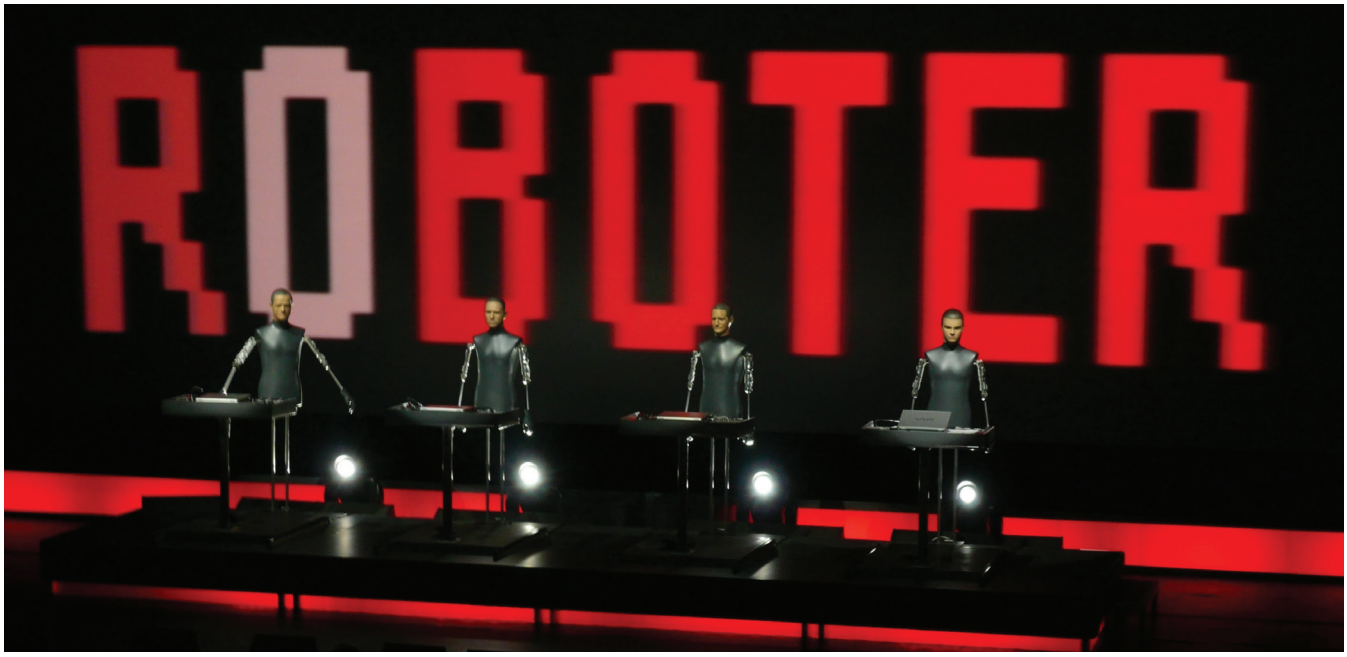
Analysen & Argumente

Konrad Adenauer Stiftung

SEPTEMBER 2016
AUSGABE 221




# Invasion der Meinungs-Roboter

*Simon Hegelich*

## Zum Mitnehmen

- Social Bots beeinflussen Meinung, ihr bevorzugter Wirkungsraum sind die sozialen Netzwerke: Bei Debatten um den Brexit, bei Ereignissen wie die russische Annexion der Krimhalbinsel, während des Ukrainekonflikts, und aktuell im Wahlkampf zwischen Trump und Clinton haben sie bereits in den Meinungsbildungsprozess eingegriffen.

- Social Bots sind von Menschen programmierte Software-Roboter. Sie sammeln Informationen und Daten, setzen aber auch bewusst Trends und Topthemen in den sozialen Medien, ohne dass der Nutzer davon Kenntnis hat. Das Beeinflussungspotenzial – der sogenannte „Bot-Effekt" – ist theoretisch sehr groß, lässt sich empirisch aber nur schwer nachweisen.

- Es wird immer schwerer, Bots von Menschen zu unterscheiden. Bots betreiben Fake-Profile und geben somit vor, Menschen zu sein. Sie mischen sich bewusst in die öffentliche Diskussion in den sozialen Medien ein. Vermehren sich Bots in den sozialen Medien überproportional, könnten sie sich disruptiv auf bestehende Nachrichtenplattformen wie z.B. Twitter auswirken, da die Nutzer keinen Sinn mehr darin sehen, auf einer Plattform zu kommunizieren, auf der sich zum großen Teil nur noch Maschinen als Gesprächspartner befinden.

