government at a Glance 2015 | OECD READ edition. www.keepeek.com/Digital-Asset-Management/oecd/governance/government-at-a-glance-2015_gov_glance-2015-en#page149 (3.2.2017)
Reichert, K. (2012): Plädoyer für eine Algorithmen-Ethik: Relevanz ist alles. www.faz.net/aktuell/feuilleton/debatten/plaedoyer-fuer-eine-algorithmen-ethik-relevanz-ist-alles-11934495-p4.html (14.12.2016)
Sandvig, C.; Hamilton, K.; Karahalios, K.; Langbort, C. (2016): When the algorithm itself is a racist: Diagnosing ethical harm in the basic components of software. In: International Journal of Communication 10, S. 4972–90
Schieb, J. (2016): Social Bots verpesten das Netz. https://blog.wdr.de/digitalistan/social-bots-verpesten-das-netz/ (13.5.2016)
Seibt, P. (2015): Abgeordnete auf Twitter: Die-140-Zeichen-Macht. www.spiegel.de/politik/deutschland/bundestagsabgeordnete-auf-twitter-wer-wie-viel-schreibt-und-mit-wem-a-1041402.html (3.2.2017)
Shiffman, D. (2015): What is Node.js? – Twitter bot tutorial. www.youtube.com/watch?v=RF5_MPSNAtU&list=PLRqwX-V7Uu6atTSxoRiVnSuOn6JHnq2yV (9.12.2016)
SPIEGEL ONLINE (2016): Kriselnder Kurznachrichtendienst: Disney prüft offenbar Gebot für Twitter. www.spiegel.de/wirtschaft/unternehmen/twitter-disney-prueft-offenbar-uebernahme-a-1114069.html (12.12.2016)
Statista GmbH (2009): Twitter-Nutzer in Deutschland nach Bildungsstand 2009. Umfrage. https://de.statista.com/statistik/daten/studie/13057/umfrage/anteil-der-twitter-nutzer-nach-jeweiligem-bildungsstand-maerz-2009/ (27.2.2017)
Statista GmbH (2016a): Facebook – Statista Dossier. Hamburg
Statista GmbH (2016b): Twitter – Statista-Dossier. Hamburg
Steppat, T. (2016): Trump, AfD, Pegida: Wie Populisten durch Facebook groß werden. www.faz.net/aktuell/politik/inland/wie-facebook-populisten-wie-trump-afd-und-pegida-gross-macht-14518781.html (14.12.2016)
Subrahmanian, V.S.; Azaria, A.; Durst, S.; Kagan, V.; Galstyan, A.; Lerman, K.; Zhu, L.; Ferrara, E.; Flammini, A.; Menczer, F. (2016): The DARPA Twitter Bot Challenge. In: COMPUTER 49(6), S. 38–46
Thomas, K. (2013): FDP will ominöse Twitter-Fans wieder loswerden: Geschenkte Follower. www.sueddeutsche.de/politik/neue-twitter-follower-raetselhafter-zuwachs-fuer-die-fdp-auf-twitter-1.1605861 (22.11.2016)
Tutt, C. (2017): Social Bots: Automatisierte Posts gefährden Demokratie und Börse. www.wiwo.de/politik/deutschland/social-bots-automatisierte-posts-gefaehrden-demokratie-und-boerse/19310738.html (1.2.2017)
Voß, J. (2015): Der Feind in meinem Netzwerk: Social Bots. http://politik-digital.de/news/der-feind-in-meinem-netzwerk-social-bots-144563/ (13.5.2016)

