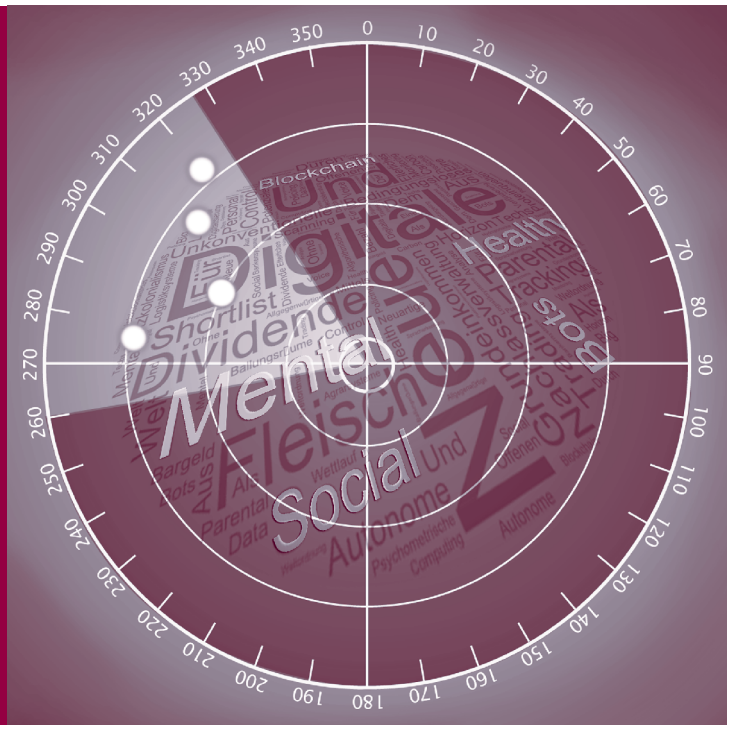
BÜRO FÜR TECHNIKFOLGEN-ABSCHÄTZUNG
BEIM DEUTSCHEN BUNDESTAG

Simone Ehrenberg-Silies
Daniel Thiele

Social Bots



Themenkurzprofil Nr. 10
Mai 2016

Social Bots

Kurzdarstellung des Themas

Social Bots (Social Robots) sind Computerprogramme, die darauf ausgerichtet sind, in sozialen Netzwerken, beispielsweise auf Facebook oder Twitter, maschinell erstellte Beiträge (Kommentare, Antworten, 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 durch einfache Anpassungen leicht skalieren, sodass beispielsweise auf Twitter tausende Accounts 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 sowie von Terrororganisationen gezielt eingesetzt werden. Die Social Bots sind in der Lage, sinnvolle Texte in einer Qualität zu erzeugen, die der von Menschen geschriebenen Texten ähnelt. Für Menschen ist es also selten offensichtlich, dass sie nicht mit einem Menschen, sondern mit einer Maschine kommunizieren. Die Menschenähnlichkeit wird auch dadurch suggeriert, dass der Social Bot nicht immer politisch agiert und kommentiert, sondern auch mehr oder weniger Belangloses bietet (Kommentare zu Fußballergebnissen, Hinweise auf Serieninhalte etc.). Von August 2015 bis Juli 2017 läuft ein Forschungsprojekt »Social Media Forensic« an der Universität Siegen mit dem Ziel, Wege zu finden, wie Social Bots im Internet identifiziert werden können. Für den Gesetzgeber ist es von Bedeutung, das Ausmaß und die Auswirkungen von Social Bots im Internet einschätzen und eventuelle gesellschaftliche Gefahren, die aus gezielten Manipulationsstrategien erwachsen, bewerten zu können. Gegebenenfalls sind gesetzliche Anpassungen notwendig, um derartige Aktivitäten im Internet rechtlich verfolgen zu können.

Hintergrund und Stand der Entwicklung

Die frühen Social Bots agierten zunächst recht simpel, indem sie massenweise Inhalte posteten und versuchten, ihren Wirkungskreis dadurch zu erweitern, dass sie beispielsweise auf Twitter Follower anderer Kontoinhaber wurden. Einem Team an der Texas A&M University gelang es somit 2011 noch relativ einfach, diese Social Bots zu enttarnen. Sie legten einige Fakeaccounts an, über die sie nun selbst Nonsensinhalte verbreiteten, die für menschliche Follower recht unattraktiv waren. Ihre Follower wurden daher nur Social Bots (Ferrara et al. 2014, S. 3).