- Politische Gruppen und Parteien können Social Bots auch in Deutschland für sich nutzen. Der erfolgreiche Umgang mit Bots in den USA wird auch in Deutschland ankommen und dort zu einem intensiven Einsatz von Social Bots hinsichtlich politischer Kommunikation führen.

- Transparenz und der Anstoß einer offenen Debatte können entscheidend zu einer Aufklärung und einem kompetenten Umgang mit Social-Bots beitragen. Die Gleichung, dass Qualität und Quantität zusammengehören, gilt für das Internet nicht.

INHALT



## Einleitung

Ob Brexit, Russland-Ukraine-Konflikt oder der US-Präsidentschaftswahlkampf: Immer häufiger treten in den sozialen Netzwerken Social Bots auf, die versuchen, Einfluss auf politische Debatten zu nehmen. Der folgende Text beschreibt, was Bots sind, wie Social Bots funktionieren und welche Gefahren damit verbunden sind. Darüber hinaus werden Beispiele für politische Aktivitäten von Social Bots aufgeführt. Abschließend wird prognostiziert, welche Entwicklungen in diesem Bereich in naher Zukunft zu erwarten sind.

## Was sind Bots?

Der Begriff „Bots" als Kurzform von Roboter hat sich entwickelt, um damit autonom agierende Programme im Internet zu bezeichnen. Diese Bezeichnung ist aber nicht eindeutig und bedarf einer Konkretisierung: Häufig werden z. B. die Skripte, mit denen Suchmaschinen wie Google das Internet durchkämmen, Bots genannt, oder auch Computer, die von einer Schadsoftware befallen wurden und jetzt ein Eigenleben führen. Aktuell geht es bei Bots aber eher um automatisierte Accounts in den sozialen Netzwerken, die als „Chat-Bots" oder einfache künstliche Intelligenz Routineaufgaben übernehmen, oder aber als „Social Bots" ihre wahre Identität verschleiern, und den Nutzern vorgeben, sie wären echte Menschen. Vor mehr als 20 Jahren hat der Wissenschaftler Roger Clark bereits auf die Gefahren hingewiesen, die von einer „active digital persona" ausgehen können.[1]

## Wie funktionieren Social Bots?

Social Bots werden zunehmend im politischen Kontext eingesetzt

Während Bots derzeit von Technologieunternehmen wie Facebook, Google und IBM als neuer Trend ausgerufen werden, durch den Apps und Webseiten überflüssig gemacht werden sollen, weil die Nutzer direkt mit dem Bot-Assistenten interagieren, werden Social Bots zunehmend im politischen Kontext eingesetzt. Dabei geht es darum, die Öffentlichkeit oder bestimmte Zielgruppen durch die automatisch generierten Inhalte und Interaktionen zu beeinflussen.[2]

Technisch gesehen sind Social Bots heute sehr einfach zu erstellen. Man braucht dafür drei Elemente: Nutzeraccounts, die in dem entsprechenden sozialen Netzwerk registriert sind, Zugriff auf eine automatisierte Schnittstelle (API) des sozialen Netzwerks und ein Programm, das die Bot-Accounts automatisch steuert. Die registrierten Nutzeraccounts werden in der Regel im Internet käuflich erworben. Anbieter von falschen Social Media Accounts erstellen diese entweder per Hand oder gleich automatisiert oder bieten auch Zugangsdaten zu gehackten Accounts an. Je nach Qualität zahlt man derzeit für 1.000 falsche Accounts zwischen 45 $ (einfache Twitter-Accounts) und 150 $ („gealterte" Facebook-Accounts). Die Anbieter sind in der Regel im Ausland (häufig Russland) tätig.

Social Bots kann man mit einfachen Mitteln erstellen

Die APIs stellen die sozialen Netzwerke im Prinzip kostenlos zur Verfügung, um Entwickler für ihre Plattform zu gewinnen. Dabei gibt es allerdings große Unterschiede hinsichtlich des Registrierungsprozesses und der Benutzerfreundlichkeit der API, was dazu führt, dass Netzwerke wie Twitter und Instagram wesentlich mehr Bots aufweisen als z. B. Facebook - einfach weil es dort einfacher ist, auf die API zuzugreifen.

