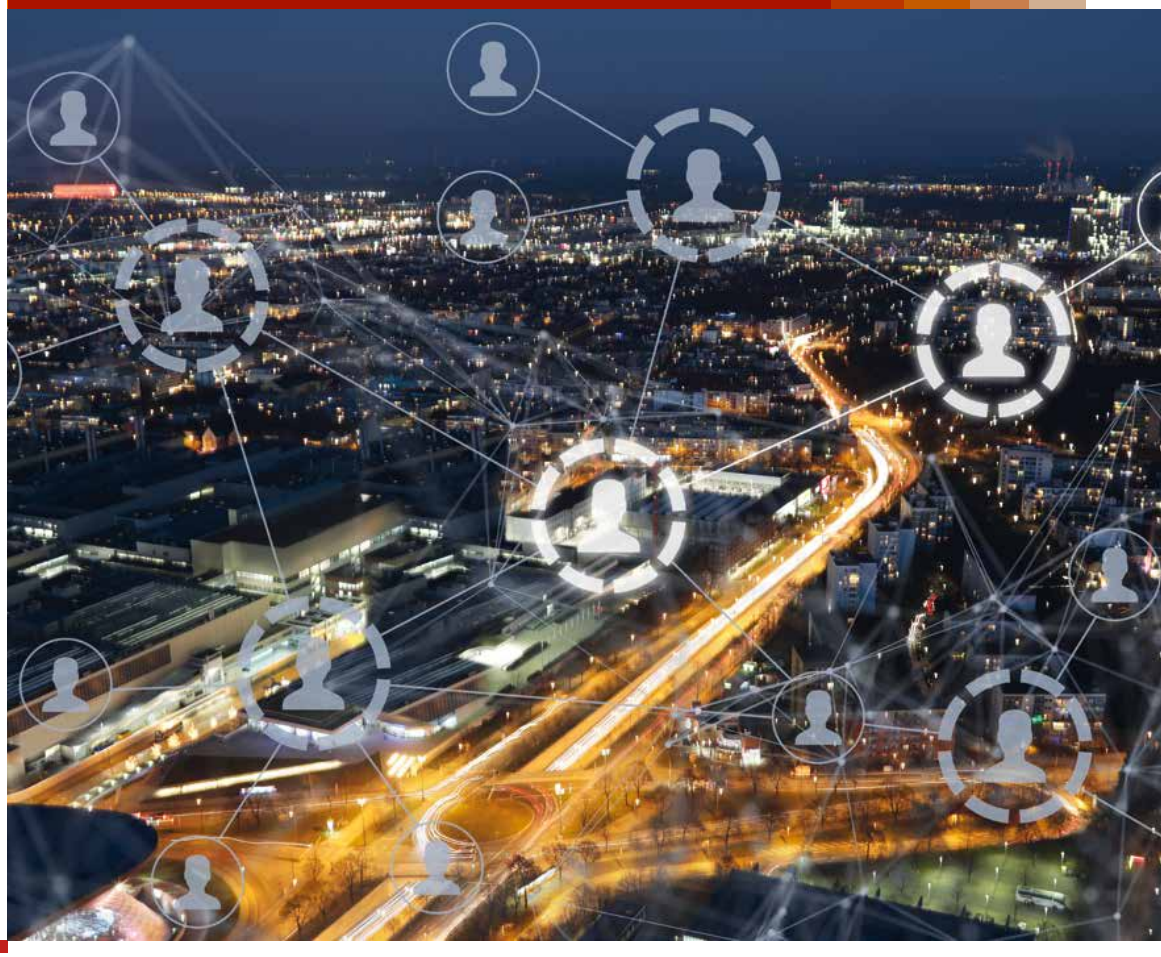
www.pwc.de
www.pwclegal.de

# *Social Bots: Gefahr für die Demokratie?*

*Whitepaper mit Handlungsempfehlungen für Unternehmen, Medien und Politik.*

*August 2017*



pwc

# *Social Bots: Gefahr für die Demokratie?*

*Whitepaper mit Handlungsempfehlungen für Unternehmen, Medien und Politik.*

*August 2017*

pwc

**Social Bots: Gefahr für die Demokratie?**

Herausgegeben von der PricewaterhouseCoopers GmbH Wirtschaftsprüfungsgesellschaft (PwC)

August 2017, 36 Seiten, 11 Abbildungen, Softcover

# Inhaltsverzeichnis

# Abbildungsverzeichnis

# Vorwort

Als eine Jury von Sprachexperten jüngst über den Anglizismus des Jahres 2016 zu entscheiden hatte, fiel die Wahl wenig überraschend – und noch vor „Darknet“ und „Hate Speech“ – auf „Fake News“. Tatsächlich hat sich selten zuvor ein englischstämmiger Begriff derart rasch in der deutschen Sprache etabliert wie dieser. Das lag zum einen natürlich an der prominenten Rolle, die dem Phänomen während des US-Präsidentschaftswahlkampfs zugeschrieben wurde. Es dürfte zum anderen aber auch damit zu tun haben, dass es für Fake News im Deutschen keine echte Entsprechung gibt. Begriffe wie „Propaganda“ oder „Desinformation“ zielen zwar in eine ähnliche Richtung, haben jedoch nicht dieselbe Bedeutung. „Falschmeldung“ wäre zwar eine naheliegende Übersetzung, allerdings schwingt bei diesem Wort nicht zwingend mit, was ganz entscheidend das Wesen von Fake News ausmacht: Es geht um Falschmeldungen (früher sagte man auch „Enten“), die nicht irrtümlich, sondern bewusst verbreitet werden, mit dem Ziel, die öffentliche Meinung zu manipulieren.

Neben dieser intentionalen Verbreitung lässt sich noch ein zweites Merkmal definieren, das Fake News von klassischen Falschmeldungen unterscheidet, nämlich, dass es sich bei Fake News um eine Erscheinung des Internetzeitalters oder, genauer noch, der Social-Media-Ära handelt. Das heißt natürlich nicht, dass es analoge Formen der Fake News nicht zu allen Zeiten gegeben hätte. Schon im alten Rom versuchten Octavian und Marcus Antonius, sich gegenseitig durch das Streuen von Lügengeschichten zu diskreditieren. Und spätestens mit der Erfindung des Buchdrucks wurden Fake News zu einem immer machtvolleren Mittel der Meinungsmanipulation. Als eines der bekanntesten Beispiele gelten die reißerischen und teils wohl auch falschen Berichte, mit denen die Regenbogenpresse in den USA den spanisch-amerikanischen Krieg 1898 heraufbeschwor.

Dennoch wäre es falsch, so zu tun, als wären Fake News, wie sie speziell das vergangene Jahr geprägt haben, ein längst bekanntes Phänomen. War die großflächige Beeinflussung der öffentlichen Meinung bislang den Massenmedien oder Regierungen (in autokratischen Ländern mit entsprechendem Zugriff auf Fernsehen und Radio) vorbehalten, steht diese Möglichkeit in Zeiten von Facebook, Twitter und Instagram theoretisch jedem zur Verfügung. Dies gilt umso mehr – und darin liegt eine neue Qualität –, als hinter der Verbreitung falscher Nachrichten nicht mehr unbedingt Menschen stehen müssen. Stattdessen wird die Meinungsschlacht in den sozialen Medien inzwischen zu einem (zumindest quantitativ) beträchtlichen Teil von sogenannten Social Bots geführt. Das sind automatisierte Programme, die sich zum Beispiel bei Twitter als echte Menschen ausgeben und versuchen, die dort geführten Debatten durch Likes, Tweets oder Retweets in die von ihren Urhebern gewünschte Richtung zu lenken.

In größerem Ausmaß traten Social Bots erstmals während des Arabischen Frühlings in Erscheinung. Danach spielten sie auch in der Ukrainekrise, bei der Brexit-Entscheidung und vor allem bei der US-Präsidentenwahl eine Rolle. So soll der Anteil echter Twitter-Follower sowohl beim republikanischen Kandidaten Donald

Trump als auch bei der demokratischen Bewerberin Hillary Clinton zeitweise gerade einmal bei 60 % gelegen haben.[1] Das US-Magazin Wired berichtete zudem, dass mitunter 50 bis 55 % der Clintonschen Twitter-Aktivität (also bei den Likes, Follows oder Retweets, die sie über die Plattform erhielt) von Social Bots gestammt hätten. Bei Trump seien es bisweilen sogar 80 % gewesen.[2]

Nun sind die hohen quantitativen Werte noch kein Beleg dafür, dass Social Bots die US-Wahl entscheidend beeinflusst hätten – schließlich kommt es ja in einem Meinungsbildungsprozess auch und vor allem auf die Qualität der Beiträge an. Trotzdem haben wir es bei Social Bots als Urhebern und Multiplikatoren mutmaßlicher Fake News inzwischen mit einem signifikanten Phänomen zu tun, dem durch die weitere Verfeinerung von Big-Data- oder Artificial-Intelligence-Technologien in den kommenden Jahren eine nochmals wachsende Bedeutung zukommen könnte.

Als Nischenphänomen lassen sich die neuen Formen der Meinungsmache jedenfalls nicht mehr abtun. Wie aus einer aktuellen PwC-Umfrage hervorgeht, glaubt inzwischen jeder zweite Bundesbürger, über Fake News „relativ gut Bescheid zu wissen“. Weitere 34 Prozent meinen, sie wüssten zumindest „ungefähr, was sich dahinter verbirgt“. Der Bekanntheitsgrad von Social Bots ist zwar deutlich geringer, allerdings auch nicht zu vernachlässigen: 14 Prozent sagten, sie wüssten darüber „relativ gut Bescheid“, 22 Prozent geben an, dass sie „ungefähr wissen, was sich dahinter verbirgt“. Aus derselben Umfrage geht zudem hervor, dass 68 Prozent der Deutschen Plattformbetreiber wie Facebook oder Twitter verpflichten wollen, Fake News auf ihren Kanälen grundsätzlich zu löschen. Bei Social Bots wiederum befürworten 90 Prozent eine stärkere Reglementierung – und sogar 43 Prozent ein gesetzliches Verbot.

Ob solche Mittel tatsächlich geeignet sind, Meinungsmache im Internet zu bekämpfen – darüber lässt sich sicherlich streiten. Zweifelsohne allerdings stellen sich eine Reihe von Fragen: Wie lassen sich Social Bots identifizieren? Welche Risiken, aber womöglich auch Chancen bergen sie – und zwar nicht nur für politische Institutionen, sondern auch für Unternehmen? Welche Rolle werden sie bei der bevorstehenden Bundestagswahl spielen? Und vor allem: Wie kann man sich vor den Gefahren durch Social Bots wirksam schützen?

Das vorliegende Whitepaper soll Ihnen, liebe Leserinnen und Leser, erste Antworten auf diese Fragen geben und einen Diskussions- und Debattenbeitrag sein. Ich wünsche Ihnen eine aufschlussreiche Lektüre!

***Werner Ballhaus***
Leiter Technologie, Medien und Telekommunikation

[1] Vgl. S. Hegelich, „Invasion der Meinungs-Roboter“, Analysen und Argumente, Nr. 221, 2016.
[2] Vgl. D. Alba, „The Political Twitter Bots Will Rage This Election Day“, Wired.com, 2016.

# A Was sind Social Bots?

Social Bots sind Computerprogramme, die in sozialen Medien in automatisierter Form Nachrichten oder Meinungen verbreiten – zum Beispiel durch Likes, Tweets oder Retweets bei Diensten wie Twitter. Dabei wird der Eindruck erweckt, hinter den entsprechenden Social-Media-Profilen stünden reale Menschen. Tatsächlich sind es aber Maschinen, die von ihren Betreibern gezielt eingesetzt werden, um die öffentliche Meinung zu manipulieren.

Diese Definition ist nicht neutral. Denn das Wort „manipulieren" ist negativ konnotiert und deutet an, dass hinter dem Einsatz von Social Bots generell schlechte Absichten stehen. Ob das im Einzelfall immer zutrifft, wird zu überprüfen sein – und ist in letzter Konsequenz natürlich auch eine Frage des Standpunkts. Was man allerdings festhalten kann: Der irreführende Charakter von Social Bots (sie geben vor, jemand zu sein, der sie nicht sind) widerspricht den Gepflogenheiten des demokratischen Diskurses. Wir gehen in diesem Whitepaper deshalb grundsätzlich davon aus, dass die Motive der Betreiber von Social Bots kritisch zu betrachten sind.