Inzwischen sind Social Bots weitaus intelligenter. 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 Aktivitätsverhalten 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. Hochentwickelte Formen sollen sogar das Verhalten von real existierenden Nutzern weitestgehend kopieren können (stimmige inhaltliche Konversation, Imitierung zeitlicher Muster des Nutzungsverhaltens in sozialen Netzwerken) (Ferrara et al. 2014, S. 4). Allerdings sind durchaus noch Rückschläge zu verzeichnen, wie jüngst bei »Tay« zu beobachten war – einem Computerprogramm von Microsoft, welches in Dialogen mit Twitternutzern eingesetzt wurde und von diesen letztlich ohne Weiteres so manipuliert werden konnte, dass es sich rassistisch äußerte (Frankfurter Allgemeine Zeitung 2016).

Die Motive für die Verwendung von Social Bots sind unterschiedlich: In westlichen etablierten Demokratien werden sie beispielsweise von Politikern eingesetzt, die durch sie ihre Anzahl von Followern erhöhen wollen, um so populärer zu erscheinen. Von solchen Fällen wurde aus Australien, Italien, dem Vereinigten Königreich sowie den USA berichtet (Woolley 2016, S. 6), aktuell beispielsweise mit Bezug zum US-amerikanischen Präsidentenwahlkampfs: So gehen Experten davon aus, dass jeder Vierte von den 8 Mio. Twitterfollowern des republikanischen Präsidentschaftsbewerbers Donald Trump ein Social Bot sei (Moorstedt 2016). Auch im Zusammenhang mit politischen Parteien wird in den Medien vereinzelt der Verdacht geäußert, dass auch diese zur Erhöhung ihrer Followerzahlen Social Bots einsetzen. Ob es sich bei den berichteten Fällen tatsächlich um Social Bots handelte und ob diese von den Parteien selbst oder von einem politischen Gegner gekauft worden sind, konnte allerdings nicht geklärt werden (politik-digital.de 2016); (Moorstedt 2016). Grundsätzlich ist es jedoch möglich, »virtuelle Freundschaften in Hunderterpaketen« (Schieb 2016) bei Agenturen zu kaufen. Das Marktvolumen des Handels mit gefälschten Nutzerprofilen wird auf 40 bis 360 Mio. US-Dollar geschätzt (Fischer 2016).

In Deutschland sind Parteien jedoch auch Opfer von Manipulationen geworden: Es wird beispielsweise vermutet, dass Social Bots gezielt eingesetzt werden, um Parteien zu diskreditieren. (DRadio Wissen 2016).

Nicht nur autoritäre Regime (Aserbaidschan, Bahrein, Saudi Arabien) und Regime mit autoritärer Tendenz (Russland, China, Venezuela), sondern auch demokratisch agierende Systeme – allerdings mit Einschränkungen – (Argenti-

nien, Mexiko, Südkorea) nutzen Social Bots sogar, um in den sozialen Netzwerken Pro-Regierungs-Botschaften zu verbreiten oder gegen die Opposition vorzugehen (Woolley 2016, S. 7).

Sie werden ebenfalls von Regierungen verwendet, um gegen feindliche Aktivitäten im Ausland vorzugehen. Im Februar 2011 war beispielsweise auf der Ausschreibungsplattform FBO.gov der US-Bundesregierung eine Ausschreibung zu finden, in der ein Unternehmen gesucht wurde, welches eine »Persona Management Software« liefern könne (Lischka 2011). Diese Software sollte es jedem Anwender ermöglichen, zehn Netztarnidentitäten einzunehmen (SPIEGEL Online 2011). Diese wollte das US-Oberkommando Centcom nutzen, »um Centcom in die Lage zu versetzen, der Propaganda von gewalttätigen Extremisten und Feinden von außerhalb der USA zu begegnen«, indem Netznachrichten auf Arabisch, Farsi, Urdu und Paschtu verbreitet würden (SPIEGEL Online 2011). Forscher um Simon Hegelich von der Hochschule für Politik in München haben im Januar 2015 eine »Bot-Armee« beobachtet, die mit 15.000 Twitterprofilen Propaganda im Ukraine-Russland-Konflikt verbreitete (Breithut 2016).