Einmal programmiert, kann ein Bot zu einer ganzen Armee ausgebaut werden

Die Software zur Steuerung der Bots kann entweder ebenfalls käuflich erworben werden. Eine sehr hochwertige Software, mit der sich 10.000 Twitter-Accounts steuern lassen, kostet ca. 500 $. Auch auf Basis von bestehenden Software-Bibliotheken können Bots leicht selber programmiert werden (ein „Minimal-Bot" kommt mit nur 15 Zeilen Code aus). Die Unterschiede zwischen den Bots sind sehr groß. Im einfachsten Fall beschränkt sich das selbständige Handeln dieser Roboter darauf, vorgefertigte Nachrichten zu versenden. Es gibt aber auch Bots (wenn auch seltener), die in der Lage sind, mit echten Nutzern zu interagieren und eigenständig neue Texte zu generieren. Da die normale Kommunikation in den sozialen Netzwerken in der Regel nicht besonders komplex ist, fallen aber auch die primitiven Bots häufig nicht auf. Ein typischer Bot auf Twitter könnte z. B. Nachrichten selbstständig generieren, die auf Texten aus zuvor ausgewählten Webseiten basieren, anderen Nutzern automatisch folgen, auf „Knopfdruck" oder auch nach einem zufallsvarierten Zeitplan vorgefertigte Propagandanachrichten senden und diese mit Stichworten und Hashtags schmücken, die derzeit populär sind. Von der technischen Seite ist es wichtig zu bedenken, dass diese Bots im Prinzip beliebig skalierbar sind: Wer ein Programm hat, mit dem sich ein Bot steuern lässt, kann damit auch eine ganze Armee von Bots lenken.

## Gefahren durch Social Bots

Bots manipulieren Trends im großen Stil

Aus der schieren Masse der Nachrichten, die sich durch ein Botnetz absenden lassen ergibt sich die aktuell bedeutendste Gefahr: Bots manipulieren die Trends in sozialen Netzwerken und diese Trends fließen in politische und wirtschaftliche Entscheidungsprozesse ein. Unter dem Schlagwort „Big Data" setzen immer mehr Unternehmen in den unterschiedlichsten Bereichen darauf, das Verhalten der Nutzer in den sozialen Netzwerken zu analysieren, um Erkenntnisse über die Position der eigenen Marke, aber auch über das Verhalten von potentiellen Kunden zu erhalten oder gesellschaftliche Trends zu entschlüsseln. Auch im politischen Bereich werden solche Analysen bereits eingesetzt.[3] Während man dabei in Deutschland noch relativ zurückhaltend agiert[4], hat sich die politische Social Media Analyse international bereits zu einem bedeutenden Markt entwickelt, auf dem sich Akteure wie Civics Analytics (derzeit für Hillary Clinton aktiv) und Cambridge Analytica (im Auftrag von Donald Trump) engagieren. Wenn nun Trends im großen Stil durch Bots manipuliert sind und Bots in allen Debatten von Bedeutung mitmischen (siehe nächstes Kapitel) - dann liegen diese Analysen im harmlosesten Fall einfach daneben. Im schlimmsten Fall verleiten sie aber Politiker dazu, in ihren Statements oder sogar in ihrer Politik auf solche Trends einzugehen wodurch die Position, für die die Bots stehen unter Umständen einen Zuspruch erhält, den die Bots alleine nicht erreicht hätten.

Social Bots können ein aufgeheiztes Diskussionsklima erzeugen

Die zweite Gefahr besteht darin, dass bestimmte Gruppen in ihrer Meinung durch Bots beeinflusst werden. Dabei ist allerdings relativ sicher ausgeschlossen, dass Manipulation quasi auf Zuruf der Bots passiert: Alle Studien sprechen dagegen, dass jemand seine politische Überzeugung ändert, nur weil er eine Nachricht in den sozialen Netzwerken sieht. Eine subtilere Manipulation ist aber sehr wahrscheinlich. Wenn beispielsweise durch Bots massenhaft extreme Inhalte in einem Diskussionskontext (wie z.B. eine Facebook-Gruppe oder ein thematischer Hashtag) verbreitet werden, dann wird dies in der Regel dazu führen, dass sich gemäßigte Personen aus diesem Diskussionszusammenhang zurückziehen. Personen, die eine radikal konträre Position zu den Bot-Nachrichten haben, fühlen sich herausgefordert, gegen diese Inhalte vorzugehen, was wiederum Personen, die die von den Bots verbreitete Meinung teilen, auf die Barrikaden bringt. So entsteht ein aufgeheiztes Diskussionsklima, in

dem Personen, die tendenziell für radikale Positionen empfänglich sind, sich ermutigt fühlen.

Drittens können Bots auch gezielt in einem Cyber-Warfare Szenario angewandt werden. Dabei reicht die Spannbreite von der Unterwanderung sozialer Netzwerke zur Ausspionierung der Nutzer, über die gezielte Verbreitung von Falschnachrichten (z. B. in Krisensituationen), bis hin zu Cyber-Attacken wie der Verbreitung von Schadsoftware oder auch der Organisation von sogenannten DDoS-Attacken[5].

## Bots in freier Wildbahn – der „Bot-Effekt"

Die folgenden Beispiele zeigen, dass die oben genannten Strategien bereits im großen Umfang eingesetzt werden. Die Analyse dieser Bot-Einsätze verdeutlicht aber auch, wie gegen solche Aktionen vorgegangen werden kann und welche Risiken tatsächlich realistisch sind.