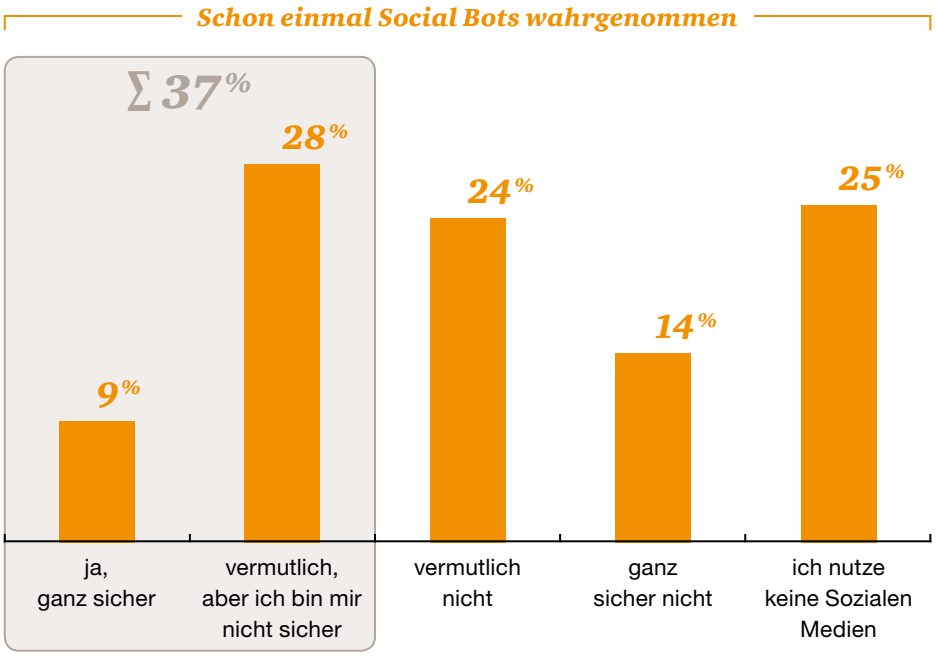
Gleichwohl – so viel schon vorweg – werden wir im weiteren Verlauf auch der Frage nachgehen, ob es sozusagen „gute" Social Bots geben kann. Womit wiederum die Frage verbunden ist, ob Social Bots ihr wahres Wesen zwingend verschleiern müssen. Denn warum sollen sich die Urheber nicht wie die artverwandten Chatbots (zum Unterschied zwischen beiden Begriffen siehe Abb. 1) offen zu erkennen geben? Daran knüpft sich eine weitere Frage an: Sind Social Bots für politische oder wirtschaftliche Institutionen nur ein Abwehrthema (Wie kann ich mich schützen?) – oder werden sich in den kommenden Jahren auch legitime Möglichkeiten ergeben, Social Bots selbst zu nutzen?

**Abb. 1 Wahrnehmung von Social Bots**

Fast vier von zehn Deutschen haben bereits Social Bots wahrgenommen.

Haben Sie in letzter Zeit schon einmal Beiträge von derartigen Social Bots zu politischen Themen in sozialen Netzwerken wahrgenommen?

Basis: Alle Befragten (Einfachnennung), n = 1.000



Rein technisch sind die Meinungsroboter relativ leicht zu kreieren und praktisch beliebig vermehrbar. Voraussetzung für die Erstellung sind Nutzer-Accounts, die in den entsprechenden sozialen Netzwerken bereits registriert sind. Sie werden auf dem Schwarzmarkt inzwischen in großen Stückzahlen gehandelt. So kosten 1.000 falsche Accounts laut dem Data-Science-Experten Simon Hegelich von der TU München zwischen 45 US-Dollar (für einfache Twitter-Konten) und 150 US-Dollar (für „gealterte" Facebook-Konten).[3] Die Anbieter solcher Account-Sammlungen sitzen vor allem in Russland.

Darüber hinaus benötigen die Betreiber ein Algorithmus-basiertes Programm, das den Social Bot steuert. Die letzte Hürde ist schließlich die Programmierschnittstelle, kurz API, die Betreiber von sozialen Netzwerken externen Entwicklern kostenlos zur Verfügung stellen, um die eigene Plattform erweiterbar zu machen. Diese APIs sind es, die auch dem Social-Bot-Account den Zugang zum Netzwerk ermöglichen. Als besonders roboterfreundlich gelten die APIs von Twitter – was auch ein Grund dafür ist, dass Social Bots auf Twitter deutlich stärker verbreitet sind als auf anderen Plattformen.

Die Qualität der Meinungsroboter ist sehr unterschiedlich. Simpel programmierte Bots beschränken sich in erster Linie auf die Streuung bereits vorformulierter Mitteilungen. Es gibt aber auch Bots, die mit anderen, auch echten, Nutzern kommunizieren und in der Lage sind, eigenständig immer wieder neue Nachrichten zu generieren. Insgesamt haben sich die Social Bots in den vergangenen Jahren stark weiterentwickelt. Dadurch – und aufgrund ihrer schieren Masse – wird es immer schwieriger, die automatisierten von den realen Accounts zu unterscheiden. Angesichts der rasanten Fortschritte im Bereich der künstlichen Intelligenz dürften Social Bots ihre kommunikativen Fähigkeiten in den kommenden Jahren weiter verbessern.

## *Worin unterscheiden sich Bots, Botnets, Chatbots und Social Bots?*

„Bot" ist eine Kurzform von Roboter. Ursprünglich wurde der Begriff vor allem für Computer verwendet, die von einer Schadsoftware befallen wurden und darum nun ein Eigenleben führen. Für eine Vielzahl untereinander verbundener Schadprogramme bürgerte sich deshalb auch die Bezeichnung „Botnet" ein.

Inzwischen wird der Begriff „Bot" tendenziell eher mit automatisierten Computerprogrammen bzw. Social-Media-Accounts assoziiert. Am bekanntesten sind Dialogsysteme, wie sie als sogenannte Chatbots von immer mehr Unternehmen in der Kundenkommunikation eingesetzt werden. Ein Beispiel ist Ikeas virtueller Assistent „Anna".

Zur Unterscheidung von Chatbots und Social Bots bieten sich die beiden folgenden Merkmale an:

1. Chatbots kommunizieren in der Regel reaktiv, während Social Bots auch selbst aktiv werden.
2. Chatbots lassen sich in der Regel einer Quelle zuordnen, während Social Bots ihre Urheberschaft zu verschleiern suchen.

[3] Vgl. Hegelich, 2016.

# B Wie lassen sich Social Bots identifizieren?

Bei einer Untersuchung der Universität Reading im Jahr 2014 konnten gut 30 % der Testpersonen den Chatbot „Eugene Goostman" – er imitiert die Persönlichkeit eines 13-jährigen Jungen – angeblich nicht von einem menschlichen Konversationspartner unterscheiden.[4] Das Ergebnis erlangte große Aufmerksamkeit. Es lässt sich allerdings auch andersherum lesen: Sieben von zehn Testpersonen, also die klare Mehrheit, erkannten den Roboter offenbar als das, was er ist, nämlich eine Maschine. Und: Bei vier anderen Bots schnitten die Testpersonen teils sogar deutlich besser ab.

Dieses Resultat deckt sich mit der Einschätzung von Experten, wonach ein geschulter Internetnutzer einen Chatbot oder Social Bot in aller Regel identifizieren kann. Wie überlegen die menschliche Intelligenz der künstlichen in dieser Hinsicht noch immer ist, zeigt auch der Irrlauf des Microsoft-Chatbots Tay im Frühjahr 2016. Den hatten menschliche Chatpartner mit ihren Fragen solange fehlgeleitet, bis der Roboter irgendwann – zum Entsetzen seiner Programmierer – sogar rassistische Bemerkungen von sich gab.[5]

Tatsächlich lassen sich die meisten Bots noch immer anhand einfacher Checklisten identifizieren: Formuliert er wirklich wie ein Mensch? Macht er auch mal eine Pause? Und warum hat sein Profil kein Foto? Geht es daher um einen einzigen Social Bot, der Fake News via Twitter oder Facebook verbreitet, dann sind Journalisten oder andere Profis in der Lage, diesen Täuschungsversuch zu enttarnen. Was aber, wenn es nicht mehr nur um einen, sondern um Abertausende von Social Bots geht, die versuchen, politische Debatten in bestimmte Richtungen zu lenken? Was, wenn die schiere Menge von frisierten Tweets, Retweets oder Likes dazu führt, dass die sogenannten Trending Topics – die viel beachteten Listen, die bei Twitter die aktuell meistdiskutieren Themen anzeigen – manipuliert werden? Ist die menschliche Intelligenz dann immer noch in der Lage, den Überblick zu behalten? Und was passiert, wenn die Urheber ihre Social Bots in den kommenden Jahren technisch weiter aufrüsten?

Fest steht, dass die Grenze zwischen eindeutig menschlichen und eindeutig maschinellen Verhaltensweisen undeutlicher wird. Dank steigender Rechnerkapazitäten können Social Bots auf immer größere Datenbestände zugreifen. Durch den kombinierten Einsatz von Big-Data- und Artificial-Intelligence-Technologien sind die in der Lage, humanoide Verhaltensmuster immer überzeugender nachzuahmen. Manche Meinungsroboter werden inzwischen so programmiert, dass ihre Accounts ähnliche Aktivitätskurven aufweisen wie die Social-Media-Profile menschlicher Nutzer, inklusive entsprechender Ruhephasen (die der Bot in Wirklichkeit gar nicht braucht). Inzwischen gibt es sogar Social Bots – sogenannte Cyborgs –, die zumindest partiell von Menschen unterstützt werden. Ihre Wirkung lässt sich noch verstärken, wenn sich die Cyborgs gehackter Profile einer authentischen Historie bedienen.

[4] Vgl. The Guardian, „Computer simulating 13-years-old boy becomes first to pass Turing test", Guardian.com, 2014.
[5] Vgl. E. Hunt, „Tay, Microsoft's AI chatbot, gets a crash course in racism from Twitter", Guardian.com, 2016.

Um Social Bots zuverlässig zu identifizieren, wird es auch in Zukunft auf das menschliche Urteilsvermögen ankommen. Daneben gilt es aber – ebenfalls auf Basis von Big Data und künstlicher Intelligenz – technische Lösungen zu entwickeln, die den Meinungsrobotern auch im großen Umfang gewachsen sind. Ein bereits existierendes Tool ist die Web-API BotOrNot für Twitter (inzwischen Botometer genannt; siehe dazu Kapitel H). Bei Tests kam sie auf eine Treffsicherheit von rund 95 %.[6]

Trotz solcher Erfolge steht die Entwicklung von Anti-Bot-Technologien allerdings noch am Anfang. Zudem gilt für die Social-Bot-Enttarnung, was analog zum Beispiel auch für Anti-Virus-Programme gilt: Um einen Bot zu bekämpfen, muss man ihn erst einmal kennen. Diese Regel impliziert, dass die Entwickler von Meinungsrobotern den Entwicklern von Identifikationstools notwendigerweise immer mindestens einen Schritt voraus sein werden. Was Unternehmen und politische Institutionen tun können, um sich dennoch gegen Social Bots zu schützen, werden wir in Kapitel G ausführlicher diskutieren. Zuvor werden Professor Dr. Jens Lehmann, Lead Scientist am Fraunhofer-Institut für Intelligente Analyse- und Informationssysteme (IAIS), und seine Kollegin Klaudia Thellmann die technologischen Hintergründe von Social Bots in einem Gastbeitrag erklären.

