BÜRO FÜR TECHNIKFOLGEN-ABSCHÄTZUNG
BEIM DEUTSCHEN BUNDESTAG

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

Social Bots

Thesenpapier zum öffentlichen Fachgespräch
»Social Bots – Diskussion und Validierung
von Zwischenergebnissen«
am 26. Januar 2017 im Deutschen Bundestag

Januar 2017
VDI/VDE Innovation + Technik GmbH

Inhaltsverzeichnis

1 Vorbemerkung

Das Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag (TAB) erarbeitet durch seinen Konsortialpartner VDI/VDE-IT aktuell eine Sondierungsstudie zur gesellschaftlichen und politischen Relevanz des Themas „Social Bots“. Im Mittelpunkt steht die Untersuchung von Gefahren durch eine mögliche Manipulation politischer Diskussionen und Trends in sozialen Netzwerken.

Das vorliegende Papier fasst die Zwischenergebnisse und den bisherigen Wissenstand der seit Oktober 2016 laufenden Kurzstudie in Form von Thesen zusammen.

Grundlage der einzelnen Aussagen sind Ergebnisse einer Literatur- und Quellenanalyse sowie 25 Interviews mit Fachexperten und -expertinnen. In einer systematischen Literatur- und Quellenanalyse wurden wissenschaftliche Veröffentlichungen sowie das Feld der Grauen Literatur sondiert, ergänzend wurde eine quantitative Web-of-Science-Analyse vorgenommen. Die Interviews wurden mit Experten aus sechs Bereichen/Themenfeldern durchgeführt: Wissenschaft, Behörden, Verbände, Social-Media-Beauftragte der Parteien, Medien/Presse sowie Wirtschaft. Vertreter von sozialen Netzwerken wie Facebook und Twitter konnten trotz intensiver Bemühungen nicht für ein Interview gewonnen werden. Auch der Internetversandhandel Amazon und das IT-Unternehmen Microsoft haben sich auf unsere Anfragen nicht zurückgemeldet.

Das Thesenpapier dient als Basis für ein öffentliches Fachgespräch von TAB und dem Ausschuss für Bildung, Forschung und Technikfolgenabschätzung (ABFTA) am 26. Januar 2017 im Deutschen Bundestag. Zur leichteren Einordnung von Social Bots gegenüber anderen Internetphänomenen werden ihre wesentlichen Eigenschaften vorab kurz erläutert.

2 Definition und Eigenschaften von Social Bots

- Social Bots sind Computerprogramme, die eine menschliche Identität vortäuschen und zu manipulativen Zwecken eingesetzt werden, indem sie wie Menschen im Internet kommunizieren (Bilton 2014; Fuchs 2016; Woolley und Howard 2016a, 2016b; Voß 2016). Echte Menschen, die mit dem Social Bot kommunizieren, nehmen diese nicht als durch Algorithmen ausgelöste automatische Kommunikation, sondern als echte Internetteilnehmer wahr und sind sich der Manipulation nicht bewusst.
- Social Bots unterscheiden sich von unterstützenden Bots (z. B. Chat Bots, digitale Assistenten) nur hinsichtlich ihrer Zielsetzung. Ihre technischen Grundlagen sind verwandt.
- Social Bots, Trolle als menschliche Akteure sowie Spam-E-Mails eint die Zielsetzung der Manipulation oder Desinformation.
- Die Initiatoren und Urheber von Social Bots können bislang bis auf wenige Ausnahmen nicht identifiziert oder rückverfolgt werden. Mutmaßliche Initiatoren politisch motivierter Manipulationen sind Geheimdienste, Terrorgruppen, terroristisch motivierte Einzelpersonen („Lone Wolves“), aber auch andere Akteure wie Unterstützer im Wahlkampf.
- 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.
- 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 des zu programmierenden Bots stark an, wenn diese bspw. Sprachanalysen durchführen und Dialoge simulieren.
- Die Herstellung von Social Bots kann auch in Auftrag gegeben werden. Hierzu existiert eine Wertschöpfungskette mit global verteilten Produktionsstufen.