Je 30 Prozent der Twitter-Follower der beiden Kanditaten im US-Präsidentschaftswahlkampf sind keine Menschen

Im aktuellen amerikanischen Präsidentschaftswahlkampf ist davon auszugehen, dass Social Bots einen beträchtlichen Anteil der Follower der Kandidaten ausmachen. Das online-Magazin „vocativ" berichtet, dass der Anteil der realen Twitter-Follower sowohl bei der demokratischen Kandidatin Hillary Clinton als beim republikanischen Kandidaten Donald Trump um die 60 Prozent liegen. Zudem wäre die Zahl von Trumps Fake Follower im Vergleich zu einer im Sommer 2015 durchgeführten Analyse stark angestiegen.[6]

Bereits im US-Präsidentschaftswahlkampf 2012 wurde ein plötzlicher Anstieg der Follower des damaligen Herausforderers festgestellt und auf den Einsatz von Fake Follower zurückgeführt.[7] Auch bei den politischen Parteien in der Schweiz wurden massenhaft Fake User festgestellt.[8] Vor dem italienischen Parlamentswahlkampf 2013 wurden die Twitter-Follower eines Kandidaten-Accounts mittels eines „Boterkennungs-Algorithmus" überprüft und dabei festgestellt, dass über die Hälfte Fake Follower waren.[9] Die „Twiplomacy Studie" stellt in ihrem aktuellen Ranking der Twitteraccounts von Staatsoberhäupter und politischen Führern fest, dass der venezolanische Präsident am zweithäufigsten Tweets auf Twitter postet und an dritter Stelle bei der retweet-Statistik steht.[10] Auffällig dabei ist, dass seine Nachrichten viel weniger häufig favorisiert werden, was darauf hindeutet, dass es sich bei einem Teil seinen Follower um Fake User handelt.

„likes" und shares" sind die Kenngrößen bei der Manipulation von Trends

Diese einfachste Art der Manipulation sozialer Netzwerke, in der durch Bots pure Masse und gar keine neuen Inhalte erzeugt werden, mag zunächst als eine relativ harmlose Manipulation erscheinen, jedoch sind die Auswirkungen nicht unerheblich.[11] Hinzu kommt, dass die sozialen Netzwerke über Algorithmen gesteuert werden, die beliebte Inhalte präferieren. Wer viele Follower hat, wird von den sozialen Netzwerken privilegiert behandelt und erreicht somit auch mehr echte Nutzerinnen und Nutzer. Eine weit verbreitete Art, Trends in den sozialen Netzwerken zu manipulieren, besteht darin, gezielt die Kenngrößen anzugreifen, die rein quantitativ erhoben werden. Das sind z. B. „likes" und „shares" auf Facebook und die Häufigkeit von Hashtags auf Twitter.

Im Zuge der Brexit-Debatte konnten Wissenschaftler feststellen, dass sehr viele der Tweets mit dem Hashtag „#Brexit" von Bots stammten.[12] Hashtags, die mit der „Remain-Kampagne" verbunden wurden (wie z. B. „#StongerIn") wurden wesentlich seltener von den Bots benutzt. Dieses Beispiel zeigt aber auch, dass die Gefahr durch Bots schnell überschätzt wird: Theoretisch hätte im Vorfeld der Eindruck ent-

stehen können, dass die Brexit-Kampagne klar vorne in der Wählergunst liegt. Dies hätte eventuell Remain-Anhänger veranlasst, nicht abzustimmen, weil die Wahl anscheinend schon entschieden ist. Bekanntlich war die Einschätzung jedoch allgemein so, dass es einen (vermutlich knappen) Sieg für Remain geben würde. Es ist auch nicht ersichtlich, dass die Bots einen spürbaren Effekt auf das Abstimmungsverhalten gehabt haben. Twitter wird in Großbritannien fast ausschließlich von jüngeren Personen mit hohem Bildungsniveau verwendet. Genau diese demografische Gruppe stimmte aber gegen den Brexit. Zudem zeigen die analysierten Daten, dass ein großer Teil der Bots sowohl die pro-Brexit als auch die remain-Hashtags bedient hat. Vermutlich, weil es sich bei vielen Bots gar nicht um politische Bots handelte, sondern einfach um Werbespam, die ihre Werbebotschaft mit genau den Hashtags versehen, die gerade im Trend sind. Das Beispiel zeigt also, dass selbst die massenhafte Beeinflussung von Trends noch nicht mit einer effektiven Manipulation gleichzusetzen ist.