Voß, O. (2013): Online-Wahlkampf. Steinbrücks falsche Twitter-Freunde. www.wiwo.de/politik/deutschland/online-wahlkampf-steinbruecks-falsche-twitter-freunde/8352354.html (20.3.2017).
Wagner, C.; Mitter, S.; Körner, C.; Strohmaier, M. (2012): When Social Bots attack. modeling susceptibility of users in online social networks. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.232.2188&rep=rep1&type=pdf#page=46 (10.5.2016)
Wang, G.; Mohanlal, M.; Wilson, C.; Wang, X.; Metzger, M.; Zheng, H.; Zhao, B.Y. (2013): Social turing tests: Crowdsourcing sybil detection. https://arxiv.org/pdf/1205.3856v2.pdf (6.12.2016).
Weck, A. (2016): Wie Social-Media-Trends durch Bots manipuliert werden. http://t3n.de/news/social-media-trends-bots-694529/ (7.6.2016)
Weizenbaum, J. (1978): Die Macht der Computer und die Ohnmacht der Vernunft. Frankfurt a. M.
Wetzel, K. (2016): Blockchain – Im Fieber. www.sueddeutsche.de/wirtschaft/blockchain-im-fieber-1.2908084 (27.4.2016)
Woolley, S.C. (2016): Automating power. Social bot interference in global politics. First Monday 21(4), http://firstmonday.org/article/view/6161/5300
Woolley, S.C.; Howard, P.N. (2016a): Bots unite to automate the presidential election. www.wired.com/2016/05/twitterbots-2 (25.11.2016)
Woolley, S.C.; Howard, P.N. (2016b): Political communication, computational propaganda, and autonomous agents. In: International Journal of Communication 10, S. 4882–90
Zeifman, I. (2017): Bot traffic report 2016. www.incapsula.com/blog/bot-traffic-report-2016.html (14.2.2017)
ZEIT ONLINE (2016): Ashley Madison: Dating-Website gab Chatbots als Frauen aus. www.zeit.de/digital/internet/2016-07/ashley-madison-online-dating-website-betrug-bots (7.12.2016)

Anhang

Social-Bot-Programmierung 1.

Der Twitter-Bot wurde mithilfe der Plattform Node.js (https://nodejs.org) und einer Twit-Bibliothek programmiert.

Der Bot wurde auf einem Rechner mit Linux-Betriebssystem ausgeführt. Die für die Programmierung genutzte Linux-Kommandozeile ist sehr ausgereift und gut für die Netzwerkkommunikation geeignet. Die Installation der nötigen Programme und Bibliotheken bedingte eine stetige Internetverbindung.

Der erste Schritt zum Betrieb eines Social Bots war die Installation der Java Script-Bibliothek Node.js, die sich besonders gut für die Erstellung von Webanwendungen mit der weitverbreiteten Programmiersprache JavaScript eignet. JavaScript ist nach Python die am zweithäufigsten verwendete Programmiersprache für Social Bots.

Ein Code für einen Twitter-Bot fand sich auf GitHub. GitHub ist eine unter Programmierern sehr geläufige Versionskontrollplattform, auf der mehr als 4.000 Codebeispiele allein für Twitter-Bots dokumentiert sind (Kollanyi 2016).

Nach der Installation von Node.js erfolgte eine erste Funktionsüberprüfung per Konsolenbefehl: »node–version«.

Dieser Befehl gibt die installierte Version von Node.js wieder. An einer erfolgreichen Rückgabe kann erkannt werden, dass das Programm ordnungsgemäß installiert wurde. In einem beliebig gewählten Verzeichnis wird nun die Datei »bot.js« erstellt. Der Dateiname ist beliebig und beschreibt in diesem Fall die spätere Funktion des Programms, nämlich die Ausführung eines Bots. Die Datei »bot.js« wird mit einem Texteditor, im Idealfall mit einer Syntaxhervorhebung für JavaScript, geöffnet und folgende Zeile eingefügt: »console.log(›Hello World!‹);«.

Die Datei wird gespeichert und in der Kommandozeile zum Verzeichnis der Datei gewechselt. Das Wechseln von Verzeichnissen erfolgt unter Linux per: »cd/Pfad/zum/Verzeichnis/« und unterscheidet sich im Fall von Windows- oder Unix-basierten (beispielsweise Linux-Derivate und MacOS) Betriebssystemen. Das Programm wird auf der Konsole gestartet per: »node bot.js«.