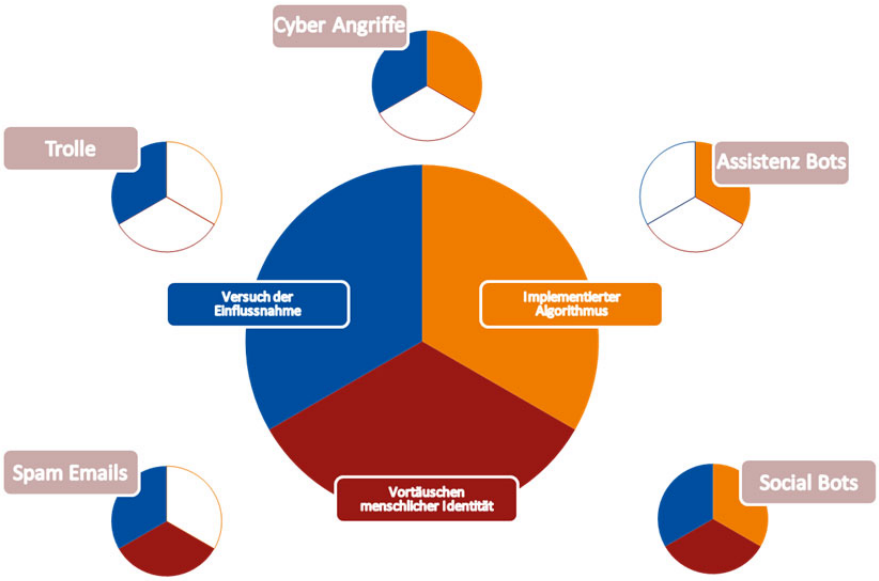

Abbildung 1: Abgrenzung von Social Bots zu anderen Internetphänomenen

3 Überblick Thesen

(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 schon seltener Facebook. Das Ausmaß der tatsächlichen Einflussnahme ist allerdings noch kaum belegt.

(2) Social Bots werden momentan im Wesentlichen dafür eingesetzt, Diskussionen inhaltlich zu verzerren, die Wichtigkeit von Themen oder die Popularität von Personen und Produkten künstlich zu überhöhen. 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 bspw. 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 über das sogenannte Influencer Marketing bis hin zu ganzen Märkten (Bsp. 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 diese 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 dem Verkauf von Nutzerdaten finanzieren, aber nur echte Menschen Kaufentscheidungen treffen.

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

(9) Social Bots und ähnliche Internetphänomene werden 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 Internets“ befördert wird.

4 Erläuterungen zu den Thesen

(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 schon seltener Facebook. Das Ausmaß der tatsächlichen Einflussnahme ist allerdings noch kaum belegt.

Eine erste wissenschaftliche Arbeit zu Social Bots wurde im Jahr 2011 publiziert (Boshmaf et al. 2011). Seit 2012/2013 etabliert sich die wissenschaftliche Auseinandersetzung mit Social Bots zunehmend. Noch ist es jedoch ein kleiner Kreis nationaler und internationaler Autoren, die im Forschungsfeld Social Bots publizieren. Zum Zeitpunkt Dezember 2016 stammen die meisten wissenschaftlichen Veröffentlichungen von folgenden Forschern: Emilio Ferrara von der University of Southern California, Simon Hegelich von der Hochschule für Politik München, Philip Howard von der University of Oxford und Sam Woolley von der University of Washington (Ferrara et al. 2016; Howard und Kollanyi 2016; Bessi und Ferrara 2016; Hegelich 2016; Hegelich und Janetzko 2016; Woolley 2016; Woolley und Howard 2016a, 2016b).

In Deutschland beschränkt sich die Forschung auf zwei Vorhaben. Seit Sommer 2015 laufen die vom Bundesministerium für Bildung und Forschung (BMBF) geförderten Forschungsprojekte „PropStop“ und „Social Media Forensics“, die sich mit der Erkennung, dem Nachweis und der Bekämpfung von verdeckten Propagandaangriffen über Onlinemedien beschäftigen. Parallel zur wissenschaftlichen Auseinandersetzung wird über das Thema Social Bots – verstärkt seit dem Sommer 2015 – in Online-, Print- sowie TV-Medien berichtet.