Ein wesentlich komplexeres Botnetzwerk wurde im Kontext des Ukrainekonflikts aufgespürt[13]. Hier sind ca. 15.000 Twitter-Accounts aktiv, die im Durchschnitt 60.000 Meldungen pro Tag absetzen. Die Inhalte der Meldungen sind auf die antizipierten Interessen junger Männer in der Ukraine ausgerichtet: Die Bots reden viel über Fußball, erzählen sexistische Witze und verbreiten Links zum illegalen Download aktueller amerikanischer Kinofilme. Zwischendurch werden aber gezielt Propaganda-Nachrichten des „Rechten Sektors" – einer ultranationalistischen ukrainischen Vereinigung mit paramilitärischem Ableger – verbreitet. Dabei lassen sich verschiedene Strategien der Manipulation identifizieren. Zum einen geht es auch hier um die Verfälschung von Trends, indem bestimmte Hashtags besonders populär gemacht werden. Darüber hinaus verknüpfen die Bots aber bewusst Schlagworte wie „Maidan" und „Euromaidan" mit dem Hashtag „Rechter Sektor", offenbar, um die Algorithmen von Twitter dazu zu bringen, Nutzern, die nach „Maidan" suchen, auch Inhalte des „Rechten Sektors" zu präsentieren. Als weitere Strategie wird die Verbreitung von Falschinformationen hier deutlich: So verbreitete das Botnetz die Nachricht, die Separatisten hätten von Russland Raketen erhalten und würden nun auf Kiev schießen. Außerdem folgen die Bots gezielt ukrainischen Politikern, um ihre eigene Reichweite zu erhöhen. Denn selbst wenn diese nicht auf die Bots hereinfallen und bewusst oder versehentlich deren Nachrichten weiterleiten wird Twitter so die Nachrichten der Bots eher anderen Nutzern präsentieren, die ebenfalls diesen Politikern folgen. Die Ukraine-Bots verfügen zudem über ein ganzes Arsenal an Tricks, wie sie klassischen Bot-Erkennungsalgorithmen ausweichen können: Sie folgen sich gegenseitig und haben dadurch ein ausgewogenes Verhältnis von Freunden und Followern, sie posten nach einem zeitlichen Muster, das Pausen und Schlafenszeiten simuliert, aber trotzdem zufällig ist und sie verfügen über die Fähigkeit, Nachrichten geringfügig abzuwandeln, so dass die Aussage zwar identisch bleibt, automatische Programme aber die Texte nicht als identisch erkennen können.

Trick der Bots: Simulation von Schlafzeiten, ausgewogenes Verhältnis von Freunden und Followern

Von Russland wird berichtet, dass im Jahr 2013 ein großes Projekt zum Aufbau einer Infrastruktur zur Manipulation sozialer Medien abgeschlossen wurde. Neben der sogenannten „Trollfabrik", die in Sankt Petersburg schon seit geraumer Zeit Meinungen aller Art produziert, sind Social-Bots die logische Weiterentwicklung. Insbesondere im Rahmen des Krieges in der Ukraine waren russlandfreundliche Kommentare im deutschsprachigen Internet in der deutlichen Überzahl, was im Widerspruch zu Umfragewerten und der Position der mit dem Thema befassten Journalisten sowie Volksvertreter steht.

Technisch primitiver, dafür aber von der übergeordneten Strategie her sehr ambitioniert, agiert derzeit ein Botnetz, das sich mit Donald Trump beschäftigt. Die Bots –

ausschließlich gutaussehende junge Frauen und Männer – haben sich auf die Verbreitung von Witzen spezialisiert. Dabei werden allerdings sehr viele Nachrichten gepostet, die blanker Rassismus und Antisemitismus sind. Zwischendurch werden Nachrichten eingestreut, die Donald Trump beleidigen. Vermutlich gehen die Macher dieses Botnetzes davon aus, dass Anhänger von Trump es gar nicht mitkriegen würden, wenn ihr Kandidat im Internet beleidigt wird. Die rassistischen Witze sollen also sozusagen die Filterbubble durchdringen, damit die diskreditierende Nachricht ihre Wirkung entfalten kann. Dass auf diesen Weg massenhaft rassistische Propaganda der übelsten Sorte als Kollateralschaden ins Internet gelangt, scheint die Macher dieses Botnetzes wenig zu stören.