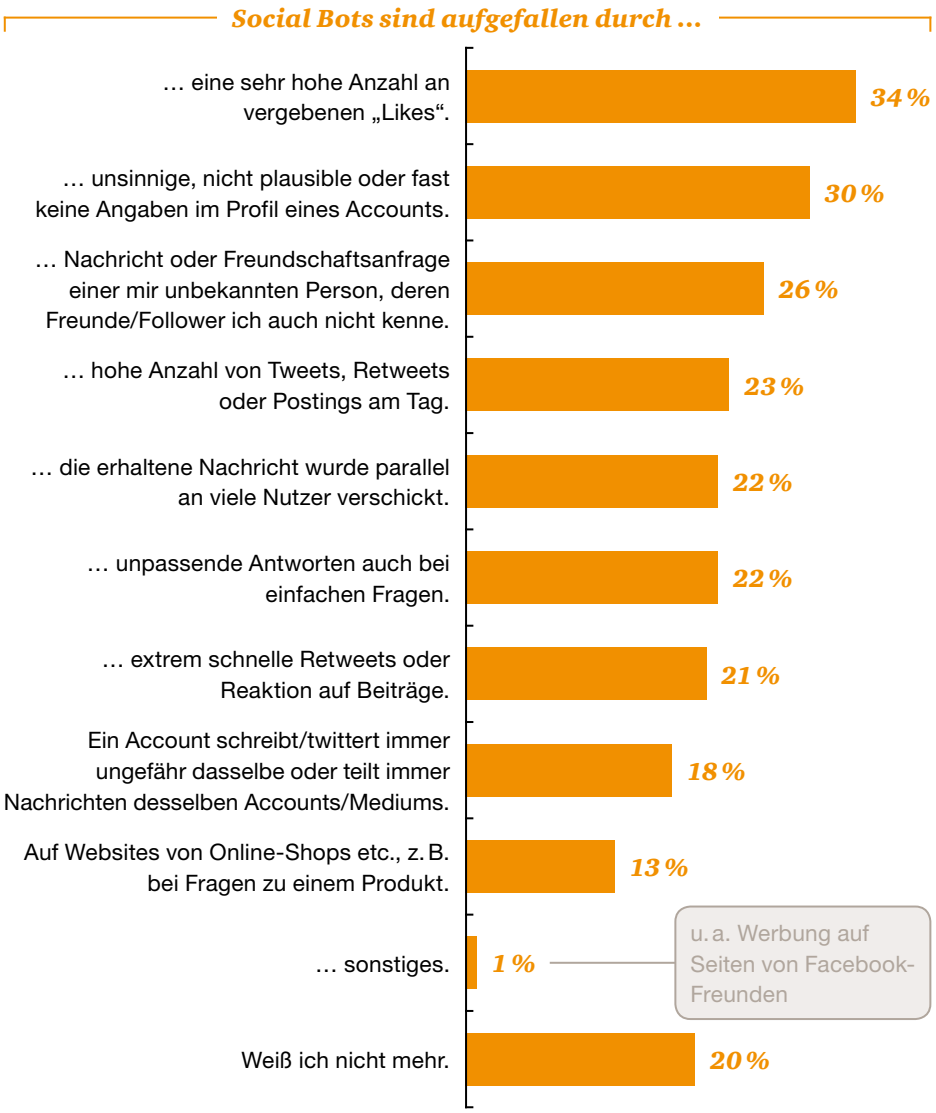
**Abb. 2 Erkennen von Social Bots**

Social Bots wurden vor allem wegen ihrer vielen vergebenen „Likes“ und ihres verdächtigen Profils „enttarnt“.

Wie sind Ihnen die Social Bots aufgefallen?

Mehrfachnennung waren möglich

Basis: Befragte, die Social Bots wahrgenommen haben, n = 371




[6] Vgl. E. Ferrara et al., „The Rise of Social Bots“, Communications of the ACM, Bd. 59 Nr. 7, S. 96–104, 2016.

# C Gastbeitrag: Zum technischen Hintergrund von Social Bots

***Von Prof. Dr. Jens Lehmann und Klaudia Thellmann, Fraunhofer IAIS.***

Die technische Komplexität von Chatbots reicht von einfachen Bots, die anhand einer Heuristik bestimmte Muster in einer Nachricht erkennen und darauf mit einer entsprechenden vorgefertigten Antwort reagieren, bis hin zu solchen, die auf Grundlage erlernter Modelle selbstständig Antworten generieren.[7] Dabei werden Dialogsysteme, die auf eine Reihe von präparierten Antworten zurückgreifen, als Retrieval-basiert bezeichnet. Systeme, die ohne ein solches Korpus von präparierten Antworten auskommen, heißen generative Systeme.

***Retrieval-basierte Dialogsysteme***

Retrieval-basierte Systeme verwenden zur Auswahl der passenden Antwort auf eine Benutzereingabe Regeln, die dazu dienen, Muster in der Eingabe zu erkennen. Diese Systeme liefern vorhersehbare, grammatikalisch korrekte Antworten. Sie sind einfach zu programmieren, da es bereits zahlreiche Bibliotheken mit Regeln gibt. Im Gegensatz zu den generativen Systemen sind sie aber bei nicht vorgesehenen Eingaben weniger flexibel.

Der erste wissenschaftlich beschriebene Chatbot nannte sich Eliza. Er wurde bereits 1966 von dem deutsch-amerikanischen Informatiker Joseph Weizenbaum entwickelt.[8] Eliza war Retrieval-basiert und baute auf einfachen Regeln zur Erkennung von Mustern in Eingaben auf. Der Bot war vor allem darauf ausgelegt, Aussagen geschickt in Rückfragen umzuwandeln. Dadurch konnte trotz einfacher Mittel eine kontinuierliche Konversation stattfinden.

Zur Erstellung von Retrieval-basierten Chatbots führte der US-Informatiker Richard Wallace in den 90er Jahren die Chatbot-Sprache AIML (Artificial Intelligence Markup Language) ein. Auf ihrer Grundlage wurde der Chatbot ALICE[9] programmiert, mit dem Wallace mehrmals den Loebner-Preis für die menschenähnlichste Dialogführung erhielt (siehe Abb. 3).

**Abb. 3 AIML-Regeln für Chatbot ALICE**

```
<category>
  <pattern>WHAT IS YOUR NAME</pattern>
  <template>
    My name is
    <bot name="name"/>
    .
  </template>
</category>
```

Quelle: ALICE.

*Der erste wissenschaftlich beschriebene Chatbot nannte sich Eliza.*

[7] M. L. Mauldin, „Chatterbots, tinymuds, and the turing test: Entering the Loebner prize competition“, AAAI, Bd. 94, 1994.
[8] D. Britz, „Deep Learning for Chatbots“, WILDML, www.wildml.com/2016/04/, 2016.
[9] L. Bradesko und D. Mladenic, „A survey of chatbot systems through a loebner prize competition“, Proceedings of Slovenian Language Technologies Society Eighth Conference of Language Technologies, 2012.

AIML besteht im Grunde aus einer Ansammlung von in Kategorien gruppierten Mustern mit entsprechenden vorformulierten Antworten. Die Muster decken jeweils eine oder auch mehrere mögliche Benutzereingaben ab, auf die der Chatbot mit einer vorgegebenen Antwort reagiert.

**Abb. 4 Dialogausschnitt Chatbot ALICE[1]**

*Human:* ***What is your name?***
**ALICE: My name is Alice.**
*Human:* ***Are you evil?***
**ALICE: No. I try to be good, but at worst I'm harmless.**
*Human:* ***Are you harmless?***
**ALICE: I don't know whether or not I am harmless. I am a Homo Sapiens.**

You say:

Say

[1] ALICE: http://alice.pandorabots.com/.

Quelle: ALICE.

Eine weitere regelbasierte Chatbot-Sprache mit einer ausgereifteren Umsetzung für das Pattern-Matching und die Kontexterkennung ist das 2011 von Bruce Wilcox – einem auf künstliche Intelligenz spezialisierten Programmierer – veröffentlichte ChatScript. Auf dieser Sprache basieren auch die Chatbots Suzette und Rosette, mit denen Wilcox 2010 und 2011 den Loebner-Preis gewann.

Im Unterschied zu AIML setzt das Programm ChatScript Textanalyse-techniken (Techniken des neuro-linguistischen Programmierens) zum Verarbeiten der Eingabe ein. So etwa erkennt es Wortarten (POS-Tagging) und Synonyme. Darüber hinaus ist ChatScript zustandsbehaftet, das heißt, es kann sich Gesprächsverläufe merken.

**Abb. 5 ChatScript-Regeln und Konzepte für Chatbot Rose**

```
#!CONCEPTS
concept:~like[adore admire love]
concept:~meat[bacon ham beef chicken]

#!RULE
?: MEAT ( << you ~like ~meat >>) I love bacon
```

Quelle: Rose.

Ähnlich wie bei AIML bestehen ChatScript-Regeln aus einem Muster für die Eingabe und einer Vorlage für die Antwort. Zusätzlich zu den Regeln unterstützt ChatScript Begriffshierarchien und Synonyme durch Definition von Konzepten (siehe Abb. 5).

**Abb. 6 Dialogausschnitt Chatbot Rose[1]**

*User:* ***What is your name?***
**Rose: My name is Rose.**
*User:* ***Are you evil?***
**Rose: Of course not.**
*User:* ***Are you harmless?***
**Rose: Absolutely.**
*User:* ***Why not?***
**Rose: I'd love to really dig down deep into all my thoughts about that, but it's really not appropriate right now.**

Name: User
Message:
Send Input

[1] Rose: http://brilligunderstanding.com/rosedemo.html.

Quelle: Rose.

Zum Finden von Synonymen, Unterbegriffen und Beziehungen zwischen Begriffen können maschinenauswertbare Wissensdatenbanken wie WordNet oder OpenCyc verwendet werden. WordNet enthält semantische und lexikalische Beziehungen zwischen den Wörtern der englischen Sprache. OpenCyce ermöglicht über die zugrunde liegende Ontologiesprache CycL logisches Schlussfolgern über Sachverhalte.[10]

Um eine Konversation menschlicher erscheinen zu lassen, werden darüber hinaus diverse Tricks wie etwa Tippfehler, die Simulation von Tastatureingaben, biografische Modelle oder Sprünge von einem Thema zum anderen eingesetzt.[10]

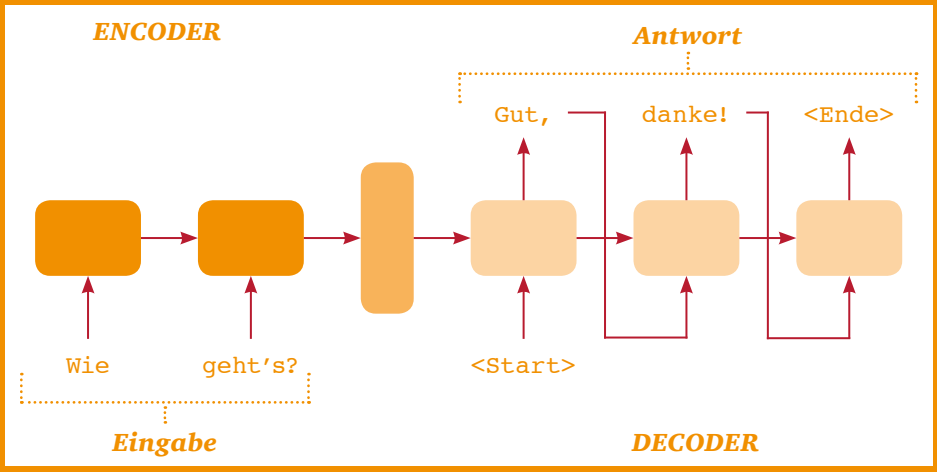
### *Generative Dialogsysteme*

Generative Systeme bauen häufig auf künstlichen neuronalen Netzen (KNN) auf.[11] Diese wurden in den vergangenen Jahren sehr erfolgreich in verschiedenen Bereichen der künstlichen Intelligenz eingesetzt, mit teilweise beeindruckenden Resultaten. Das Spektrum reicht von der Erkennung von Objekten auf Bildern über das autonome Fahren bis hin zur Identifizierung menschlicher Sprache und noch vielem mehr. Oft werden dabei Resultate erzielt, die Leistungen von Menschen nahekommen oder diese sogar übertreffen.

Für generative Dialogsysteme können neuronale Netze mit sogenannten Sequence-to-Sequence-Modellen eingesetzt werden. Eine Sequenz kann dabei eine nahezu beliebige Eingabe sein; zum Beispiel kann es sich bei der Eingabesequenz um einen deutschen Text und bei der Ausgabesequenz um einen englischen Text handeln. In diesem Fall würde das neuronale Netz lernen, Texte vom Deutschen ins Englische zu übersetzen. Damit dies gelingt, muss das neuronale Netz seine Fähigkeiten anhand einer Unmenge vorgegebener korrekter Beispiele trainieren. Ein Beispiel besteht dabei aus einer richtigen Übersetzung von einer Eingabesequenz in eine Ausgabesequenz. Dafür wären in diesem Fall Tausende von richtig übersetzten Texten aus Trainingsmaterial nötig.