Bis heute gibt es nur eine überschaubare Anzahl von Beispielen in der wissenschaftlichen Literatur, bei denen der Einsatz von politisch motivierten Social Bots auf Twitter nachgewiesen werden konnte. Die drei am häufigsten in den Experteninterviews, in der wissenschaftlichen Literatur sowie 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 (Kollanyi et al. 2016). Nicht immer ist geklärt, ob zusätzlich auch Trolle zum Einsatz kamen, was zumindest für das Ukraine-Beispiel vermutet wird.

Der Anteil an der Kommunikation zu bestimmten Themen auf Twitter ist dabei durchaus beachtlich. Es konnte nachgewiesen werden, dass fast 20 % der Tweets auf Twitter im US-Präsidentschaftswahlkampf durch Social Bots verbreitet wurden (Bessi/Ferrara 2016), und im belegten Fall der Social-Bot-Aktivitäten im Ukrainekonflikt wurden von 15.000 Profilen etwa 60.000 Tweets pro Tag abgesetzt (Hegelich 2016, S. 5).

Der primäre Wirkungsraum für Social-Bot-Aktivitäten scheint – zumindest momentan – Twitter zu sein. Wirkräume für Social Bots ergeben sich aber grundsätzlich in allen sozialen Netzwerken, die nutzerfreundliche und hürdenfrei zugängliche Application Programming Interfaces (API) besitzen, was besonders auf Twitter, Facebook oder Google+ zutrifft. Twitter ist aufgrund seiner sehr geringen Hürden eine von Social Bots hochfrequentierte Plattform, die gleichzeitig im Zentrum der Forschung steht, da sie für die Forscher eine leichtere Datenzugänglichkeit im Vergleich zu anderen Plattformen bietet.

Die tatsächlichen Effekte der Social Bots auf die politische Meinungsbildung und wirtschaftliche Prozesse beruhen jedoch überwiegend noch auf Annahmen, weil keine der bisherigen Studien einen gesicherten Nachweis der Wirkungen und Effekte von Social Bots liefern konnte.

(2) Social Bots werden momentan im Wesentlichen dafür eingesetzt, Diskussionen inhaltlich zu verzerren, die Wichtigkeit von Themen oder die Popularität von Personen und Produkten künstlich zu überhöhen. 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: (1) für das Ersticken oppositioneller Gegenmeinungen durch das Fluten von Hashtags mit ablenkenden, polarisierenden oder banalen Nachrichten, (2) Verbreitung von Propaganda und Meinungsmache sowie (3) 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 Twitter Accounts einzelner Politiker. So kam es vereinzelt zu massiven Anstiegen von Followern bei Spitzenpolitikern, zudem konnten Social-Bot-Aktivitäten auf den Webseiten der Parteien während der Flüchtlingsbewegung beobachtet werden.

Aktuell sind die anlassbezogenen Aktivitäten von Social Bots in sozialen Medien die augenfälligste Form der Beeinflussung. Gegenwärtige Risiken durch Social Bots ergeben sich ferner im Bereich Cybermobbing, indem Einzelpersonen per Bots mit diskreditierenden Botschaften persönlich beleidigt und belästigt werden. Social-Bot-Aktivitäten auf Foren von Onlinemedien wie z. B. SPON, Welt oder Bild sind aufgrund der höheren technischen Zugangshürden hingegen noch weitgehend unbekannt.

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 viel publizierten 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. 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). Ein zweiter Fall behandelt Fakeprofile auf der US-amerikanischen Onlinedatingplattform Ashley Madison. Social Bots gaben vor, Frauen zu sein und verwickelten Männer in kostenpflichtige Chatgespräche (Newitz 2015).

Es ist bestätigt, dass Social Bots in den sozialen Netzwerken sehr weit verbreitet 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. Accounts auf Facebook Social Bots sein (ca. 1,8 bis 2,1 %) sowie 62 bis 80 Mio. der Twitterprofile (ca. 20 bis 25 %).

Und schon heute sind die technischen Voraussetzungen für den großflächigen Einsatz von Social Bots in Form von Bot-Armeen gegeben, was auf ihr mögliches Gefahrenpotenzial schließen lässt.

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

Eigene Trends werden von Social Bots in der Regel in politischen Diskussionen im Internet nicht gesetzt, vielmehr springen sie zumeist auf schon vorhandene Trends auf, um diese als Vehikel zur Verbreitung von Meinungen zu nutzen. Besonders erfolgreich 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.