Mit rassistischen Witzen gegen die Filterbubble

Bots müssen sich aber nicht auf die Verbreitung von Nachrichten beschränken. Ihre Aufgabe kann auch weit darüber hinausgehen und in den Bereich Cyber-Warfare übergreifen. Dabei werden sogenannte „Social Engineering" Strategien angewandt, bei denen es darum geht, mit Hilfe von psychologischen Tricks wie zum Beispiel Suggestion Einfluss auf den User zu nehmen, um den gewünschten Effekt zu erzielen:

Auf der Hackerkonferenz „Black Hat" wurde ein Konzept vorgestellt, wie künstliche Intelligenz genutzt werden kann, um einzelne Nutzer über Bots mit Schadsoftware zu infizieren.[14] Dafür entwickelten sie ein Programm, das automatisch so etwas wie den perfekten Social Media-Freund für einen beliebigen Nutzer generiert. Das Programm analysiert die Nachrichten des Nutzers und versucht dann selbstständig Nachrichten zu generieren, die für diesen Nutzer von großem Interesse sind. Diese Nachrichten werden mit einem Link verbunden, der auf eine Internetseite mit Schadsoftware verweist. In Tests klickte die Hälfte der Testpersonen diesen Link tatsächlich an. Bei diesem Vorgehen handelt es sich um eine perfide Unterkategorie des so genannten Phishing: Im herkömmlichen Verfahren werden einfach massenhaft Nachrichten verbreitet, von denen man hofft, dass sie viele Leute interessieren („Sie haben gewonnen!", „Hallo, kennst du mich noch?" etc.). Dabei klicken aber in der Regel nicht einmal 5 % der Nutzer auf die verbreiteten Links. Das sogenannte Spear-Phishing passt die Nachrichten an die einzelnen Nutzer an und benutzt dafür Informationen, die aus den sozialen Netzwerken gesammelt werden. Dies nun über eine Software zu automatisieren und mit einem Botnetzwerk zu verbinden, also *Automated Spear Phishing*, bedeutet, dass im Zweifelsfall jeder von einem ganz persönlich auf ihn abgestimmten Bot angegriffen werden kann.

Darüber hinaus muss davon ausgegangen werden, dass der massive Einsatz von algorithmisch gesteuerten Fake Follower Accounts und die damit einhergehende, gelenkte Verbreitung von Inhalten in sozialen Netzwerken inzwischen zu einer außenpolitischen Strategie geworden ist: Seit 2011 wird darüber berichtet, dass die U.S. Air Force das sogenannte „persona management" entwickelt hat.[15] Dabei handelt es sich um eine Software, die es in kurzer Zeit ermöglicht, Massen von Social Bots zu erstellen und so zu tarnen, dass diese zum Beispiel Terrorzellen in sozialen Netzwerken infiltrieren können. Allerdings wäre diese Software ebenfalls in der Lage, andersartige Aufgaben zu übernehmen.[16]

Fake Follower Accounts gehören inzwischen auch zu einer außenpolitischen Strategie

## Was bringt die Zukunft?

Social Bots werden nicht mehr verschwinden. Zwar werden die Verfahren, um Bots aufzuspüren, immer besser, aber dasselbe trifft eben auch auf die Bots zu. Für beide Seiten gilt, dass neue Verfahren relativ schnell analysiert werden können und entsprechende Gegenmaßnahmen entwickelt werden. Insgesamt wird sich der Anteil der Bots an den sozialen Netzwerken daher vermutlich langfristig auf einem relativ hohen Niveau einpendeln.

Kurzfristig können aber immense Verwerfungen auftreten, insbesondere dann, wenn die Aktivitäten der Bots quantitativ plötzlich ansteigen oder es einen neuen Qualitätssprung bei der Bot-Technik gibt. Ersteres ist besonders in Bezug auf singuläre Ereignisse, wie Wahlen oder Krisensituationen bedenklich. Hier kann es sein, dass die Bots tatsächlich kurzzeitig sehr wirkmächtig werden, weil die Manipulation erst enttarnt wird, wenn das eigentliche Ereignis schon wieder vorbei ist. Ein Qualitätssprung bei den Bots zeichnet sich bereits sehr deutlich ab: Immer mehr hervorragende Entwicklungsumgebungen für Bereiche der künstlichen Intelligenz, in denen es um das Verständnis und die Generierung von Text geht (*natural language processing, natural language generation*) werden derzeit frei zugänglich gemacht, weil Konzerne wie Google, Facebook und IBM sich davon Entwicklungsschübe für ihre Technik erhoffen. Mit diesen Werkzeugen ausgestattet, arbeiten die Bot-Entwickler derzeit an einer neuen Generation von Bots, die für den normalen Nutzer nicht mehr zu enttarnen sein wird.

