TAB BÜRO FÜR TECHNIKFOLGEN-ABSCHÄTZUNG
BEIM DEUTSCHEN BUNDESTAG

SOCIAL BOTS – DIE POTENZIELLEN MEINUNGSMACHER

TAB-Fokus Nr. 16 zum Horizon-Scanning Nr. 3 April 2017

In Kürze

- Social Bots werden im Wesentlichen dafür eingesetzt, Diskussionen inhaltlich zu verzerren sowie die Bedeutung von Themen oder die Popularität von Personen und Produkten zu beeinflussen.
- Sie bergen das Potenzial, die politische Debattenkultur im Internet durch die massenhafte Verbreitung von (Falsch-)Nachrichten zu verändern und durch eine »Klimavergiftung« das Vertrauen in die Demokratie zu untergraben.
- Das noch junge Phänomen Social Bots wurde bislang insbesondere auf der Plattform Twitter nachgewiesen. Die tatsächliche Wirkung auf die (politische) Willensbildung ist bislang kaum belegt.
- Die technischen Enttarnungsmöglichkeiten hinken der schnellen Weiterentwicklung der Social Bots hinterher.

Worum es geht

Soziale Medien erfreuen sich als Nachrichtenquelle wachsender Beliebtheit. Doch nicht nur Menschen posten dort Beiträge. Seit geraumer Zeit übernehmen dies auch Social Bots. Bei diesen handelt es sich um Computerprogramme, die darauf ausgerichtet sind, in sozialen Netzwerken wie Facebook oder Twitter Beiträge zu generieren, um Diskurse zu beeinflussen bzw. zu manipulieren. Sie können sinnvolle Texte (z. B. Kommentare, Antworten oder Meinungsäußerungen) erzeugen, die von Menschen geschriebenen Texten ähneln. Es ist selten offensichtlich, dass die Beiträge nicht von einem Menschen, sondern von einer Maschine stammen.

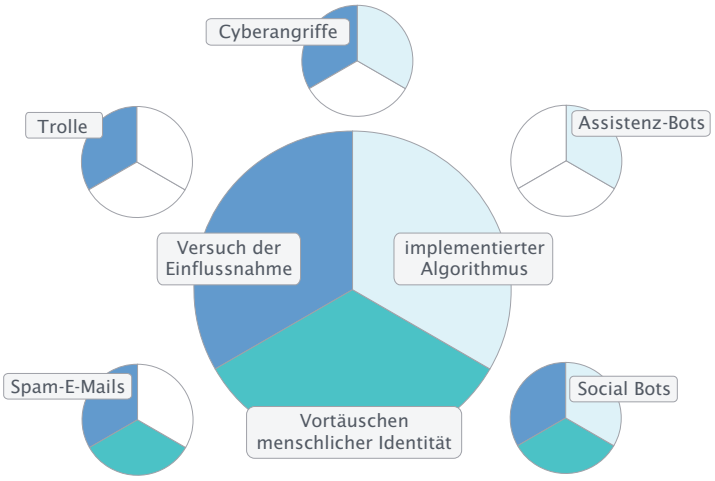
Die Aufdeckung von Fakeaccounts von Social Bots, d. h. gefälschten Nutzerprofilen, hinter denen keine authentischen Personen stehen, wird dadurch erschwert, dass für diese reale Nutzernamen und persönliche Informationen (Bilder, Links) realer Nutzer übernommen werden. Solche Fakeaccounts lassen sich leicht vervielfachen, sodass beispielsweise auf Twitter tausende Benutzerkonten geschaffen werden können, die wiederum zehntausende Tweets pro Tag erzeugen. Es wird vermutet und ist teilweise auch belegt, dass Social Bots sowohl von Staaten als auch von Unternehmen und Interessengruppen gezielt eingesetzt werden.

Eigenschaften von Social Bots

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

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

Abb. 1 Abgrenzung verschiedener Internetphänomene



Social Bots unterscheiden sich von Assistenz-Bots (z. B. Chat-Bots, digitale Assistenten) vor allem hinsichtlich ih-

Auftraggeber und Themeninitiative
Ausschuss für Bildung, Forschung und Technikfolgenabschätzung
+49 30 227-32861
bildungundforschung@bundestag.de

ISSN-Print 2364-2610 | ISSN-Internet 2364-2629

rer Zielsetzung, während ihre technischen Grundlagen verwandt sind. Der Zweck von Assistenz-Bots besteht beispielsweise darin, automatisierte Meldungen wie Wetternachrichten oder Unwetterwarnungen zu versenden.