Es folgt die Ausgabe »Hello World!«, woran erkennbar ist, dass Node.js korrekt arbeitet. Node.js beinhaltet ferner das Programm »Node Package Manager« (npm), mit dem weitere Bibliotheken nachträglich installiert werden können.

Für die Einrichtung eines Social Bots, der auf Twitter aktiv ist, eignet sich die Bibliothek »Twit«, welche in der Konsole mit folgendem Befehl installiert wird: »npm install twit--save«.

Die Anbindung des Social Bots an einen Twitteraccount erfolgt über eine Programmierschnittstelle (API). Diese API bietet einen Zugang zu Twitter, der

nicht wie im Normalfall üblich mit einer grafischen Benutzeroberfläche in einem Webbrowser erfolgt, sondern die von Twitter bereitgestellten Funktionalitäten (beispielsweise Posten, Folgen, Suchen, Retweeten etc.) über eine Programmiersprache (in diesem Beispiel JavaScript) anspricht.

Abb. A.1 Code bot.js

```
// Laden der Twitter Bibliothek

var Twit = require('twit');



// Laden der config.js und Generierung eines Twit Objekts, über das die Anbindung
an Twitter erfolgt

var T = new Twit(require('./config.js'));



// Hashtagsuche

var hashtagSearch = {q: "#bundestag", count: 100, result_type: "mixed"};



// Diese Funktion retweetet per Zufall einen Tweet aus der Hashtagsuche

function retweetLatest() {



       T.get('search/tweets', hashtagSearch, function (error, data) {

         // Fehlerausgabe auf der Konsole

         console.log(error, data);

         // Falls es keine Fehler gab

         if (!error) {

              // wird die ID eines zufälligen Tweets aus der Suche gespeichert

              var retweetId = data.statuses[Math.floor((Math.random() *
100)+1)].id_str;

              // und Twitter angewiesen, den Post zu retweeten

              T.post('statuses/retweet/' + retweetId, {   }, function (error,
response) {

                    if (response) {
```

Eigene Darstellung

Im Folgenden werden die Schritte beschrieben, die für eine Anbindung eines Social Bots an Twitter unternommen werden müssen. Erste Voraussetzung ist ein Twitterbenutzerkonto, bei dem eine Telefonnummer hinterlegt ist. Auf apps.twitter.com wird in einem zweiten Schritt eine neue Applikation erstellt. Auf einer der Registerkarten der Applikation muss sichergestellt werden, dass ein Lese- und Schreibzugriff aktiviert ist. Ferner finden sich vier API-Keys in den Einstellungen der Applikation: Consumer Key, Consumer Secret, Access Token sowie Access Token Secret. Die Keys dienen zur Authentifizierung des Bots und werden in der Datei »config.js« im selben Verzeichnis wie die »bot.js« abgelegt.

Die Abbildung A.1 zeigt den Bot-Code aus der Datei bot.js, die aus dem reichhaltigen Fundus an Codebeispielen auf Github in ca. 2 Stunden zusammengestellt und angepasst werden konnte. Sie ist der Hauptbestandteil des Programms und greift auf die Biliothek »Twit« zu, die die Grundfunktionalitäten für die Kommunikation mit Twitter über die API bereitstellt. Darüber hinaus wird die config.js (Abb. A.2) mit den relevanten API-Token hinzugeladen.

Abb. A.2 Code config.js mit anonymisierten API-Schlüsseln

```
var config = {
  consumer_key:        'XXXXX',
  consumer_secret:     'XXXXX',
  access_token:        'XXXXX',
  access_token_secret: 'XXXXX'
}
```

Eigene Darstellung

Der Bot wird gestartet per Konsolenbefehl: »node bot.js«.