Gleichzeitig führt das ökonomische Interesse an der Nutzung von Bots aber auch zu einer radikalen Veränderung der Spielregeln. Denn Bots werden sozusagen legalisiert: Sie sind nicht mehr die manipulative Bedrohung, sondern eher die helfenden Assistenten im Alltag. Dies geht häufig mit einer Kennzeichnung der Bots (wie z. B. in den Netzwerken Slack und Telegram) einher. Zwar lässt sich auch die Vorgabe, dass sich Bots zu erkennen geben müssen, umgehen. Der Anreiz dafür dürfte aber wesentlich geringer sein als momentan, wo Bots automatisch in einer Grauzone agieren. Außerdem führt die legale Verbreitung von Bots vermutlich auch zu einem anderen Bewusstsein bei den Nutzern: Wenn man im Alltag mit Bots interagiert, dann verschwindet auch der Überraschungseffekt und es wird häufiger in Frage gestellt werden, ob sich hinter einer Nachricht ein Mensch oder eine Maschine verbirgt. Insgesamt ist die Entwicklung in den sozialen Medien in vielen Bereichen so schnell und disruptiv, dass wir alle den Umgang mit diesem Instrument ständig neu lernen müssen. Am Beispiel Bots zeigt sich, dass durch die Digitalisierung eine Grundweisheit außer Kraft gesetzt wird, die bisher nahezu immer gegolten hat: Quantität ist letzten Endes ein Indiz für Qualität. Das stimmt heute nicht mehr, da auch eine Nachricht, die millionenfach verbreitet wird, absolut unwahr sein kann.

Für das Internet gilt der neue Grundsatz: Quantität ist kein Indiz für Qualität

Wichtig ist nun, dass sich sowohl der Nutzer, als auch die politischen Akteure schnell für diese Form der Kommunikation und des Agenda Settings sensibilisieren und einen adäquaten Umgang damit finden. Die große Herausforderung wird sein, zu analysieren, wie der Nutzer Bots besser erkennen kann und hierbei die digitale Medienkompetenz gesellschaftspolitisch eine noch größere Bedeutung erlangt.

1| *Clarke, Roger 1994. The Digital Persona and its Application to Data Surveillance. In: The Information Society, S.77-92, hier S. 68f.: „In extreme cases, an active agent may be capable of autonomous behavior. It may be unrecallable by its originators (as was the case with the Cornell worm). It may, by accident or design, very difficult to trace to its originator."*

2| *Boshmaf, Yzan, Ildar Muslukhof, Konstantin Beznosov, Matei Pipeanu 2013. Design and analysis of a social botnet. In: Computer Networks 57, S.556-578, hier S.556: „This is achieved by either simply mimicking the actions of a real OSN [Abkürzung für Online Social Network, Anm. d. Verf.] user or by simulating such a user using artificial intelligence, just as in social robotics."*

3| *Hegelich, Simon/Shahrezaye, Morteza 2015. The Communication Behavior of German MPs on Twitter. Preaching to the Converted and Attacking Opponents. In: European Policy Analysis 1.*

4| *U.a. Jungherr, Andreas/ Schoen, Harald/ Güldenzopf, Ralf 2016. Twitter als politische Informationsquelle. In: Konrad- Adenauer-Stiftung – Schlaglicht, www.kas.de/politischekommunikation.*

5| *„distributed denial of service"*

6| *Beckler, Ryan 2015. Which Presidential Candidates Have The Most Fake Twitter Followers? Four months ago, Donald Trump had the best real-to-fake Twitter follower ratio. What happened?. Online: http://www.vocativ.com/239402/which-presidential-candidates-have-the-most-fake-twitter-followers/. Zugegriffen: 05.07.2016: „Most interestingly though, is the fact that the 'real' proportion of Donald Trump's 4.43 million followers plummeted from 90 percent to 61 percent in just four months."*

7| *Considine, Austin 2012. Buying Their Way to Twitter Fame. Online: http://www.nytimes.com/2012/08/23/fashion/twitter-followers-for-sale.html. Zugegriffen: 05.07.2016.*

8| *Schuppisser, Raffael 2016. Die Märchen der Roboter. Auf Facebook und twitter verbreiten Maschinen Hassbotschaften und Falschmeldungen. Wir werden von ihnen manipuliert, ohne es zu merken. Denn Roboter tarnen sich als Menschen – auch in den US- Wahlen. In: Schweiz am Sonntag, S.46-47.*

9| *Squires, Nick 2012. Human or 'bot'? Doubts over Italian comic Beppe Grillo's Twitter followers. A bearded comic who has been hailed as a powerful new force in Italian politics faces claims that more than half his followers on Twitter simply do not exist. Online: http://www.telegraph.co.uk/technology/twitter/9421072/Human-or-bot-Doubts-over-Italian-comic-Beppe-Grillos-Twitter-followers.html. Zugegriffen: 05.07.2016.*