[10] L. Bradesko und D. Mladenic, „A survey of chatbot systems through a loebner prize competition", Proceedings of Slovenian Language Technologies Society Eighth Conference of Language Technologies, 2012.
[11] O. Vinyals und V. L. Quoc, „A neural conversational model", arXiv preprint, 2015.

**Abb. 7 Sequence-to-Sequence Verarbeitung**




Das gleiche Prinzip lässt sich auch auf Dialogsysteme anwenden: In dem Fall ist die Eingabe der zuletzt gesprochene Dialogteil und die Ausgabe eine Antwort darauf. Ein derartiges neuronales Netz muss also mit Hunderttausenden von existierenden Dialogen trainiert werden. Interessant ist dabei, dass das neuronale Netz – vergleichbar mit einem neugeborenen Kind – ohne vorheriges Wissen erlernt, wie Sprache funktioniert und Dialoge geführt werden. Dabei passt es sich stark an die Trainingsdialoge an. Wenn man für das Training also Texte aus einer sozialen Netzwerkplattform wie Facebook verwendet, wird das Resultat völlig anders aussehen, als wenn man das Netzwerk mit Werken von Shakespeare trainiert. Das bedeutet natürlich auch, dass man die Trainingsbeispiele vorsichtig auswählen sollte. Kann ein System wie der bereits erwähnte Chatbot Tay (siehe dazu Kapitel B) unkontrolliert mit Beispielen „gefüttert" werden, dann lässt sich sein Verhalten manipulieren.

Der Vorteil von generativen Systemen ist, dass man die Zuordnung zwischen Eingabe und Antwort nicht durch Regeln abbilden muss, da das neuronale Netz diese Zusammenhänge selbstständig erlernt, wenn man ihm große Mengen an Trainingsdaten bietet. Nachteilig ist, dass die aktuellen Systeme oft noch sehr allgemeine Antworten erzeugen, etwa „OK" oder „Wie geht es Dir?", statt auf die individuelle Situation einzugehen. Zudem werden die neuronalen Netze durch die riesige Menge an benötigten Trainingsdaten oft mit Dialogen verschiedener Personen trainiert. Dadurch entsteht ein uneinheitliches Persönlichkeitsbild. Nach unserer Einschätzung wird die Forschung in diesem Bereich jedoch in den nächsten zehn Jahren große Fortschritte erzielen und in der Lage sein, beeindruckend menschenähnliche Chatbots zu entwickeln.

## *Turing-Test und Loebner-Preis*

Der Turing-Test ist benannt nach dem berühmten britischen Informatiker Alan Turing (1912–1954). Der Test soll ermitteln, ob eine Maschine dank künstlicher Intelligenz ein Denkvermögen entwickeln kann, das mit dem eines Menschen vergleichbar ist. Klassischerweise stellt in dem Test ein Mensch zwei Gesprächspartnern – einer ist ein Mensch, der andere eine Maschine – ohne Sicht- und Hörkontakt mittels einer Tastatur Fragen. Weiß er am Ende nicht, bei welchem seiner Konversationspartner es sich um den Menschen handelte, hat die Maschine den Test bestanden. Mit dem Loebner-Preis wird seit 1991 der Entwickler jener Maschine (bzw. jenes Chatbots) ausgezeichnet, die im Turing-Test das beste Ergebnis verzeichnet.

# D Welche Risiken bergen Social Bots?

Auch wenn Social Bots spätestens im Zuge der US-Präsidentschaftswahl zu einem viel beachteten Medienthema wurden, gibt es nur eine begrenzte Zahl von wissenschaftlich nachgewiesenen Fallbeispielen. Zu den am besten dokumentierten Fällen gehört der großflächige Einsatz von Meinungsrobotern während des Ukrainekonflikts im Jahr 2014. Dabei wiesen zwei deutsche Wissenschaftler, ausgehend von einer Analyse von abgesetzten Twitter-Beiträgen mit dem Hashtag #Ukraine, die Existenz eines mutmaßlich von ukrainischen Rechtsnationalisten gesteuerten Social-Bots-Netzwerks mit rund 15.000 aktiven Twitter-Accounts nach.[12]

Eine Untersuchung der insgesamt rund 60.000 versandten Tweets förderte aufschlussreiche Muster zutage. So ging es in den Beiträgen nicht nur um Politik, sondern die Bots „sprachen“ über populäre Themen wie Fußball, machten sexistische Witze und verbreiteten Links zum Download amerikanischer Kinofilme.[13] Damit zielten sie vermutlich auf den Geschmack der anvisierten Zielgruppe. Die rechte Propaganda, um die es den Urhebern des Netzwerks in Wirklichkeit ging, wurde in diese Konversationen sozusagen in homöopathischen Dosierungen eingestreut. Das gleiche galt für gezielte Falschinformationen wie die Behauptung, die Separatisten in der Ostukraine planten, russische Raketen auf die Hauptstadt Kiew zu richten.

Dabei folgten die Bots offensichtlich nicht nur stupiden Befehlen ihrer menschlichen „Botmaster“. Stattdessen sorgten hochkomplexe Algorithmen dafür, dass die Meinungsroboter einen „hohen Grad an Autonomie“ aufwiesen und lediglich abstrakten Regeln folgten, im Sinne von „Mache Dir einen populären Tweet zu eigen und versieh ihn mit den folgenden Hashtags“[14]. Aufgrund dieser Strategie wurde es für normale Nutzer extrem schwierig, die tatsächlichen Motive der Urheber zu erkennen.

[12] Vgl. S. Hegelich und D. Janetzko, „Are social bots on twitter political actors? Empirical evidence from a Ukrainian social botnet“, Tenth International AAAI Conference on Web and Social Media, 2016.
[13] Vgl. Hegelich, 2016.
[14] Vgl. Hegelich, Janetzko, 2016.

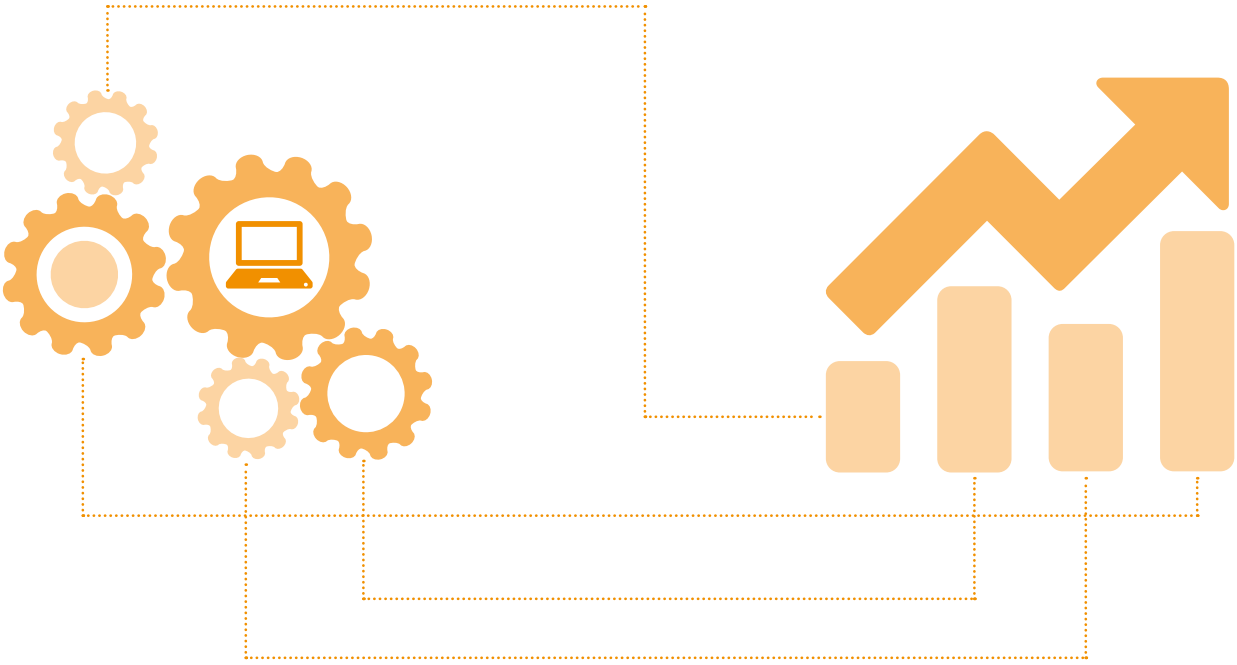
Aus diesem Beispiel und ähnlichen dokumentierten Fällen – unter anderem während der Brexit-Kampagne – lassen sich zumindest drei potenzielle Gefahren ableiten, die Social Bots für die demokratische Debattenkultur bergen:

- Durch die massenhafte Verbreitung von Fake News sind Social Bots in der Lage, gezielt „falsche Tatsachen" in Umlauf zu bringen, was vor allem in angespannten politischen Lagen potenziell dramatische Folgen haben kann.
- Durch die schiere Menge verbreiteter Beiträge können Social Bots die Trends in den sozialen Netzwerken manipulieren und so die öffentliche Meinung in eine bestimmte Richtung lenken.
- Mit ihren oftmals radikalen Positionen tragen Social Bots dazu bei, dass sich (menschliche) User aus politischen Debatten zurückziehen. Im Ergebnis betreiben die Meinungsroboter eine Verrohung des öffentlichen Diskurses.

Die potenziellen Gefahren durch Meinungsroboter sind allerdings nicht auf die politische Sphäre beschränkt. So ist denkbar, dass Social Bots eingesetzt werden, um Aktienkurse gezielt zu manipulieren. In der wissenschaftlichen Literatur wird in diesem Zusammenhang auf den mysteriösen Fall des Technologie-Start-ups Cynk aus dem USA verwiesen. Die Firma hatte zwar nur einen Mitarbeiter und erwirtschaftete keinerlei Umsätze, trotzdem stieg die Aktie im Jahr 2014 binnen weniger Wochen um rund 36.000 %, was Cynk zwischenzeitlich einen Börsenwert von rund sechs Milliarden Dollar bescherte (bevor die Aktie kurz danach zusammenbrach).[15] Auffällig ist hier, dass die Rallye des Wertpapiers mit vielen positiven Twitter-Kommentaren zusammenfiel. Eine Erklärung für den wundersamen Kursanstieg könnte deshalb darin bestehen, dass Handelsroboter die Aktie aufgrund der Twitter-Empfehlungen auch dann noch orderten, als menschliche Marktteilnehmer längst Verdacht schöpften.[16,17]

Wie real die Gefahr von Finanzmanipulation durch Social Bots tatsächlich ist, lässt sich vorerst zwar nicht mit Bestimmtheit sagen, das Bundeskriminalamt hat jedoch jüngst bereits zwei weitere Gefahrenszenarien benannt:[18]

- Die Schaffung künstlicher Märkte, um Anleger durch Bot-Kampagnen gezielt in beworbene (nicht existente) Kapitalanlagen zu treiben.
- Die Infiltrierung klassischer Vertriebs- und Beratungsmodelle durch von Social Bots verbreitete Falschnachrichten.



[15] Vgl. T. Alloway, T. Bradshaw, „Cynk sinks after 36.000 % climb", Financial Times, 2014.
[16] Vgl. E. Ferrara et al., „The Rise of Social Bots", Communications of the ACM, 2017.
[17] Vgl. M. Levine, „Cynk makes the case for buying friends", Naked Short Selling, Bloomberg, 2014.
[18] Vgl. S. Kind et al., Thesenpapier zum öffentlichen Fachgespräch „Social Bots – Diskussion und Validierung von Zwischenergebnissen" am 26. Januar 2017 im Deutschen Bundestag, 2017.