Doch nicht nur Regierungen sind Urheber von Social Bots. Private Akteure, die im Wesentlichen unentdeckt bleiben, programmieren sie, um Daten zu sammeln, indem sie beispielsweise realen Nutzern auf Facebook Freundschaftsanfragen stellen, die dann auch angenommen werden. Sie sind auf Bewertungsportalen aktiv, initiieren und führen Dialoge auf Plattformen, die Dienstleistungen gegen Bezahlung anbieten (Schieb 2016). So wurde im Jahr 2015 bekannt, dass auf der Datingplattform Ashley Madison rund 70.000 weibliche Social Bots aktiv sind, die Männern Glauben machen, es besteht eine große Auswahl an potenziellen Partnerinnen (Newitz 2015). Außerdem werden Nutzer der Dating-App Tinder von Social Bots z. B. in Abo-Fallen gelockt (politik-digital.de 2016).

Um die eigenen Produkte, das eigene Unternehmen oder die eigene Person beispielsweise auf Instagram als populärer erscheinen zulassen, können User zudem auf Webseiten wie http://bestsocialbots.com/ komplette Social-Bot-Pakete erwerben. So verspricht das Angebot »Instagram Mega Boost Package« »Follower, Likes, Shoutouts« – alles in einem (Best Social Bots 2013). Der Preis für 1.000 Fakefacebookfreunde beträgt in etwa 30 US-Dollar; 15.000 Retweets können für 15 US-Dollar erworben werden (politik-digital.de 2016). In diversen Foren wird ein reger Austausch über die Effizienz von bestimmten Social Bots diskutiert und Empfehlungen zur Verwendung ausgesprochen (Quora 2016).

2011 gelang es Forschern der University of British Columbia in Kanada, 8 Wochen lang Facebook mit Social Bots zu infiltrieren (80 % der Versuche waren erfolgreich), was zeigte, dass das von Facebook zur Abwehr solcher Angriffe genutzte Facebook Immune System keinen ausreichenden Schutz bieten konnte

(Boshmaf et al. 2011, S. 93). Bei Facebook geht man derzeit von 15 Mio. Fakeaccounts aus (Breithut 2016) (im 3. Quartal 2014 nutzten rund 1,35 Mrd. Menschen Facebook aktiv) (Statista 2016). Twitter teilte der U.S. Securities und Exchange Commission im Jahr 2014 mit, dass 23 Mio. seiner aktiven Nutzerkonten Social Bots seien (Woolley 2016, S. 1). Insgesamt gehen Experten davon aus, dass es weltweit rund 100 Mio. Fakeaccounts gibt (Schieb 2016).

Die Zunahme von Social-Bot-Manipulationen in sozialen Netzwerken erfordert die Entwicklung von validen und effektiven Enttarnungssystemen. Im Projekt Social Media Forensics (Laufzeit August 2015 bis Juli 2017), welches von der Universität Siegen und den Konsortialpartnern der Cologne Business School sowie dem Leibniz-Institut für Sozialwissenschaften (GESIS) durchgeführt wird, sollen Methoden und Konzepte entwickelt werden, wie Manipulationen in sozialen Netzwerken durch Bots, Bot-Netze und Trolle entdeckt werden können (Team FoKoS 2015). Vor allem anhand des Farbschemas des Profilfotos, welches im Nutzeraccount verwendet wird, soll ein Algorithmus überprüfen, ob es sich um einen menschlichen Nutzer oder um einen Bot handelt (Breithut 2016). Das ist möglich, da die Profilbilder von Social Bots eine charakteristische Farbstruktur haben. Für sie werden z. B. häufiger Comicbilder eingesetzt, die sich farblich von echten Fotos unterscheiden und dadurch identifizierbar werden (Weck 2016).

Alternative Systeme wie »Bot or Not?«, ein »Truthy Project« der Indiana University in Bloomington (http://truthy.indiana.edu/botornot/), bieten Twitternutzern an, in Zweifelsfällen online zu überprüfen, mit welcher Wahrscheinlichkeit es sich bei bestimmten Twitteraccounts um Social Bots oder um menschliche Eigentümer handelt. In die Analyse fließen unter anderem Nutzermerkmale, Zeitprofile (Aktivitätsverhalten in zeitlicher Dimension), gepostete Inhalte und die Art der sozialen Kontakte eines Nutzerkontos mit ein (Davis et al. 2016, S. 274). Den gleichen Service bietet – bereits seit 2012 – die Webseite https://www.twitteraudit.com/, die die Authentizität von Twitteraccounts auf Basis der Anzahl der Tweets, des Datums des letzten Tweets und des Verhältnisses von Followern zu Freunden bestimmt. Die Grundgesamtheit für die Auswertung bilden 5.000 zufällig ausgewählte Follower des zu überprüfenden Accounts (TwitterAudit 2016).