10| *Lüfkens, Matthias 2015. Twiplomacy Study 2015. Zugegegriffen: 05.07.2016.*

11| *Cresci, Stefano/ Di Pietro, Roberto/ Petrocchi, Martinella/ Spognardi, Angelo/ Tesconi, Maurizio 2015. Fame for sale: efficient detection of fake Twitter followers. In: Decision Support Systems 80, S.56-71, hier S.58: „At a first glance, acquiring fake followers could seem a practice limited to foster one's vanity—a maybe questionable, but harmless practice. However, artificially inflating the number of followers can also be finalized to make an account more trustworthy and influential, in order to stand from the crowd and to attract other genuine followers. Recently, banks and financial institutions in U.S. have started to analyze Twitter and Facebook accounts of loan applicants, before actually granting the loan. Thus, to have a "popular" profile can definitely help to augment the creditworthiness of the applicant."*

12| *Howard, Philip/ Bence, Kollanyi 2016. Bots, #StrongerIn, an #Brexit: Computational Propaganda during the UK-EU Referendum. In: Comprop, Research Note 2016 1*

13| *Hegelich, Simon 2015. Are social Bots on Twitter Political Actors? Empirical Evidence from a Ukrainian/ Russian Social Botnet. MPSA annual conference 2015 ; Hegelich, Simon 2016. Decision Trees and Random Forests. Machine Learning Techniques to Classify Rare Events. In: European Policy Analysis 2.*

14| *Seymour, John und Tully, Philip 2016. Weaponizing Data Science for Social Engineering: Automated E2E Spear Phishing on Twitter.Online: https://www.blackhat.com/docs/us-16/materials/us-16-Seymour-Tully-Weaponizing-Data-Science-For-Social-Engineering-Automated-E2E-Spear-Phishing-On-Twitter.pdf. Zugriff: 30.08.2016.*

15| *Gehl, Robert W. 2013. The Computerized Socialbot Turing Test. New Technologies of Noopower. In: SSRN Electronic Journal.; Webster, Stephen 2011. Exclusive: Military's 'persona' software cost millions, used for 'classified social media activities'. Online: http://www.rawstory.com/2011/02/exclusive-militarys-persona-software-cost-millions-used-for-classified-social-media-activities/. Zugegriffen: 05.07.2016.*

16| *Finger, Lutz/ Dutta, Soumitra 2014. Ask, measure, learn. Using social media analytics to understand and influence customer behavior. Beijing: O'Reilly, hier S.173: „While the planned applications for this software are classified, such tools would enable virtual people to be placed strategically in locations around the world, to influence the public opinion in ways that would benefit the US government."*

## LITERATUR


- *Barberá, Pablo. 2015. Birds of the Same Feather Tweet Together. Bayesian Ideal Point Estimation Using Twitter Data. Political Analysis 23: 76–91. doi: 10.1093/pan/mpu011.*

- *Hegelich, Simon. 2016b. Social Botnets auf Twitter - Der Fall Ukraine. In Media Bias im Internet // Media Bias im Internet - Tendenzfreiheit und Vielfalt von Medien(inhalten). Tendenzfreiheit und Vielfalt von Medien(inhalten) // Gemeinsame Vortragsveranstaltung der Institute für Rundfunkrecht an der Universität zu Köln und Rundfunkökonomie der Universität zu Köln vom 19. Juni 2015, Hrsg. Institut für Rundfunkrecht an der Universität zu Köln, und Roland Bornemann, 127–136. München: C.H. Beck; Verlag C. H. Beck*


### Der Autor

*Prof. Dr. Simon Hegelich, Hochschule für Politik an der Technischen Universität München*

*Prof. Hegelich (*1976) verbindet in seiner Forschung Politikwissenschaft und Computerwissenschaft zu Political Data Science. Dabei geht es sowohl um Themen der Digitalisierung, deren politische Relevanz untersucht wird, als auch um klassische politikwissenschaftliche Fragen, die mit Methoden wie maschinellem Lernen, Data Mining, Computer Vision oder Simulationen bearbeitet werden. Simon Hegelich hat an der Universität Münster Politikwissenschaft studiert und dort seine Promotion und Habilitation abgeschlossen. Von 2011 bis 2016 leitete er als Geschäftsführer das interdisziplinäre Forschungskolleg FoKoS der Universität Siegen. Seit 2016 ist Simon Hegelich Professor für Political Data Science an der Hochschule für Politik an der Technischen Universität München.*



**Konrad-Adenauer-Stiftung e. V.**

*Ansprechpartner:*
**Daphne Wolter**
*Koordinatorin Medienpolitik*
*Hauptabteilung Politik und Beratung*
*Telefon: +49(0)30/26996-3607*
*E-Mail: daphne.wolter@kas.de*

*Postanschrift: Konrad-Adenauer-Stiftung, 10907 Berlin*

*ISBN 978-3-95721-238-2*