In den vergangenen Jahren wurden soziale Netzwerke vermehrt auch von Politikern, Journalisten und seit ca. ein bis zwei Jahren ebenso von der Polizei genutzt. Eine Meinungsmanipulation kommt vor allem aber 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. 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. Befördert wird diese Entwicklung dadurch, dass das Internet zu einer der wichtigsten und auch kostengünstigsten Recherchequellen für den Journalismus geworden ist.

Eine weitere Prämisse sind die Programmierschnittstellen (API), die Social Bots den Zugang zu sozialen Netzwerken erst ermöglichen. Die Betreiber sozialer Netzwerke haben ein Interesse daran, diese Programmierschnittstellen möglichst einfach zugänglich zu machen, um auf diese Weise für Applikationsentwickler attraktiv zu sein. Je einfacher die Registrierung von neuen Nutzern, desto attraktiver wird das soziale Netzwerk für Applikationsentwickler und damit ebenso für den Einsatz von Social Bots.

Die Erstellung von Social Bots (Programmierung, massenweises Erstellen von Nutzeraccounts, Verbreitung von Botschaften) ist nach deutschem und US-amerikanischem Recht legal. Einzelne Aktionen von Social Bots, bspw. 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 AGBs dieser Unternehmen. Durch die Anwendung von Social Bots ausgelöste Straftatbestände liegen mutmaßlich vor allem im Bereich der Wirtschaftskriminalität wie Betrug, unlauterer Wettbewerb sowie unerwünschte Werbung/Spam. Darüber hinaus könnten weitere Straftatbestände berührt sein, wie z. B. Volksverhetzung, Verletzung der Privatsphäre, Identitätsdiebstahl oder Vortäuschung falscher Fakten.

Die Verbreitung und Reichweite von Social Bots ist eng an die Popularität sozialer Netzwerke geknüpft. In Nordamerika sind Twitter und Facebook für den Einsatz von Social Bots aufgrund der im Vergleich zu Deutschland noch höheren Marktdurchdringung und Nachfrage sehr attraktiv, im russischsprachigen Raum erfolgt der Einsatz von Social Bots oft über das dort sehr populäre Netzwerk VKontakte. Twitter wird in Deutschland anscheinend von sehr vielen Meinungsführern genutzt, wodurch sich ein besonderes Multiplikatorpotenzial ergibt. 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 bereits wieder geschlossen (morgenpost.de 2016). Es wäre nicht völlig ausgeschlossen, dass Twitter mittelfristig an Bedeutung verliert oder gar aus dem Markt wieder ausscheidet.

(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 sehr unterschiedlich bewertet. Die Einschätzungen reichen von eher marginal über sehr hoch bis hin zu das Internet und die demokratische Gesellschaft zersetzend. Die interviewten Experten sehen im Wesentlichen vier Einflusspotenziale:

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

(2) 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). Die interviewten Experten befürchten, dass Social Bots die Informationslage in den sozialen Medien und indirekt auch in den traditionellen Medien verfälschen. Die Manipulation und Beeinflussung politischer Debatten würde langfristig zur Unterminierung des Vertrauens in die Demokratie und demokratischer Prozesse führen und zu einer Gefahr für die innere Sicherheit werden. Mit Blick auf die Bundestagswahl 2017 müsse deshalb berücksichtigt werden, dass wichtige und unter Umständen wahlentscheidende Debatten online geführt werden und dadurch verstärkt der Beeinflussung durch Social Bots ausgesetzt seien. 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 gehörendem Spam geflutet würden. Social-Bot-Aktivitäten könnten ferner zu einer Radikalisierung beitragen, da sie wie Katalysatoren den Boden für extreme Meinungen bereiten. Extremmeinungen könnten betont, gemäßigte Meinungen marginalisiert werden. Außerdem könnten sie zur Bildung von Filterblasen und dadurch zu einer Fragmentierung gesellschaftlicher Gruppen und damit der öffentlichen Meinung beitragen.

(3) Verbreitung von Falschinformationen und Gerüchten: Die Gesellschaft könnte durch Nutzung von Social Bots in Krisensituationen destabilisiert und verunsichert werden. Es bestehe die realistische Gefahr, dass in akuten Krisensituationen gezielt Verwirrung gestiftet wird. Besonders terroristische Gruppierungen wären in der Lage, dieses Potenzial auszunutzen.