Herauszuheben ist die Funktion »setInterval(function, delay)«, welche dafür sorgt, dass die zuerst angegebene Funktion nach einem bestimmten Intervall erneut aufgerufen und in diesem Beispiel per Zufall einen Post retweetet. Das Zeitintervall wird in Millisekunden angegeben. Das Aufrufen der Twitterfunktionalitäten wird durch eine Maximalanzahl von Aufrufen pro Zeitintervall von 15 Minuten begrenzt. Das heißt, dass die Aufrufe von Twitter nicht mehr bearbeitet werden, wenn die Funktion per »setInterval(function, 1)« beispielsweise einmal pro Millisekunde aufgerufen wird.

Der Bot ist in diesem Stadium einsatzbereit und kann autonom agieren.

Interviewpartner 2.

Titel	Name	Unternehmen	Bereich
Dr.	Christian Grimme	Westfälische Wilhelms-Universität Münster	Wissenschaft
Prof. Dr.	Simon Hegelich	Hochschule für Politik München an der Technischen Universität München	Wissenschaft
Prof. Dr.	Dirk Helbing	Eidgenössische Technische Hochschule Zürich	Wissenschaft
Prof. Dr. Dr.	Dietmar Janetzko	CBS Cologne Business School GmbH	Wissenschaft
Prof. Dr.	Jürgen Pfeffer	Hochschule für Politik München an der Technischen Universität München	Wissenschaft
Prof. Dr.	Markus Strohmaier	GESIS – Leibniz-Institut für Sozialwissenschaften/Universität Koblenz • Landau	Wissenschaft
Prof. Dr.	Thorsten Quandt	Westfälische Wilhelms-Universität Münster	Wissenschaft
	Manuel Bach	Bundesamt für Sicherheit in der Informationstechnik	Verwaltung
	Holger Kriegeskorte	Bundeskriminalamt	Verwaltung
Dr.	Norbert Reez[1]	Bundesakademie für Sicherheitspolitik	Verwaltung
	Martin Fuchs	Hamburger Wahlbeobachter/ politikkommunikation.de	ZGO[2]
	Ulf-Jost Kossol	T-Systems Multimedia Solutions GmbH/ Bundesverband Digitale Wirtschaft (BVDW) e. V.	ZGO
	Timm Lutter	Bitkom e. V. (Arbeitskreis Social Media)	ZGO
	Linus Neumann	Chaos Computer Club	ZGO
	Alexander Sander	Digitale Gesellschaft e. V.	ZGO
Dr.	Steffen Wenzel	politik-digital.de	ZGO
Prof. Dr.	Christian Stöcker	Hochschule für Angewandte Wissenschaften Hamburg (ehemals tätig für SPIEGEL ONLINE)	Presse/Medien
	Benedikt Walter	freier Journalist	Presse/Medien
	Peter Welchering	freier Journalist	Presse/Medien
	Anonym	SPD	Partei
	Robert Heinrich	BÜNDNIS 90/DIE GRÜNEN	Partei
	Thomas Dudzak	Die Linke – Landesverband Sachsen	Partei
	Semjon Rens[3]	Facebook Germany	Wirtschaft
	Stephan Sachweh	Pallas GmbH	Wirtschaft
	James Kondo	SocialEmergence.org	Wirtschaft

1 Die Ausführungen stellen die persönliche Auffassung des Interviewten dar und geben nicht notwendigerweise die Einschätzung der BAKS wieder.
2 zivilgesellschaftliche Organisation
3 wird als Facebook zitiert

Abbildungen 3.

Tabellen 4.

BÜRO FÜR TECHNIKFOLGEN-ABSCHÄTZUNG BEIM DEUTSCHEN BUNDESTAG

KARLSRUHER INSTITUT FÜR TECHNOLOGIE (KIT)

Neue Schönhauser Straße 10
10178 Berlin

Tel. +49 30 28491-0
Fax +49 30 28491-119

buero@tab-beim-bundestag.de
www.tab-beim-bundestag.de