Daneben sind weitere Bereiche denkbar, in denen Social Bots in betrügerischer Absicht eingesetzt werden können – und wirtschaftliche oder sonstige Schäden anrichten. Ein relativ banales Beispiel ist der Fall der US-Datingplattform Ashley Madison. Dort verbargen sich hinter angeblich rund 70.000[19] Frauen in Wirklichkeit Bots, deren Aufgabe darin bestand, Männer in bezahlpflichtige Chats zu verwickeln. Weniger anschaulich, aber potenziell deutlich teurer sind sogenannte Spear-Phishing-Attacken, die sich nicht nur gegen Einzelpersonen, sondern mit dem Ziel der Infiltrierung auch gegen Unternehmen einsetzen lassen. Bei dieser Methode werden ausgewählte Mitarbeiter gezielt über soziale Netzwerke kontaktiert. Das Vorgehen ist vergleichbar mit Spammails – durch den Einsatz von Bots lassen sich die Nachrichten allerdings viel gezielter auf den Adressaten zuschneiden. Dadurch erhöht sich das Risiko, dass der Mitarbeiter auf den Angriff hereinfällt.

Solche „Speer-Attacken" sind nur ein Beispiel denkbarer Cyberwar-Aktivitäten. Es ist zumindest theoretisch möglich, über den Einsatz von Social Bots Schadsoftware zu verbreiten – bis hin zu sogenannten DDoS-Angriffen (DDoS: Distributed Denial of Service), bei denen mit Massenanfragen die Homepage des Unternehmens lahmgelegt wird. Dabei müssen die Cyberwarfare-Methoden gar nicht immer hochkomplex sein. Denn wenn Social Bots im politischen Kontext zur Meinungsmanipulation eingesetzt werden – warum dann nicht auch in der Wirtschaft? Das Risiko jedenfalls ist evident und potenziell extrem teuer, von der Streuung von Insolvenzgerüchten bis hin zu Rufmordkampagnen gegen handelnde Personen.

Wie Unternehmen auf die potenziellen Bedrohungen reagieren können, wird in Kapitel G erläutert. Zunächst wollen wir uns einer anderen Frage widmen: Bergen Social Bots neben Risiken nicht auch Chancen?

## *Social Bots und die Bundestagswahl*

Sind Bot-Kampagnen wie im Ukrainekonflikt auch im Zuge der Bundestagswahl denkbar? Die politischen Parteien sind jedenfalls sensibilisiert für das Thema – spätestens seitdem die AfD im Herbst 2016 heftig kritisiert wurde, nachdem ihr Vorstandsmitglied Alice Weidel in einem Interview erklärt hatte: „Selbstverständlich werden wir Social Bots in unsere Strategie im Bundestagswahlkampf einbeziehen."[20] Kurz darauf stellte die AfD klar, sie plane „keinen Einsatz sogenannter Social Bots im Wahlkampf". Bei einer Umfrage der Nachrichtenagentur Reuters betonten auch CDU, CSU, SPD, Grüne und FDP, im Wahlkampf keine Meinungsroboter zu verwenden.[21]

[19] Vgl. A. Newitz, „Ashley Madison code shows more women, and more bots", Gizmodo.com, 2015.
[20] Zeit Online, „AfD will Social Bots im Wahlkampf einsetzen", Zeit Online, 2016.
[21] Vgl. A. Rinke, „Sorge um gekaufte digitale Hilfe im Wahlkampf", Reuters, 2016.

# E Welche Chancen bieten Social Bots?

Nicht nur Parteien betonen, dass sie keine Social Bots einsetzen – auch aus der Unternehmenswelt sind bislang keine prominenten Fälle bekannt. Dabei braucht es eigentlich nicht viel Fantasie, um sich das theoretische Potenzial von Meinungsrobotern im Marketingbereich auszumalen. Ein gutes Beispiel hierfür ist der Fall Lajello.[22]

Unter diesem Namen tummelte sich vor ein paar Jahren ein Mitglied bei aNobii.com, einem sozialen Netzwerk, in dem sich Literaturfreunde über Bücher austauschen. Indem Lajello anderen Mitgliedern immer wieder Lesetipps gab, mutierte das Profil im Lauf der Zeit zum zweiteinflussreichsten User auf aNobii.com überhaupt. Doch bei Lajello handelte es sich nicht um einen Menschen, sondern um einen Social Bot. Hinter dem Fake-Profil stand eine Gruppe von Programmierern der Universität Turin. Sie betrachteten das Ganze lediglich als Experiment. Ein Literaturverlag hingegen könnte sich solch einen Bücher-Bot beispielsweise als Vertriebsinstrument zu Eigen machen.

Gleichwohl: Als irgendwann immer mehr Mitglieder den Verdacht äußerten, Lajello sei in Wirklichkeit eine Maschine, wurde das Profil vom Betreiber des Netzwerks gesperrt. Ganz abgesehen von den rechtlichen Fragen zeigte sich an diesem Punkt, warum Unternehmen beim Thema Social Bots aus gutem Grund zurückhaltend sind. Hätte hinter Lajello tatsächlich ein Verlag gestanden, wäre der Imageschaden vermutlich sehr viel größer gewesen als der Nutzen durch den Mehrverkauf von Büchern. Deshalb stellt sich die Frage: Sind Social Bots als Instrument für Unternehmen und andere seriöse Institutionen von vornherein diskreditiert?

*Auch viele Buchungsportale setzen inzwischen auf Chatbots.*

[22] Vgl. MIT Technology Review, „How a Simple Spambot Became the Second Most Powerful Member of an Italien Social Network“, MIT Technology Review, 2014.

So einfach kann man das nicht sagen. Denn wie bereits erläutert, handelt es sich bei Social Bots technisch betrachtet lediglich um eine Spielart der Chatbots. Wenn man von Social Bots als Meinungsrobotern spricht, lassen sich Chatbots analog als Kommunikationsroboter bezeichnen. Letztere indes werden inzwischen von vielen Unternehmen verwendet – eine Entwicklung, die enorm beschleunigt wurde dadurch, dass Facebook seine Messenger-App im vergangenen Jahr für die Chatbots von Fremdfirmen öffnete.[23]

Die Einsatzfelder werden dabei immer vielfältiger. Bei Taco Bell (einer US-Kette im Bereich Systemgastronomie) nimmt der Roboter inzwischen nicht nur die Essensbestellung entgegen, er kümmert sich auch um die Rechnung, gibt kulinarische Tipps und organisiert Gruppenbestellungen.[24] Auch viele Buchungsportale setzen inzwischen auf Chatbots, ebenso wie Wetterdienste oder Anbieter für Gesundheitstipps. Entsprechende Fortschritte bei künstlicher Intelligenz und maschinellem Lernen vorausgesetzt, könnten die Kommunikationsroboter in den kommenden Jahren zu virtuellen Assistenten mutieren, die menschlichen Servicemitarbeitern sowohl in der Kundenkommunikation als auch im Kundenservice immer mehr Aufgaben abnehmen.

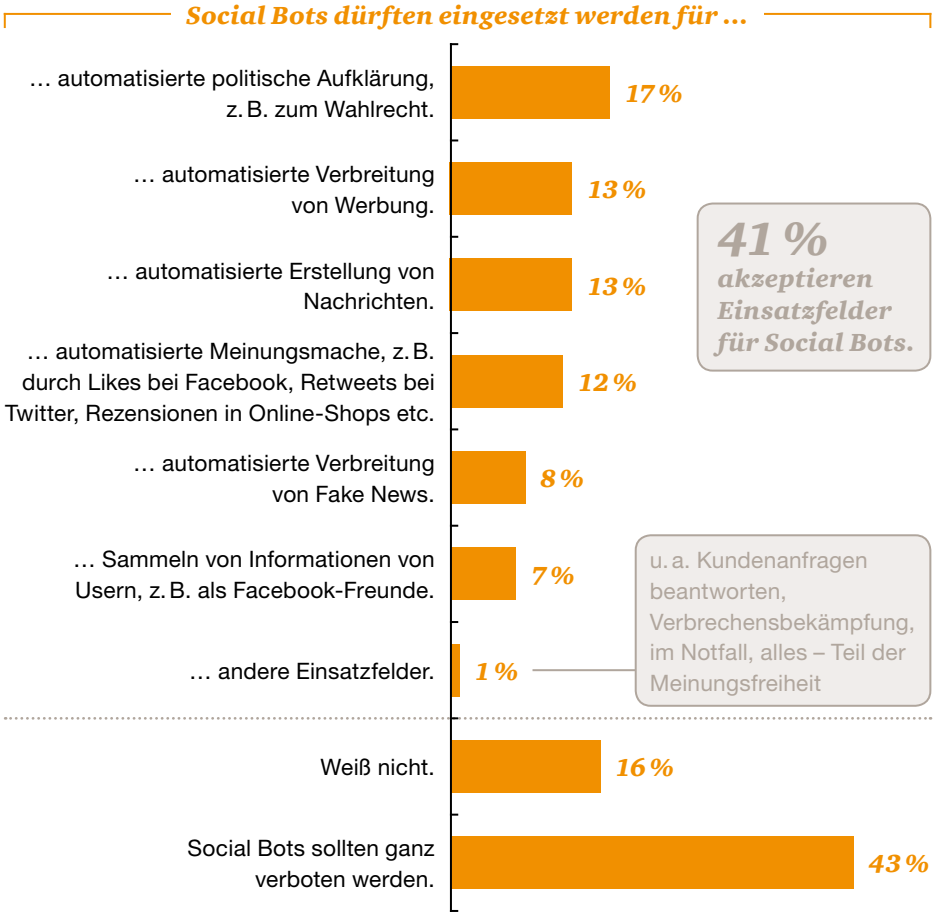
**Abb. 8 Akzeptierter Einsatz von Social Bots**

Über vier von zehn Deutschen sind für ein generelles Verbot von Social Bots.

Zu welchen Zwecken sollten Social Bots Ihrer Meinung nach eingesetzt werden dürfen?

Mehrfachnennung waren möglich

Basis: Alle Befragten, n = 1.000




[23] Vgl. J. Sablich, „How to plan your next travel with a chatbot“, New York Times, 2017.
[24] Vgl. S. Kirchhof, „Was der Hype um Social Bots bedeutet“, Horizont, 2016.

Die Grenze zwischen Chatbot und Social Bot dürfte im Zuge dieser Entwicklung fließender werden – und der kontrollierte Einsatz von Meinungsrobotern eine durchaus realistische Option. Ein potenzielles Verwendungsgebiet, für Unternehmen wie auch für politische Institutionen, ist das sogenannte Influencer-Marketing. Damit ist die Methode gemeint, das Marketing im Internet bzw. in den sozialen Medien gezielt darauf auszurichten, einflussreiche Multiplikatoren für das eigene Produkt, die eigene Marke oder eben auch die eigene Partei zu gewinnen. Klassischerweise handelt es sich bei diesen Influencern um Journalisten oder Blogger. Daneben können aber zum Beispiel auch „Fans“ (also etwa Kunden, die einem Unternehmen bei Facebook oder Twitter folgen) zu wertvollen Multiplikatoren werden.

Wie sich Mischformen aus Chatbot und Social Bots (wir wollen dafür den Begriff „Influencer-Bot“ einführen) in solche Strategien einbinden lassen, lässt sich noch nicht konkret sagen. Allerdings steht außer Frage, dass der Einsatz einem nicht nur rechtlich, sondern auch ethisch eindeutigen Kriterienkatalog zu folgen hätte. Daher wollen wir anhand von zwei Merkmalen skizzieren, welchen Anforderungen eine solche Mischform genügen müsste, um sowohl einen klaren Mehrwert zu generieren als auch öffentliche Akzeptanz zu erhalten:

- In Kapitel A haben wir definiert, dass Chatbots reaktiv kommunizieren, während Social Bots auch selbst aktiv werden. Influencer-Bots wären demgemäß Social Bots.
- Zudem definierten wir, dass sich Chatbots einer Quelle zuordnen lassen, während Social Bots ihre Urheberschaft zu verschleiern suchen. Angesichts dessen würde es sich bei Influencer-Bots um Chatbots handeln.

# F Fake News, Social Bots und die Rolle der Medien

Während in den 1980er-Jahren in den USA angeblich auf einen Journalisten ein PR-Experte kam, soll das Verhältnis mittlerweile bei eins zu fünf liegen.[25] Doch nicht nur die Übermacht professioneller Einflüsterer erschwert den traditionellen Medien das Leben. Das Internet hat aus dem einstigen Tagesgeschäft ein Minutengeschäft gemacht. Während Zeitungsredakteure früher die Nachrichten für den nächsten Morgen aufbereiteten, sollen Online-journalisten heute quasi in Echtzeit nicht nur die News, sondern im besten Fall auch die Analyse liefern. Parallel dazu sind die Werbeerlöse der klassischen Medien eingebrochen, während die Bereitschaft des Publikums, für journalistische Inhalte zu zahlen, tendenziell sinkt.