(4) Cyber Warfare: Neben der kurzfristigen, anlassbezogenen Einflussnahme, scheint vor allem die langfristige Beeinflussung der öffentlichen Meinung im Sinne einer hybriden Kriegsführung ein Gefahrenpotenzial darzustellen. Ziel von Social Bots in diesem Sinne wäre die dauerhafte Beeinflussung der öffentlichen Meinung. 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.

(5) Social Bots haben das Potenzial, das Kunden- und Kaufverhalten über das sogenannte Influencer Marketing bis hin zu ganzen Märkten (Bsp. Börsenhandel) zu manipulieren.

Ein weiteres potenzielles Feld 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. Zwar ist der Einsatz von Social Bots im Bereich Influencer Marketing noch unbekannt, doch dessen Automatisierung ist durchaus realistisch und aufgrund der Umsatzstärke dieses Bereichs attraktiv. 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 oder Journalisten. Diese prägen dann über ihre Beiträge in den sozialen Medien die Meinungen oder wirken als Multiplikatoren. Speziell die „Social Media Influencer“ zeichnen sich durch eine große Anzahl von Followern aus und erhalten meist viel Resonanz in Form von Likes, Shares und Kommentaren auf ihre Beiträge. Wird der Begriff etwas weiter gefasst, zählen dazu auch Personen ohne nachgewiesenen großen Einfluss, die im Internet Bewertungen zu einem Produkt abgeben und damit die Kaufentscheidung anderer beeinflussen können. Das Influencer Marketing wird seit ca. zehn Jahren durchgeführt und ist mittlerweile eine etablierte Marketingmaßnahme. Unternehmen könnten Social Bots zu Werbezwecken im Rahmen von Produktlaunches einsetzen. Diese Vorgehensweise wäre möglicherweise verdeckte Werbung, bei der für den Nutzer Werbung von Nachrichten kaum zu unterscheiden wäre.

Social Bots könnten zudem mit wirtschaftskriminellen Absichten eingesetzt werden. Dies betrifft insbesondere die Manipulation von börsennotierten Finanzprodukten im Sinne einer Marktmanipulation. Die Störung von Finanzmärkten hätte vielfältige Auswirkung auf die verschiedensten Bereiche der Wirtschaft; der Schutz des Vertrauens in die Integrität der Finanzmärkte würde gestört. Das Bundeskriminalamt (BKA) hat im Interview für den Bereich Wirtschaftskriminalität drei mögliche Szenarien definiert:

- Social Bots könnten den Aktienwert gezielt durch Falschmeldungen nach oben, in der Regel aber eher nach unten sinken lassen. Hierzu werden Unternehmen durch Falschmeldungen in Misskredit gezogen. Wenn Falschmeldungen gehäuft im Internet kursieren, werden diese mit größerer Wahrscheinlichkeit von Privatanlegern gelesen oder von Multiplikatoren aufgegriffen und weiter verbreitet. Die potenziellen Anleger treffen auf dieser Basis eine Investmententscheidung. Die Einnahmen werden dadurch realisiert, dass beispielsweise Optionen auf den Verlauf des Börsenkurses abgeschlossen werden, die dann realisiert werden, wenn sich der Kurs in die gewünschte Richtung bewegt.
- 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, bspw. 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 potentiellen Anlegern ein reges Interesse des Kapitalmarktes am Finanzprodukt vorgetäuscht wird.

(6) Social Bots können eine Gefahr für die IT-Sicherheit darstellen. Sie greifen primär nicht die Hardware 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 diese 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 und Internet of Things und der damit verbundenen Zunahme an vernetzten Geräten noch unwahrscheinlich, weil Social Bots Hardware oder Software von IT-Systemen nicht direkt angreifen. Vor dem Hintergrund der rasanten Entwicklungen und der immer intelligenter werdenden Geräte einerseits und (Social) Bots andererseits, ist ein zukünftiges Risiko wie z. B. das Kapern von Geräten für schadhafte Zwecke nur schwer abzuschätzen.

Im Oktober 2016 sorgte eine DDoS (Distributed Denial of Service)–Attacke auf DNS-Server dafür, dass zahlreiche Webseiten 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, die von den Social Bots abzugrenzen sind, weil sie direkt die Hardware oder Software adressieren und sich nicht wie Social Bots an Menschen wenden.