Gesellschaftliche und politische Relevanz

Soziale Netzwerke sind heutzutage u. a. zentral für die private Kommunikation zwischen Menschen – Freunden und Unbekannten –, zur Verbreitung von Werbung für Produkte und Dienstleistungen sowie als Forum für politische und gesellschaftliche Diskussionsprozesse. Meinungen und politische Positionen, Kau-

fentscheidungen für Produkte etc. verbreiten sich in ihnen in Windeseile und produzieren und reproduzieren kommerzielle Trends und politische sowie gesellschaftliche Dynamiken. Inzwischen konnte sogar durch Forschungsergebnisse belegt werden, dass sich auf Facebook geäußerte Emotionen auf die Emotionen befreundeter Personen auswirken können, also emotionale Ansteckungsgefahr besteht (Kramer et al. 2014). Werden in sozialen Netzwerken nun massenhaft Social Bots eingesetzt – sei es durch Regierungen, Politiker, Unternehmen, zivilgesellschaftlichen Organisationen oder Privatpersonen –, kann dadurch massiv die Wahrnehmung der Realität beeinflusst werden (Ferrara et al. 2014, S. 3).

Da inzwischen zahlreiche Dienstleister Prognosen und Analysen beispielsweise zu Vorlieben, politischen Meinungen und Einstellungen (Predictive Analysis) auf der Basis von Daten aus sozialen Netzwerken erstellen (z. B. Trendanalysten von Twitterhashtags wie http://trends24.in/germany/ und http://trendsmap.com/), gefährden sie mittelbar auch deren Validität und manipulieren dadurch die Entscheidungsgrundlage Dritter (politicaldatascience.blogspot.de 2016; Team FoKoS 2015).

Besonders risikoreich wird es, wenn Social Bots und andere Computerprogramme, wie z. B. automatische Handelssysteme zusammenwirken: So fand 2014 eine orchestrierte Social-Bot-Kampagne auf Twitter statt, die den Eindruck erweckte, dass Nutzer sich interessiert über ein Technikunternehmen mit dem Namen Cynk austauschten. Die Algorithmen automatischer Handelssysteme interpretierten diese Twitterdiskussion derart, dass sie begannen, intensiv mit Aktien dieser Firma zu handeln, die dadurch letztlich ihren Marktwert um das 200-Fache steigern konnte (Ferrara et al. 2014, S. 3).

Die Social Bots machen es für den Gesetzgeber notwendig, sich einen Überblick über das tatsächliche Ausmaß ihres Einsatzes sowie ihrer Wirkungskraft zu verschaffen, zumal sowohl gezielte Social-Bot-Manipulationen ausländischer Regierungen als auch Social-Bot-getriebene Hetzkampagnen, die ihren Ursprung im Inland haben, politische Diskussionen verzerren und gesellschaftliche Konflikte, wie sie sich beispielsweise in den Debatten um Einwanderung abzeichnen, verschärfen können. Es gilt zu überprüfen, ob der Rechtsrahmen für soziale Netzwerke wie Facebook, Instagram, Twitter etc. angepasst werden muss, um die Betreiber dieser Dienste stärker in die Pflicht nehmen zu können, gegen Social Bots auf ihren Plattformen vorzugehen. Ebenfalls ist zu klären, nach welchen gesetzlichen Vorgaben die Programmierung und Verbreitung von Social Bots mit manipulativer Absicht heutzutage rechtlich verfolgt werden könnten oder ob effektive gesetzliche Grundlagen erst noch geschaffen werden müssen.

Mögliche vertiefte Bearbeitung des Themas

Das Thema Social Bots könnte sowohl in Form einer Kurzstudie als auch im Rahmen eines umfassenderen TA-Projekts untersucht werden. In eine Kurzstudie könnten (unter Ausschluss von Rechtsfragen) die Ergebnisse eines Literaturscreenings, eines Expertenworkshops sowie von Experteninterviews einfließen. Da es sich bei Social Bots um ein aufkommendes Thema (Emerging Issue) handelt, zu dem nur ein sehr kleiner wissenschaftlicher Textkorpus existiert (überwiegende Anzahl der Veröffentlichungen zum Thema erscheinen in der Tagespresse, in Internetblogs oder in populärwissenschaftlichen Quellen), ist es für eine stärker expertenbasierte explorative Herangehensweise prädestiniert. Experten, die zum Thema Social Bots befragt werden könnten, sind beispielsweise Vertreter von sozialen Netzwerken, zivilgesellschaftlichen Organisationen (Verbraucherverbände, Bitcom etc.), Programmierer (Chaos Computer Club), Forscher (Entwickler von Enttarnungssystemen) etc. In der Kurzstudie könnten Fragen zu Risiken des zunehmenden Einsatzes von Social Bots erörtert und Maßnahmen zu ihrer Eindämmung diskutiert sowie deren Umsetzbarkeit bewertet werden. Im Rahmen eines umfassenden TA-Projekts könnten u. a. die rechtlichen Aspekte des weiteren Umgangs mit Social Bots (und ihren Urhebern) aufgearbeitet werden.