Erschwerend müssen sich die Redaktionen nun auch mit neuen Phänomenen wie Fake News oder Social Bots auseinandersetzen. Dabei stehen sie vor dem zusätzlichen Problem, dass ein Teil der Bevölkerung die Arbeit von Journalisten zunehmend kritisch betrachtet – oder zumindest in der Lage ist, diese Kritik (Stichwort „Lügenpresse“) via Internet direkter und heftiger zu artikulieren, als dies früher die Leserbriefschreiber konnten. Charakteristisch für diese Entwicklung ist, dass der neue US-Präsident via Twitter regelmäßig gegen Medien wie die New York Times den Vorwurf erhebt, sie selbst seien es, die Fake News produzierten. Haben Journalisten angesichts dieser schwierigen Bedingungen überhaupt noch eine Chance, ihre angestammte Rolle als Gatekeeper des demokratischen Diskurses zu verteidigen? Oder drohen sie im angeblich postfaktischen Zeitalter in einer Flut bewusst verbreiteter Falschnachrichten und böswilliger Meinungsroboter zu versinken?

Um die Debatte mit einer soliden Faktengrundlage zu untermauern, hat PwC im April und Mai 2017 eine repräsentative Bevölkerungsumfrage zum Thema „Social Bots und Fake News“ durchführen lassen; daran nahmen 1.000 Bundesbürger ab 18 Jahren teil. Dabei zeigte sich, dass die meisten Befragten mit dem Begriff Fake News deutlich mehr anzufangen wissen als mit dem Begriff Social Bots. So meinten 84 %, sie wüssten über Fake News „relativ gut“ oder zumindest „ungefähr“ Bescheid; bei Social Bots waren es hingegen nur 36 %. Demgegenüber meinten 25 %, sie würden Social Bots nur dem Namen nach kennen, während 39 % angaben, sie könnten mit dem Stichwort gar nichts anfangen. Nachdem die Befragten aufgeklärt wurden, was es mit den Meinungsrobotern auf sich hat, meinten 9 %, sie hätten Social Bots „ganz sicher“ schon einmal in den sozialen Netzwerken wahrgenommen. 28 % meinten, dies sei „vermutlich“ der Fall, ganz sicher waren sie aber nicht.

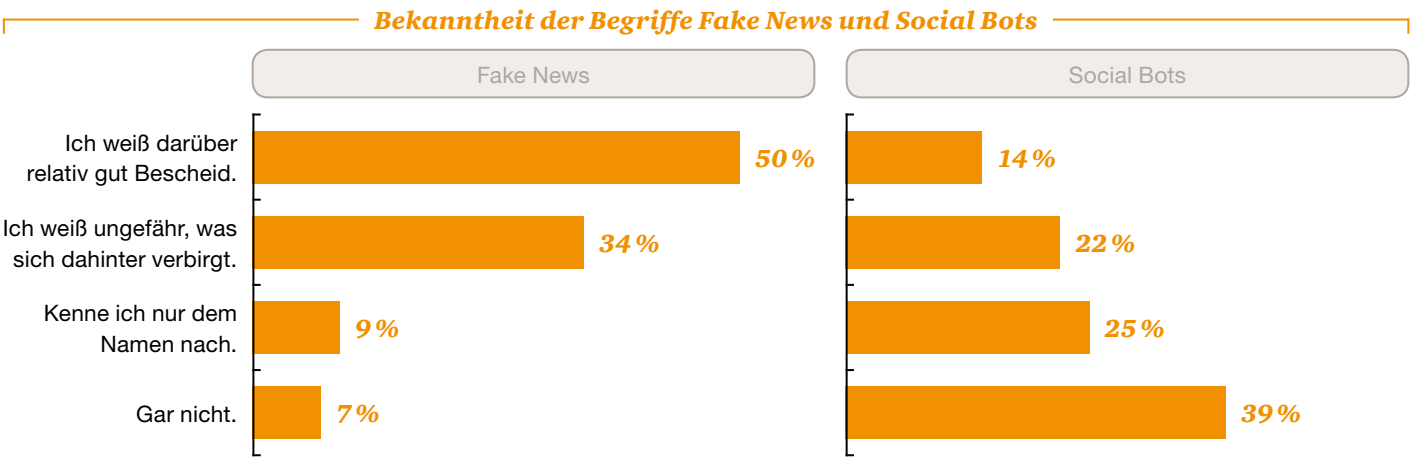

[25] Vgl. S. Russ-Mohl, „Am Ende des Aufklärungszeitalters“, Neue Zürcher Zeitung, 2016.

**Abb. 9 Bekanntheit von Begriffen**

Die Hälfte der Deutschen weiß über Fake News relativ gut Bescheid. Social Bots sind hingegen vier von zehn Befragten nicht bekannt.

Inwieweit kennen Sie die folgenden Begriffe?

Basis: Alle Befragten (Skalierte Abfrage), n = 1.000




Interessanterweise bietet die Umfrage starke Hinweise darauf, dass Fake News oder Social Bots die Arbeit etablierter Medien nicht zwingend unterminieren müssen, sondern im Gegenteil sogar dazu beitragen könnten, das Vertrauen in die klassische journalistische Arbeit wieder zu stärken. So rechnen nur 5 % der Deutschen damit, in kostenpflichtigen Tages- oder Wochenzeitungen auf Fake News zu treffen – während dies bei Twitter 66 % und Facebook sogar 79 % tun. Dazu passt, dass 61 % der Befragten meinte, es sei sogar eine originäre Aufgabe klassischer Medien (Zeitungen, Magazine, Fernsehen, Radio), die Öffentlichkeit über Phänomene wie Fake News und Social Bots aufzuklären. Dagegen sahen nur 57 % die Plattformbetreiber selbst (also z. B. Twitter oder Facebook) und auch nur 53 % den Gesetzgeber in der Verantwortung. Tatsächlich wünschten sich neun von zehn Befragten, dass die Redaktionen personell aufgestockt werden, damit sie Informationen intensiver prüfen können. Allerdings: Nur ein Viertel zeigte sich bereit, dafür auch zu zahlen.

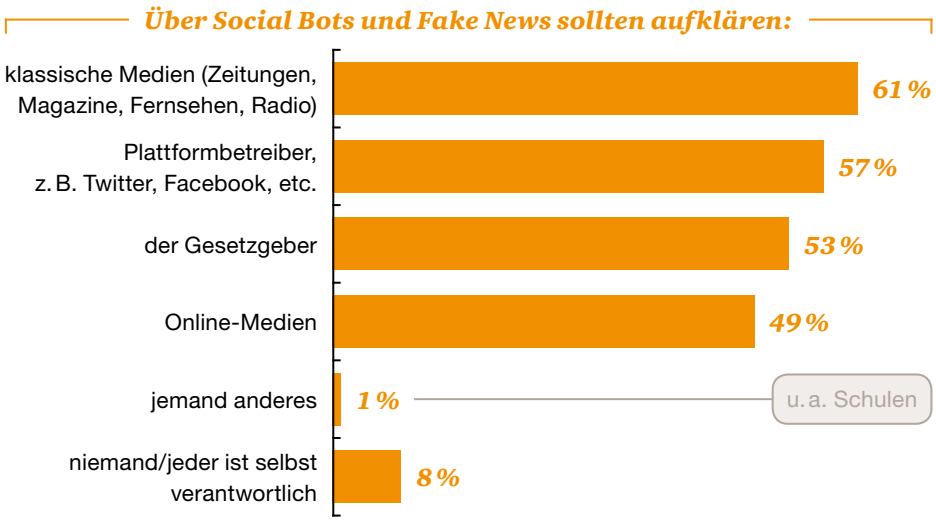
**Abb. 10 Aufklärung über Social Bots und Fakes News**

Die Aufklärung über Social Bots und Fake News sollte in erster Linie durch die klassischen Medien erfolgen.

Wer sollte Ihrer Meinung nach über Fake News und Social Bots aufklären?

Mehrfachnennung waren möglich

Basis: Alle Befragten, n = 1.000




Hier zeigt sich ein grundsätzlicher Widerspruch. Denn dass insbesondere Twitter von immer mehr Journalisten als Informationsquelle genutzt wird, liegt nicht nur an den Geschwindigkeitsvorteilen, die der Kurznachrichtendienst etwa gegenüber Korrespondenten oder Nachrichtenagenturen bietet – sondern auch daran, dass soziale Medien als Rechercheinstrument günstig sind. Viele Redaktionen haben das Scannen der Social-Media-Kanäle längst institutionalisiert. So gibt es beispielsweise bei der Deutschen Presseagentur (dpa) einen Listening Officer, der „soziale Medien jedweder Art auf Klumpen von Nachrichten [beobachtet], die darauf hindeuten, dass irgendwo etwas passiert".[26]

Zugleich ist im Zuge von Fake News und Social Bots aber auch die Sensibilität im Umgang mit den neuen Quellen enorm gestiegen. Auch hier ist die dpa ein gutes Beispiel. Denn parallel zum Listening Officer wollte die Agentur in diesem Jahr die Rolle eines sogenannten Verification Officers einführen, „der große Erfahrung darin hat, zu erkennen, ob Meldungen plausibel sind".[27]

Redaktionen, die es sich leisten können (oder wollen), haben den Kampf gegen Fake News und Social Bots jedenfalls aufgenommen. Das vielleicht beste Beispiel ist die First Draft Coalition, deren Mitglieder sich in Zukunft gegenseitig bei Recherche und Verifikation unterstützen wollen.[28]

Aus Deutschland gehören unter anderem ARD und ZDF diesem Verbund an, aus den USA die Nachrichtenagentur AP und aus Großbritannien die Tageszeitung Guardian. Das vielleicht Bemerkenswerteste allerdings ist: Neben klassischen Medien schlossen sich auch Technologieunternehmen wie Facebook und Twitter der First Draft Coalition an. Quasi parallel hat Facebook Anfang dieses Jahres – offenbar als Reaktion auf die Kritik an der Verbreitung von Fake News während des US-Präsidentschaftswahlkampfs – das Facebook Journalism Project ausgerufen.[29]

[26] News Aktuell, „Die große Falle: Was das Phänomen Fake News für Kommunikation und PR bedeutet", News Aktuell, 2017.
[27] Ebenda.
[28] Vgl. Meedia, „Große Koalition gegen Fake News: Globales Bündnis von über 40 Medien und Web-Konzernen geht an den Start", Meedia, 2017.
[29] Vgl. Zeit Online, „Facebook startet Projekt gegen Falschmeldungen", Zeit Online, 2017.

# G Wie können sich Unternehmen und Institutionen schützen?

Handelt es sich bei Social Bots in erster Linie um Instrumente zur Manipulation der öffentlichen Meinung – oder sind sie längst auch zur Waffe in einem immer undurchsichtigeren Cyberwar mutiert? Mitte Mai berichtete das US-Magazin Time von einer russischen Cyberattacke auf das amerikanische Verteidigungsministerium.[30] Demnach hatten zwei Monate zuvor mehr als 10.000 Ministeriumsmitarbeiter über Twitter scheinbar harmlose Mitteilungen erhalten, deren Inhalt exakt auf die Interessen ihrer Empfänger zugeschnitten war. Wer sich bei Twitter zum Beispiel als Sportfan zu erkennen gab, der erhielt einen Link, der angeblich zu einem Bericht über ein Sportereignis führte. Tatsächlich jedoch verbargen sich hinter den Links gefährliche Schadprogramme. Es handelte sich mithin um eine Spear-Attacke (siehe Kapitel D) auf eine der mächtigsten Behörden der Welt.

Dass die sozialen Medien nicht nur ein Verbreitungskanal für Fake News, sondern auch ein potenzielles Einfallstor für Cyberangriffe darstellen, liegt auf der Hand. Über Netzwerke wie LinkedIn oder Xing lassen sich für Außenstehende heutzutage die Organigramme ganzer Unternehmen nachvollziehen. Und bei Twitter kommunizieren „Professionals“ häufig sehr offen mit „Kontakten“, deren Identität sie in vielen Fällen vermutlich nicht wirklich überprüft haben. Wenn selbst das amerikanische Verteidigungsministerium zum Ziel einer über Social Media lancierten Cyberattacke wird – dann kann potenziell auch jede andere Institution zum Opfer eines solchen Angriffs werden.