Ein potenziell schädlicher Einsatz von Social Bots zur Schädigung von IT-Systemen und IT-Infrastrukturen von Social Bots 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 Webseiten mit Ihren Passwortdaten einzuloggen. Das Spear Phishing (von engl. Speer) hebt sich dadurch ab, dass Nachrichten nicht breit gestreut werden, sondern sich der Angriff auf eine bestimmte Zielgruppe, bspw. 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 völlig unbemerkt im Hintergrund ihre schädliche Wirkung entfalten kann. Über diese Vorgehensweise ließen sich Social Bots auch zur Organisation von DDoS-Attacken einsetzen (Hegelich 2016, S. 4; Kind und Weide 11.10.2016, S. 2). 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.

(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 dem Verkauf von Nutzerdaten finanzieren, aber nur echte Menschen Kaufentscheidungen treffen.

Die Geschäftsmodelle sozialer Netzwerke basieren überwiegend auf dem Verkauf von Werbung und/oder Nutzerdaten (Falch et al. 2009, S. 3–19). Facebook erzielte 2015 rund 95 % seiner Umsätze (17,08 Mrd. USD) aus Werbeeinnahmen. Twitter hingegen finanziert sich weitgehend über den Verkauf von Nutzerdaten (Higgins 2016, S. 32).

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 echte Menschen richtet, da nur Menschen eine Kaufentscheidung treffen und Produkte kaufen. Wenn die Ansprache echter Menschen den Werbeanbietern nicht garantiert werden kann, verlieren die Investoren das Interesse. 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 speech* so stark gestört, dass sie sich von diesem Medium abwenden.

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 vor Social Bots gefährdet. Bei Facebook und Snapchat werden Kontakte über das sogenannte Invite-Modell geknüpft, d. h. dass die Nutzer ihre potenziellen Kontakte selbst auffordern ins Kontaktnetzwerk aufgenommen zu werden. Umgekehrt findet die Verknüpfung bei Twitter nach dem „Followermodell“ statt, d. h. die eigenen Follower müssen lediglich bestätigt werden. Auch wenn die Follower immer noch bewusst angeklickt werden müssen, scheint die Selektion nach dem Followermodell weniger selektiv als nach dem Invite-Modell vorgenommen zu werden. soziale Netzwerke, die mit dem Invite-Modell arbeiten, sind demzufolge tendenziell besser vor Social Bots geschützt. Ein technischer Faktor, der den Zugang von Social Bots erleichtert, ist die offene Programmierschnittstelle. Facebook hat im Vergleich zu Twitter eine weniger offene Programmierschnittstelle als Twitter, wodurch die Wahrscheinlichkeit von Social Bots auf Facebook gegenüber Twitter sinkt. Inwieweit Social Bots die Geschäftsmodelle sozialer Netzwerke bereits real geschädigt haben, kann nicht beantwortet werden. Die zuletzt gescheiterten Verkaufsversuche von Twitter könnten jedoch ein Indikator dafür sein, dass Zweifel am Potenzial des Geschäftsmodells und an der Validität der Daten bestehen. Ein kausaler Zusammenhang zwischen dem misslungenen Firmenverkauf und dem Vorhandensein von Social Bots kann jedoch nicht belegt werden.

Der Umgang der sozialen Netzwerke mit Social Bots ist weitgehend intransparent. So pflegen bspw. Twitter und Facebook keine offene Kommunikation dazu, wie sie zum Thema Social Bots stehen oder welche Gegenaktivitäten sie beabsichtigen. Ein möglicher Grund kann darin liegen, dass die Unternehmen schlechte PR vermeiden möchten. Es führt die sozialen Netzwerke auch vor ein Dilemma. Entweder sie gehen dagegen vor und müssen sich möglicherweise dem Vorwurf der Zensur stellen oder sie bleiben inaktiv und unterstützen damit Beeinflussungsprozesse.

(8) 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 zu Anti-Virus-Software, 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 bspw. das Alter des Accounts, das Interaktionsverhalten, die Anzahl 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).