Literatur

Best Social Bots (2013): Instagram Mega Boost Package. 25.12., http://bestsocialbots.com/?p=1494 (13.5.2016)

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

Breithut, J. (2016): Wie Social Bots uns manipulieren, wer daran verdient und wie die Fakes auffliegen. 12.4., http://www.bento.de/gadgets/social-bots-manipulieren-facebook-und-twitter-einige-verdienen-damit-geld-258770/

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

DRadio Wissen (2016): Hasskommentare von Fake-Accounts. DRadio Wissen. 9.2., http://dradiowissen.de/beitrag/social-bots-hasskommentare-von-fake-accounts (9.6.2016)

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

Fischer, F. (2016): Twitter-Bots. Ferngesteuerte Meinungsmache. 25.5., www.zeit.de/digital/internet/2013-05/twitter-social-bots (9.6.2016)

Frankfurter Allgemeine Zeitung (2016): Microsoft Tay. Der Chat-Computer dreht schon wieder durch. 30.3., www.faz.net/aktuell/wirtschaft/netzwirtschaft/chat-bot-tay-von-microsoft-dreht-schon-wieder-durch-14151785.html (13.5.2016)
Kramer, A.D.; Guillory, J.E.; Hancock, J.T. (2014): Experimental evidence of massive-scale emotional contagion through social networks. In: Proceedings of the National Academy of Sciences of the United States of America 111(24), S. 8788–90
Lischka, K. (2011): US-Sicherheitsfirma HBGary. Computerknacker im Staatsauftrag. 23.2. www.spiegel.de/netzwelt/web/us-sicherheitsfirma-hbgary-computerknacker-im-staatsauftrag-a-746969.html (10.5.2016)
Moorstedt, M. (2016): US-Wahl – Trumps Twitter-Bots werden zur politischen Gefahr. 23.5., www.sueddeutsche.de/digital/us-wahl-wie-trumps-twitter-bots-zur-politischen-gefahr-werden-1.3002280 (9.6.2016)
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)
politicaldatascience.blogspot.de (2016): Social Media Forensics. 11.5., http://politicaldatascience.blogspot.de/p/somefo.html (11.5.2016)
politik-digital.de (2016): Der Feind in meinem Netzwerk: Social Bots. http://politik-digital.de/news/der-feind-in-meinem-netzwerk-social-bots-144563/ (13.5.2016)
Quora (2016): What are the top 3 Instagram bots that automatically like hashtags you choose? https://www.quora.com/What-are-the-top-3-Instagram-bots-that-automatically-like-hashtags-you-choose (13.5.2016)
Schieb, J. (2016): Social Bots verpesten das Netz. 22.1., https://blog.wdr.de/digitalistan/social-bots-verpesten-das-netz/ (13.5.2016)
SPIEGEL Online (2011): US-Cyber-Krieg über Facebook und Co.: Angriff der Sockenpuppen. 17.3., www.spiegel.de/netzwelt/netzpolitik/us-cyber-krieg-ueber-facebook-und-co-angriff-der-sockenpuppen-a-751567.html (10.5.2016)
Statista (2016): Facebook. Monatlich aktive Nutzer weltweit 2016. http://de.statista.com/statistik/daten/studie/37545/umfrage/anzahl-der-aktiven-nutzer-von-facebook/ (11.5.2016)
Team FoKoS (2015): Social Media Forensics – Projektvorstellung. 17.12., https://www.uni-siegen.de/fokos/forschungsprojekte/somefo/?lang=de (11.5.2016)
TwitterAudit (2016): About TwitterAudit. https://www.twitteraudit.com/ (9.6.2016)
Weck, A. (2016): Wie Social-Media-Trends durch Bots manipuliert werden. 6.4., http://t3n.de/news/social-media-trends-bots-694529/ (7.6.2016)
Woolley, S.C. (2016): Automating power. Social bot interference in global politics. In: First Monday 21(4), http://journals.uic.edu/ojs/index.php/fm/article/view/6161/5300

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