Wie können sich Regierungen, Parteien, Unternehmen und andere Organisationen gegen solche Angriffe zur Wehr setzen? Die Betreiber der sozialen Netzwerke – also Milliardenkonzerne wie Facebook oder Twitter – müssten zum Schutz der eigenen Glaubwürdigkeit eigentlich ein vitales Interesse daran haben, Phänomene wie Fake News, Social Bots oder Spear-Attacken mit aller Macht zu bekämpfen. Tatsächlich veränderte Facebook jüngst seine Algorithmen, um mögliche Falschnachrichten leichter erkennen zu können. Fast zeitgleich ergriff auch Google eine Reihe von Maßnahmen, um die Verbreitung von Fake News zu erschweren. Trotzdem drängt sich bisweilen der Eindruck auf, dass die Schlacht nur halbherzig geführt wird. Zwar betont auch Twitter, dass die eigenen Algorithmen darauf ausgerichtet würden, Manipulationen der Trendliste zu erkennen und gegebenenfalls reagieren zu können. Als das Unternehmen zu dem Angriff auf das Verteidigungsministerium gefragt wurde, gab es jedoch keinen Kommentar ab.[31]

Der Fairness halber muss gesagt werden, dass das Thema für die Plattformbetreiber heikel ist. Zum einen geht es natürlich um monetäre Fragen – der Kampf gegen Fake News oder Social Bots kostet Geld. Zum anderen geht es aber auch um sehr grundsätzliche Erwägungen. Netzwerke wie Twitter oder auch Instagram basieren technologisch gesehen ganz entscheidend auf dem Prinzip offener Schnittstellen. Deshalb dürften sich die Betreiber dagegen sträuben, den Urhebern von Social Bots zum Beispiel dadurch das Handwerk zu legen, dass sie ihnen den Zugang zu den Schnittstellen (siehe Kapitel A) erschweren. Auch andere theoretisch denkbare Abwehrmaßnahmen dürften aufgrund ihrer Radikalität den Plattformbetreibern kaum gefallen. Dazu würde zum Beispiel eine Art „Ausweispflicht“ gehören. Sie würde darauf hinauslaufen, dass Nutzer bei der Eröffnung eines Facebook- oder Twitter-Accounts einen ähnlichen Identifizierungsprozess durchlaufen wie etwa bei einem Girokonto.

Darüber hinaus befinden sich die Netzwerkbetreiber auch politisch auf schwierigem Terrain: Sollen zum Beispiel in den USA beheimatete Unternehmen wie Facebook, Twitter oder Instagram in ihrem Kampf gegen Social Bots, Spear-Phishing- oder DDoS-Attacken mit den amerikanischen Geheimdiensten kooperieren – oder dürfen sie gerade das nicht tun? Ein anderes Beispiel: Wie sieht der richtige Umgang mit falschen Nachrichten aus? Wer entscheidet überhaupt, was eine Fake News ist und was nicht? Welche Geschichte ist objektiv falsch – und welche lediglich politisch „gespinnt“. Bei Facebook weiß man um die enorme Brisanz solcher Fragen. Während des US-Wahlkampfs sah sich das Unternehmen sogar Vorwürfen ausgesetzt, bei der redaktionellen Kuratierung der Trending News „liberal“ geprägte Storys gegenüber „konservativen“ gezielt zu bevorzugen.[32]

[30] Vgl. M. Calabresi, „Inside Russia’s social media war on America“, Time, 2017.
[31] Vgl. A. Breland, „Social media fights back against fake news“, The Hill, 2017.
[32] Vgl. M. Nunez, „Former Facebook workers: We routinely suppressed conservative news“, Gizmodo.com, 2016.

Natürlich spielen auch rechtliche Aspekte eine Rolle. Zum Zeitpunkt der Fertigstellung des vorliegenden Whitepapers wurde in Deutschland erregt über das sogenannte Hate-Speech-Gesetz (offizielle Bezeichnung: „Netzwerkdurchsetzungsgesetz") diskutiert. Der Entwurf von Justizminister Heiko Maas sah vor, dass die Netzwerkbetreiber offenkundig strafbare Inhalte in der Regel binnen 24 Stunden, in komplexen Fällen innerhalb von sieben Tagen löschen müssen; verstoßen sie gegen diese Vorgaben, drohen Bußgelder von bis zu 50 Millionen Euro. Medienberichten zufolge kritisierte Facebook das Gesetz als verfassungswidrig. In einem Lobbypapier des Konzerns hieß es demnach: „Der Rechtsstaat darf die eigenen Versäumnisse und die Verantwortung nicht auf private Unternehmen abwälzen. Die Verhinderung und Bekämpfung von Hate Speech und Falschmeldungen ist eine öffentliche Aufgabe, der sich der Staat nicht entziehen darf."[33]

In der Tat begibt sich die Bundesregierung mit dem Hate-Speech-Gesetz auf rechtliches Neuland. Denn der zuletzt diskutierte Ministeriumsentwurf läuft darauf hinaus, Ordnungswidrigkeiten oder gar Straftatbestände von privater Seite – sprich: von Facebook, Twitter usw. – feststellen zu lassen. Dieser Ansatz ist in der deutschen Gesetzgebung bislang ohne Beispiel. Hinzu kommt, dass die Grenzen zwischen einer gesellschaftlich unerwünschten und einer rechtlich verbotenen Äußerung fließend sind. Der Entwurf von Heiko Maas fordert also im Extremfall eine sichere Bewertung nicht sicher zu bewertender Sachverhalte – und das von einem privatwirtschaftlichen Unternehmen unter Vorgabe einer zeitlich eng gefassten Frist.

Dieser juristische Drahtseilakt zeigt exemplarisch, wie schwierig es ist, Social-Media-Phänomene wie Hate Speech, Fake News oder Social Bots mit den Mitteln des Rechts in den Griff zu bekommen. Selbst wenn man annähme, die Linie zwischen Recht und Unrecht ließe sich trennscharf ziehen, bliebe das Problem der Durchsetzung. Die Urheber illegaler Handlungen sitzen häufig im fernen Ausland und entziehen sich so der nationalstaatlichen Rechtsprechung. Auch die Macht der Plattformbetreiber stößt hier an Grenzen. Denn was nützen schärfere AGBs, wenn kaum Aussicht besteht, Rechtsverletzungen zu sanktionieren?

Die potenzielle Gefahr, die von Fake News, Social Bots oder Cyberattacken in den sozialen Medien ausgeht, verlangt nach gesamtgesellschaftlichen Antworten. Im Mittelpunkt muss dabei die Aufklärung stehen. Hier ist zum Beispiel die ehrenamtliche Initiative Botswatch zu nennen, die sich zur Aufgabe gemacht hat, verdächtige Twitter-Aktivitäten bei politischen Ereignissen in Deutschland zu analysieren. Daneben gibt es zwei vom Bundesministerium für Bildung und Forschung geförderte Projekte, die sich mit Fake News und verwandten Phänomenen auseinandersetzen. Sie heißen PropStop und Social Media Forensics. Ziel muss es sein, solche Initiativen zukünftig auch auf breiter internationaler Ebene zu verankern.

Zudem muss das Problem nicht nur auf der Makro-, sondern auch auf der Mikroebene angegangen werden. So werden Parteien, Unternehmen und sonstige Institutionen nicht umhinkommen, eigene Schutzmechanismen gegen die hier beschriebenen Risiken zu entwickeln. Wir wollen an dieser Stelle noch keine komplette Roadmap entwerfen. Klar allerdings ist, dass die entsprechenden Maßnahmen von zusätzlichen Investitionen in die IT-Sicherheit über Vorkehrungen zur Krisenkommunikation bis hin zu einer stärkeren Sensibilisierung der Mitarbeiterschaft reichen müssen. Wie komplex die Probleme sind, vor denen wir stehen, illustriert abschließend ein weiterer Gastbeitrag von Professor Dr. Jens Lehmann und Klaudia Thellmann.

[33] Spiegel Online, „Facebook nennt Maas-Gesetz verfassungswidrig", Spiegel Online, 2017.

Fraunhofer IAIS

# H Gastbeitrag: Zwei technische Ansätze zur Identifizierung von Social Bots

***Von Prof. Dr. Jens Lehmann und Klaudia Thellmann, Fraunhofer IAIS.***

Auf technischer Seite kann durch Anwendungen und Dienste den Nutzern eine Stütze zur Verfügung gestellt werden, um Bots, Falschinformationen und Manipulationsversuche so sicher wie möglich zu erkennen.

Dabei unterscheidet man grundsätzlich zwei Methoden: Die eine ist auf die zugrunde liegende Graphstruktur des sozialen Netzes ausgelegt. Es geht darum, mittels Graphalgorithmen Verbindungen von Profilen zu untersuchen, um Gruppen von Bots und Gruppen von legitimen Nutzern zu unterscheiden und somit Bot-Netzwerke ausfindig zu machen.[34]

Eine andere, etwas effektivere Gruppe von Ansätzen wertet zur Bot-Detektion Profilinformationen –sogenannte Features – aus. Zu den untersuchten Profilinformationen zählen unter anderem: Alter des Accounts, Vernetzungs- und Interaktionsverhalten, Anzahl der Beiträge pro Tag, Inhalt der Beiträge, Anzahl von Freunden und Followern oder plausible Timeline.[35,36,37]

***Bot-Erkennung über Graph-basierte Ansätze***

Die Ansätze, die in Richtung Graph-analyse gehen, sind auf das Erkennen von Gemeinschaften ausgelegt. Dabei werden Cluster von Nutzerprofilen, die überdurchschnittlich eng miteinander verknüpft sind, um ein als vertrauenswürdig gekennzeichnetes Profil herum identifiziert[34]. Diese Analyse der Vernetzung von Social-Bot-Profilen wird auf Grundlage der Annahme vorgenommen, dass sich Bots tendenziell mehr mit anderen Bots vernetzen als mit legitimen Nutzern. Das Verfahren ermöglicht somit eine Partitionierung des Graphen, also des sozialen (Teil)-Netzes, in Gruppen von Bots und von legitimen Nutzern beziehungsweise ein Ranking von (wahrscheinlichen) Fake-Profilen[38].

**Abb. 11 Darstellung eines sozialen Netzes als Graph**

[34] B. Viswanath, A. Post, K. P. Gummadi und A. Mislove, „An analysis of social network-based sybil defenses“, ACM SIGCOMM Computer Communication Review, 2010.
[35] E. Ferrara, O. Varol, C. Davis, F. Menczer und A. Flammini, „The rise of social bots“, arXiv preprint, 2014.
[36] C. A. Davis, O. Varol, E. Ferrara, A. Flammini und F. Menczer, „BotOrNot: A system to evaluate social bots“, Proceedings of the 25th International Conference Companion on World Wide Web, 2016.
[37] O. Varol, E. Ferrara, C. A. Davis, F. Menczer und A. Flammini, „Online human-bot interactions: Detection, estimation, and characterization“, arXiv, 2017.
[38] Q. Cao, M. Sirivianos, X. Yang und T. Pregueiro, „Aiding the detection of fake accounts in large scale social online services“, Proceedings of the 9th USENIX conference on Networked Systems Design and Implementation, 2012.

Den meisten Graph-basierten Ansätzen liegt die Annahme zugrunde, dass Bots sich mit vielen anderen Bots vernetzen, während legitime Nutzer die Vernetzung mit Bots meiden. Diese Annahmen haben sich jedoch als nicht immer zutreffend erwiesen.[39] In der Studie von Jing et al.[40], in der das Vernetzungsverhalten von einer halben Million Bot-Accounts auf der sozialen Plattform Renren untersucht wurde, konnten keine stark vernetzten Bot-Gemeinschaften beobachtet werden. Im Gegenteil waren die Bots eher darauf programmiert, legitime Gemeinschaften zu infiltrieren.