Eine einfache nichttechnische Möglichkeit zur Enttarnung ist die Überprüfung der verdächtigen Accounts 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 bspw. 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 bspw. Accounts, die sowohl von Menschen als auch von Bots gesteuert werden, nicht still, sodass auch Enttarnungsmechanismen dieser Art ausgehebelt werden können.

Eine weitere Möglichkeit zur Enttarnung sind Algorithmen, die über die Verbindung von Profilen in sozialen Netzwerken stark vernetzte Gemeinschaften und damit Botnets identifizieren können. Social Bots sind oft untereinander vernetzt, um ein menschliches Freundenetzwerk vorzutäuschen (Hegelich und 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 Accounts von Bots gesteuert werden (Boshmaf et al. 2013, S. 574).

Denkbar wäre, dass zukünftig Dienste wie Kloud eine größere Bedeutung bekommen. Über Kloud ist es möglich, sowohl die eigene Reputation in den sozialen Medien als auch die anderer anhand eines Scoringwertes zu überprüfen. Ein solcher Scoringwert ist eine Bestätigung dafür, dass es sich bei dem Nutzer um einen echten Menschen handelt. Zunehmend wird diese Anwendung auch in Plattformen integriert. Hierbei handelt es sich zwar nicht um ein Enttarnungssystem im eigentlichen Sinne, aber die Glaubwürdigkeit und Echtheit des Nutzers kann auf einen Blick erkannt werden. Die technischen Enttarnungsmechanismen flankierend könnten Block-Chain-Technologien aus der Welt der Kryptowährungen die Echtheit von Accounts und damit ihren menschlichen Ursprung überprüfen (Ehrenberg-Silies 20.10.2016, S. 7).

Eine Hürde haben Entwickler von Enttarnungssystemen und Bots gleichermaßen zu nehmen: die API der sozialen Plattformen ermöglicht bzw. beschränkt 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 bspw. Entwicklern von Enttarnungsmechanismen höhere API-Bandbreiten zur Verfügung stellen.

(9) Social Bots und ähnliche Internetphänomene werden 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 geschütztere „Second Internet“ befördert wird.

Social Bots werden auch als Treiber innerhalb der Debatte um das „postfaktische Zeitalter“ beschrieben: Lügen und Fakten seien immer schwerer voneinander unterscheidbar, Unwahrheiten würden 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. Falschmeldungen verbreiten sich immer schneller im Netz und prägten die Meinungsbildung. Der Erfolg von Populisten werde hierdurch und durch die nicht transparenten 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 wäre. So könnte einerseits das aktuelle weitgehend kostenfreie Netz bestehen bleiben, in dem Werbung, Hatespeech, Shitstorms und eben auch Social Bots vorzufinden seien, und andererseits könnte ein kostenpflichtiges Internet entstehen, das frei von diesen Phänomenen ist (Bovenschulte 14.10.2016, S. 4). Dies wäre der völlige Gegenentwurf zu dem bereits bestehenden, als Deep oder Dark Net 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 betreibt, ist offen. Ansätze zu geschlossenen Interneträumen gibt es schon heute. So existieren einige Chaträume und Foren, zu denen der Zutritt nur auf Empfehlung oder Einladung möglich ist (bspw. spezifische Chats auf quakenet).

Ein weiterer Aspekt, der im Zusammenhang von Social Bots und Zukunft des Internets von den Experten angemerkt wurde, ist die Anonymität und Ethik von Algorithmen (s. a. Reichert 2012). Für Algorithmen gebe es keinen "Ausweiszwang", keine Besteuerung und nur wenige Gesetze. Die Urheber von Algorithmen seien unbekannt, so dass diese intransparent und anonym agierten. Dies führe dazu, dass Algorithmen nicht rückverfolgt oder die Urheber verantwortlich gemacht werden könnten und die ausgelösten Schäden folgenlos für die Verursacher blieben (Helbing 2016, S. 7; Angwin 2016). Algorithmen sollten daher einer Rechenschaftspflicht nachkommen (Angwin 2016). Algorithmen könnten „markiert“ werden, um Herkunft und Identität eines sozialschädlichen Bots nachweisen zu können. Hierbei stellten 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 Ethik von Algorithmen wurde die Idee einer „Sozialverträglichkeitsprüfung“ von Algorithmen“ vorgeschlagen, vergleichbar mit einer Umweltverträglichkeitsprüfung (UVP) 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 bzw. allgemeiner: Bevor ein Algorithmus auf den Markt kommt, 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 wird (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 betrifft sowohl die Aspekte der Meinungsbildung als auch die Einflussnahme im Bereich von Marketing.

Literatur

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

Bessi, A., Ferrara, E. (2016): Social bots distort the 2016 U.S. Presidential election online discussion. In: First Monday 21(11).

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=.

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.

Bovenschulte, Marc (14.10.2016): Interview. Medien. Interview mit Peter Welchering.

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.

Ehrenberg-Silies, Simone (20.10.2016): Interview. ETH Zürich. Interview mit Dirk Helbing.

Falch, M., Henten, A., Tadayoni, R., Windekilde, I.M. (2009): Business Models in Social Networking. In: : CMI International Conference on Social Networking and Communities, S. 1–23.

Ferrara, E., Varol, O., Davis, C.A., Menczer, F., Flammini, A. (2014): The Rise of Social Bots. In: arXiv preprint arXiv:1407.5225.

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.

Fiegerman, S. (2014): The Curious Case of Cynk, an Abandoned Tech Company Now Worth $5 Billion. 10.7. http://mashable.com/2014/07/10/cynk/#CvEuP_Dbskqn (7.12.2016).

Fischer, F. (2016): Twitter-Bots. Ferngesteuerte Meinungsmache. 25.5. http://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.

Fuchs, M. (2016): Automatisierte Trolle. Warum Social Bots unsere Demokratie gefährden. 12.9. http://www.nzz.ch/digital/automatisierte-trolle-warum-social-bots-unsere-demokratie-gefaehrden-ld.116166 (8.11.2016).

Hegelich, S. (2016): Invasion der Meinungs-Roboter. In: Analysen & Argumente.

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.

Helbing, Dirk (2016): Ferngesteuert oder Selbstgesteuert - Perspektiven der Digitalen Gesellschaft. ETH Zürich - Department of Humanities, Social and Political Sciences (GESS). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2716984 (02.11.2016)

Higgins, J. (2016): Facebook. Annual Report 2015.

Howard, P.N., Kollanyi, B. (2016): #Strongerin, and #Brexit. Computational Propaganda During the UK-EU Referendum. In: Social Science Research Network.

Kind, Sonja; Weide, Sebastian (11.10.2016): Interview. TU München. Interview mit Simon Hegelich.

Kollanyi, Bence; Howard, Philip N.; Woolley, Samuel C. (2016): Bots and Automation over Twitter during the Third U.S. Presidential Debate, S. 1–4. http://politicalbots.org/wp-content/uploads/2016/10/Data-Memo-Third-Presidential-Debate.pdf (06.12.2016).

morgenpost.de (2016): Twitter Deutschland will offenbar Büro in Berlin schließen. 28.10. http://www.morgenpost.de/wirtschaft/article208553097/Twitter-Deutschland-will-offenbar-Buero-in-Berlin-schliessen.html (12.12.2016).

Newitz, A. (2015): Ashley Madison Code Shows More Women, and More Bots. 31.8. http://gizmodo.com/ashley-madison-code-shows-more-women-and-more-bots-1727613924 (13.5.2016).

Reichert, K. (2012): Plädoyer für eine Algorithmen-Ethik: Relevanz ist alles. 24.10. http://www.faz.net/aktuell/feuilleton/debatten/plaedoyer-fuer-eine-algorithmen-ethik-relevanz-ist-alles-11934495-p4.html (14.12.2016).

Steppat, T. (2016): Trump, AfD, Pegida: Wie Populisten durch Facebook groß werden. 11.11. http://www.faz.net/aktuell/politik/inland/wie-facebook-populisten-wie-trump-afd-und-pegida-gross-macht-14518781.html (14.12.2016).

Voß, J. (2016): Der Feind in meinem Netzwerk: Social Bots. http://politik-digital.de/news/der-feind-in-meinem-netzwerk-social-bots-144563/ (13.5.2016).

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).

Woolley, S.C. (2016): Automating Power. Social bot interference in global politics. In: First Monday 21(4).

Woolley, S.C., Howard, P.N. (2016a): Bots Unite to Automate the Presidential Election. 15.5. http://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.