### *Bot-Erkennung über Feature-basierte Ansätze*

Es gibt einige veröffentlichte Ansätze, die auf Grundlage großer Mengen an gesammelten Daten mittels maschineller Lernverfahren versuchen, Profilinformationen aus den sozialen Netzwerken auszuwerten. Damit sollen ähnliche Verhaltensmuster von Bots aufgedeckt und in Cluster gruppiert oder Profile von Bots aufgrund erlernter Unterscheidungskriterien erkannt werden. Neben Verhaltensmustern und Profildaten können hierbei auch Inhalte untersucht werden. Wenn ein Twitter-Nutzer zum Beispiel oft sehr ähnliche Inhalte in Posts verwendet, dann ist das ein Indikator dafür, dass es sich um einen Bot handelt, der gezielt spezielle Inhalte, zum Beispiel zur Stimmungsmache, verbreitet.

Ein prominentes Beispiel, das auch in der Praxis Anwendung findet, ist die von einer Gruppe um den Computerwissenschaftler Emilio Ferrara entwickelte kostenlose Web-API Botometer (früher bekannt als BotOrNot; siehe Kapitel B) für Twitter.[37] Für jedes Subjekt (Bot oder Nutzer) werden unterschiedliche Kennzahlen (Features) extrahiert, die Profilinformationen umfassen. Diese Feature-Vektoren werden dann als Eingabe für ein Lernverfahren verwendet, welches für jeden Nutzer eine Bewertung erstellt, anhand deren abgeleitet werden kann, ob es sich um einen Bot oder einen Menschen handelt.

Das vorgeschlagene Verfahren weist laut Varol et. al[37] eine hohe Präzision in der Detektion von Twitter-Bots auf. Allerdings wurde die Evaluierung nur auf Bots ausgeführt, die auf Honeypots reinfallen – darunter versteht man einen als Köder eingerichteten Account, der die Bots dazu verleiten soll, sich mit dem Account zu vernetzen. Dementsprechend kann dieses Klassifikationsmodell nur Bots erkennen, die ähnliche Eigenschaften haben wie solche Bots, die auf den Honeypot hereinfallen. Das Ergebnis sollte man daher nur als Ausgangspunkt für eine eigene Einschätzung nehmen, da es nicht vollständig verlässlich ist.

Zu den weiteren Beispielen für ähnliche Ansätze gehört das unter anderem von Wissenschaftlern der University of California[39] entwickelte Klassifizierungssystem zum Detektieren von Bots. Es baut auf einer Verhaltensanalyse von Nutzern auf, genauer gesagt, dem Surfverhalten von Nutzern. Hierbei wird insbesondere untersucht, wann und in welcher Abfolge Anfragen an Webseiten abgeschickt werden. Ein anderer vorgeschlagener Ansatz zum Klassifizieren von Bot-Profilen basiert ebenfalls auf Verhaltensstatistiken, insbesondere auf dem Vernetzungsverhalten vom eigentlichen Profil und den damit vernetzten Profilen.[41]

Eine andere Gruppe von Wissenschaftlern schlägt wiederum eine Detektion von Twitter-Bot-Profilen vor, die Daten zum Erlernen der Unterscheidungsmerkmale zwischen Bot- und legitimen Profilen aus den Honeypots bezieht.[42] Doch auch hier gilt: Die Honeypot-Strategie war zwar anfangs sehr effektiv und half, tausende Bots einzufangen, weil frühere Bots (i. d. R. Spam-Bots) nicht darauf ausgelegt waren, Honeypots zu erkennen. Das hat sich aber in der Zwischenzeit geändert.[35]

Da sich die technischen Möglichkeiten zur Erkennung von Social Bots noch im Entwicklungsstadium befinden und die Bot-Detektion der Bot-Entwicklung üblicherweise hinterherhinkt, kann man derzeit wenig konkrete Aussagen zu ihrer Effektivität oder Missbrauchsanfälligkeit machen. Fest steht aber, dass versucht wird, Social-Bots möglichst menschenähnlich zu gestalten (siehe Kapitel C). Dadurch wird es immer schwieriger, selbst mittels Feature-basierten Ansätzen Auffälligkeiten oder Ungereimtheiten in Profilen und Verhaltensweisen zu finden.[43]

Maschinelle Lernverfahren, die Modelle zur Klassifikation von Social Bots produzieren, könnten auch zur Entwicklung von Bots mit menschenähnlicherem Verhalten genutzt werden. Dabei würden diese Modelle dazu genutzt, gewisse Merkmale abzuändern, die die Bots enttarnen würden. Außerdem sind diese Ansätze auf die Erhebung von Profildaten angewiesen, und manche Ansätze benötigen sogar direkten Zugriff auf das Nutzerprofil, woraus sich wieder Missbrauchspotenziale ergeben. Klar ist, dass es in den kommenden Monaten und Jahren zu einem Wettlauf kommen wird zwischen den Betreibern von Social Bots einerseits und den technischen Möglichkeiten, diese Bots zu erkennen und zu verhindern, andererseits. Noch ist unklar, wer dieses Rennen gewinnt.

---

[39] G. Wang, M. Mohanlal, C. Wilson, X. Wang, M. Metzger, H. Zheng und B. Y. Zhao, „Social turing tests: Crowdsourcing Sybil detection“, arXiv, 2012.
[40] J. Jing , C. Wilson, X. Wang, W. Sha, P. Huang, Y. Dai und B. Y. Zhao, „Understanding latent interactions in online social networks“, ACM Transactions on the Web (TWEB), 2013.
[41] Z. Yang, C. Wilson, X. Wang, T. Gao, B. Y. Zhao und Y. Dai, „Uncovering social network Sybils in the wild“, ACM Transactions on Knowledge Discovery from Data (TKDD), 2014.
[42] K. Lee, B. D. Eoff und J. Caverlee, „Seven Months with the Devils: A Long-Term Study of Content Polluters on Twitter“, ICWSM, 2011.
[43] S. Kind et al., Thesenpapier zum öffentlichen Fachgespräch „Social Bots – Diskussion und Validierung von Zwischenergebnissen“ am 26. Januar 2017 im Deutschen Bundestag, 2017.

# Quellenverzeichnis


***D. Alba, „The Political Twitter Bots Will Rage This Election Day“,***
Wired.com, 2016.

***T. Alloway, „T. Bradshaw, Cynk sinks after 36.000 % climb“,***
Financial Times, 2014.

***A. Bessi und E. Ferrara, „Social bots distort the 2016 US presidential election online discussion“,***
First Monday, 2016.

***P. Beuth, „Furcht vor den neuen Wahlkampfmaschinen“,***
Zeit Online, 2017.

***A. Breland, „Social media fights back against fake news“,***
The Hill, 2017.

***M. Calabresi, „Inside Russia's Social Media War on America“,***
Times, 2017.

***E. Ferrara, „Manipulation and abuse on social media“,***
ACM, 2015.

***E. Ferrara et al., „The Rise of Social Bots“,***
Communications of the ACM, Bd. 59, Nr. 7, S. 96–104, 2016.

***The Guardian, „Computer simulating 13-years-old boy becomes first to pass Turing test“,***
Guardian.com, 2014.

***S. Hegelich, „Invasion der Meinungs-Roboter“,***
Analysen und Argumente, Nr. 221, 2016.

***S. Hegelich und D. Janetzko, „Are social bots on twitter political actors? Empirical evidence from a Ukrainian social botnet,“***
Tenth International AAAI Conference on Web and Social Media, 2016.

***P. N. Howard und B. Kollanyi, „Bots,#StrongerIn, and#Brexit: computational propaganda during the UK-EU Referendum “,***
Social Science Research Network 2798311, 2016.

***E. Hunt, Tay, „Microsoft's AI Chatbot, gets a crash course in racism from Twitter“,***
Guardian.com, 2016.

***S. Kind et al., Thesenpapier zum öffentlichen Fachgespräch „Social Bots – Diskussion und Validierung von Zwischenergebnissen“***
am 26. Januar 2017 im Deutschen Bundestag, 2017.

***S. Kirchhof, „Was der Hype um Social Bots bedeutet“,***
Horizont, 2016.

***M. Levine, „Cynk makes the case for buying friends“,***
Naked Short Selling, Bloomberg, 2014.

***Meedia, „Große Koalition gegen Fake News: Globales Bündnis von über 40 Medien und Web-Konzernen geht an den Start“,***
Meedia, 2017.

***MIT Technology Review, „How a simple spambot became the second most powerful member of an Italien Social Network“,***
MIT Technology Review, 2014.

***A. Newitz, „Ashley Madison Code shows more women, and more bots“,***
Gizmodo.com, 2015.

***News Aktuell, „Die große Falle: Was das Phänomen Fake News für Kommunikation und PR bedeutet“,***
News Aktuell, 2017.

***M. Nunez, „Former Facebook workers: We routinely suppressed conservative news“,***
Gizmodo.com, 2016.

***A. Rinke, „Sorge um gekaufte digitale Hilfe im Wahlkampf“,***
Reuters, 2016.

***M. Rosenbach und G. Traufetter, „Betreiben von Social Bots soll unter Strafe stehen“,***
Spiegel, 2017.

***S. Russ-Mohl, „Am Ende des Aufklärungszeitalters“,***
Neue Zürcher Zeitung, 2016.

***J. Sablich, „How to plan your next travel with a chatbot“,***
New York Times, 2017.

***Spiegel Online, „Facebook nennt Maas-Gesetz verfassungswidrig“,***
Spiegel Online, 2017.

***A. M. Turing, „Computing machinery and intelligence“,***
Mind, Bd. 59, Nr. 236, S. 433–460, 1950.

***R. S. Wallace, „The anatomy of ALICE“, in Parsing the Turing Test,***
Springer, 2009.

***G. Wang, T. Konolige, C. Wilson, X. Wang, H. Zheng und B. Y. Zhao, „You are how you click: Clickstream analysis for Sybil detection“,***
Usenix Security, 2013.

***J. Weizenbaum, „ELIZA – a computer program for the study of natural language communication between man and machine“,***
Communications of the ACM, Bd. 9, Nr. 1, 1966.

***O. Westerhagen, „Der Feind im Netz. Bot-Netze als Gefahr für die Gesellschaft.“,***
c't, 2017.

***Zeit Online, „AfD will Social Bots im Wahlkampf einsetzen“,***
Zeit Online, 2016.

***Zeit Online, „Facebook startet Projekt gegen Falschmeldungen“,***
Zeit Online, 2017.

# Ihre Ansprechpartner

***Werner Ballhaus***
Leiter Technologie, Medien und Telekommunikation
Tel.: +49 211 981-5848
werner.ballhaus@pwc.com

***Bernd Reimer***
Forensic Services
Tel.: +49 71 125 034-3571
bernd.reimer@pwc.com

***Dr. Christian Dressel***
Praxisgruppe IP IT & Datenschutzrecht
Tel.: +49 211 981-1815
christian.dressel@pwc.com

***Mathias Elsäßer***
Data Driven Marketing
Tel.: +49 71 125 034-3307
mathias.elsaesser@pwc.com

## Pressekontakt:

***Julia Wollschläger***
Communications
Tel.: +49 211 981-5095
julia.wollschlaeger@pwc.com

***Über uns***
Unsere Mandanten stehen tagtäglich vor vielfältigen Aufgaben, möchten neue Ideen umsetzen und suchen Rat. Sie erwarten, dass wir sie ganzheitlich betreuen und praxisorientierte Lösungen mit größtmöglichem Nutzen entwickeln. Deshalb setzen wir für jeden Mandanten, ob Global Player, Familienunternehmen oder kommunaler Träger, unser gesamtes Potenzial ein: Erfahrung, Branchenkenntnis, Fachwissen, Qualitätsanspruch, Innovationskraft und die Ressourcen unseres Expertennetzwerks in 157 Ländern. Besonders wichtig ist uns die vertrauensvolle Zusammenarbeit mit unseren Mandanten, denn je besser wir sie kennen und verstehen, umso gezielter können wir sie unterstützen.

**PwC.** Mehr als 10.300 engagierte Menschen an 21 Standorten. 1,9 Mrd. Euro Gesamtleistung. Führende Wirtschaftsprüfungs- und Beratungsgesellschaft in Deutschland.

**PwC Legal.** Mehr als 200 Rechtsanwältinnen und Rechtsanwälte an 18 Standorten. Integrierte Rechtsberatung für die Praxis.

www.pwc.de
www.pwclegal.de