Mit Blick auf die Internetphänomene Trolle (als menschliche Akteure) sowie Spam-E-Mails haben diese mit Social Bots die Zielsetzung der Manipulation oder Desinformation gemein. Mit Cyberangriffen eint Social Bots deren technische Basis und ebenfalls die Zielsetzung der Einflussnahme.

Social Bots können je nach technischer Entwicklungsstufe eine menschliche Identität unterschiedlich gut vortäuschen. Einfache Social Bots erkennen Schlüsselbegriffe, wie z. B. Refugees, und reagieren darauf, indem sie Bilder aus dem Internet posten oder Kommentare retweeten. Einige imitieren das Verhalten menschlicher Nutzer, indem sie zu unterschiedlichen Tageszeiten einen unterschiedlichen Grad an Aktivität vortäuschen. Komplexere Social Bots können Kommunikationsinhalte analysieren und Dialoge führen. Zurzeit dominieren einfache Social Bots im Internet.

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

In den nächsten Jahren sind erhebliche Entwicklungssprünge im Bereich der Bot-Technologie zu erwarten. Die technologische Reife der Social Bots wird von den Fortschritten in den Bereichen künstliche Intelligenz, Machine Learning und Big Data profitieren. Social Bots werden deshalb zukünftig noch menschenähnlicher agieren können und schwieriger zu enttarnen sein. Technische Möglichkeiten ihrer Enttarnung folgen dieser Entwicklung, haben jedoch – analog zu Antivirensoftware – immer einen zeitlichen Rückstand.

Einfluss und Wirksamkeit von Social Bots

Es gibt lediglich eine begrenzte Anzahl prominenter Beispiele der Einflussnahme durch Social Bots, auf die sowohl in der Presse als auch in wissenschaftlichen Artikeln immer wieder Bezug genommen wird. Die drei am häufigsten in der Presse und Literatur genannten Beispiele sind Social-Bot-Einsätze während der Protestbewegung in der Ukraine, im Verlauf der Brexit-Kampagne sowie im US-Präsidentschaftswahlkampf 2016.

Social Bots wurden bislang in erster Linie auf Twitter nachgewiesen, das eine für Programmierer leicht zugängliche technische Schnittstelle anbietet. Bisher gab es noch keine wissenschaftlichen Studien, in denen der Nachweis erbracht wurde, dass die Beeinflussung von gesellschaftlichen Gruppen durch Social Bots tatsächlich gelingt. Das Ausmaß der tatsächlichen Einflussnahme ist daher kaum belegt.

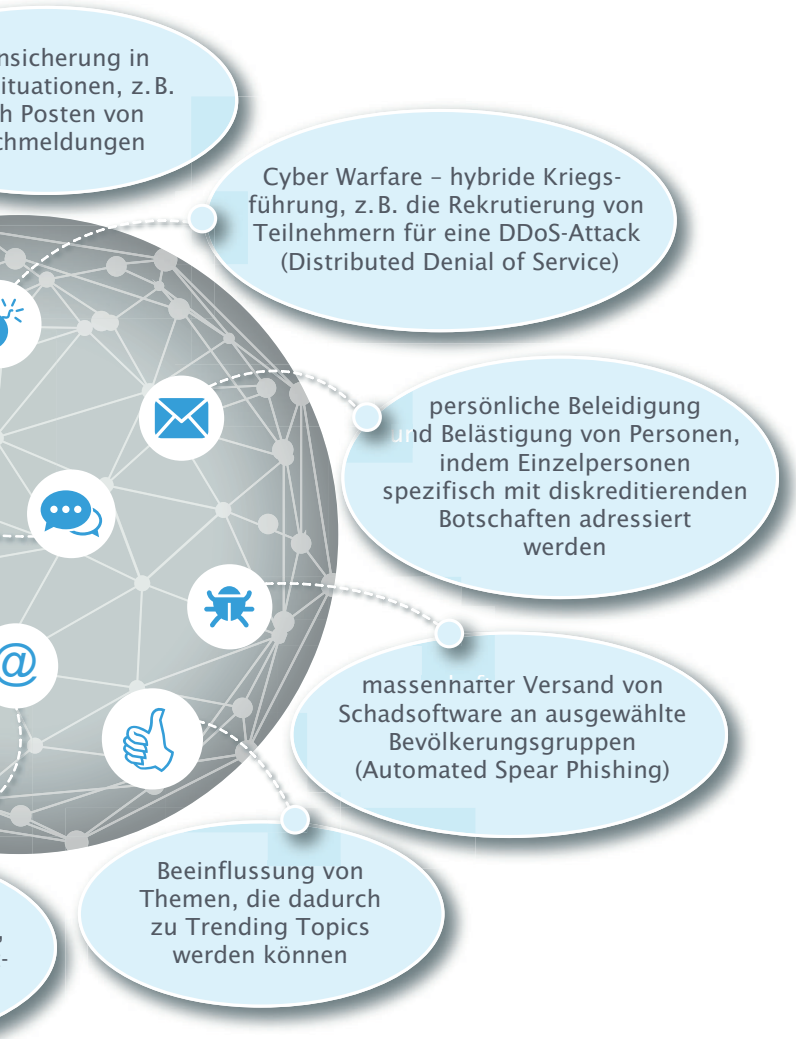
Wesentliche Einsatzgebiete für Social Bots sind bislang Wahlkämpfe, Proteste oder der Versuch, politische Strömungen zu beeinflussen (Abb. 2). Dabei werden die Social Bots für vier Ziele eingesetzt:

Abb. 2 Mögliche Wirkungsbereiche von Social Bots

- für das Ersticken oppositioneller Gegenmeinungen durch das Fluten von Hashtags mit ablenkenden, polarisierenden oder banalen Nachrichten,
- zur Verbreitung von Propaganda und Meinungsmache,
- für das künstliche Erzeugen hoher Followerzahlen auf Twitter, die die Bedeutung der eigenen Position unterstreichen sollen,
- zur Diskreditierung, Beleidigung oder Verführung von Personen zum Kauf von entgeltpflichtigen Diensten im Internet.

Icons: designed by Freepik

Potenziell einflussreich scheinen Social Bots im Zusammenhang mit politischen Kulminationspunkten zu sein, wenn es in politischen Entscheidungsprozessen um knappe Mehrheiten geht, so wie dies im Wahlkampf zwischen Hillary Clinton und Donald Trump oder bei der Brexit-Kampagne zu beobachten war. Fernsehduelle im Wahlkampf bieten einen Anlass, um währenddessen oder unmittelbar im Anschluss an die Sendungen per Social Bots Meinungen zu verbreiten.



Zukünftige Einflusspotenziale und Einsatzmöglichkeiten von Social Bots

Das Potenzial von Social Bots in Bezug auf **politische Prozesse** wird von Experten überwiegend hoch bewertet. Social Bots können dafür genutzt werden, Nachrichten im Internet zu verbreiten, um so Trends zu manipulieren oder politische Debatten und Diskurse zu beeinflussen. Besonderes Gefahrenpotenzial besteht, wenn Social Bots massenhaft Falschnachrichten in Krisensituationen, z. B. nach Anschlägen, verbreiten. So können Social Bots zur Veränderung der politischen Debattenkultur im Internet beitragen und zu Desinformation und zur »Klimavergiftung« im öffentlichen Diskurs führen.

Ein weiterer Einflussbereich von Social Bots sind **wirtschaftliche Prozesse**. Social Bots bergen das Potenzial, das Kunden- und Kaufverhalten Einzelner (über das sogenannte Influencer Marketing) zu beeinflussen und sogar ganze Märkte wie den Börsenhandel zu manipulieren.

Mit Blick auf die **IT-Sicherheit** im Kontext von Industrie 4.0, dem Internet of Things und der damit verbundenen Zunahme vernetzter Geräte scheint eine Gefährdung durch Social Bots aktuell noch unwahrscheinlich, weil Social Bots Hard- oder Software von IT-Systemen nicht direkt angreifen. Vor dem Hintergrund der rasanten Entwicklungen und der immer intelligenter werdenden Geräte einerseits und der zukünftigen Fähigkeiten von (Social) Bots andererseits ist ein zukünftiges Risiko, wie z. B. das Kapern von Geräten für schadhafte Zwecke, nur schwer abzuschätzen. Social Bots können insbesondere dann eine Gefahr für die IT-Sicherheit darstellen, wenn sie den Menschen als potenzielle Schwachstelle der IT-Sicherheit ins Visier nehmen und diesen für Angriffe instrumentalisieren (z. B. durch Versenden von Links, über die Schadsoftware installiert wird).

Die **Geschäftsmodelle sozialer Netzwerke** basieren überwiegend auf dem Verkauf von Werbung und/oder von Nutzerdaten. Diese Modelle funktioniert nur dann, wenn Menschen auf den Plattformen agieren und schließlich Kaufentscheidungen treffen. Social Bots stellen langfristig eine Bedrohung für das Geschäftsmodell sozialer Netzwerke dar. Ein Teil der Nutzer könnte sich abwenden, weil sie das Vertrauen in die Echtheit der Beiträge verlieren, und Investoren könnten sich zurückziehen.

Der Einsatz von Social Bots muss nicht per se mit negativen Absichten verbunden sein. Zu den **positiven Einsatzmöglichkeiten** zählen künstlerisch-kreative Anwendungen sowie Ansätze, sie als Lockvogel oder als Gegenmaßnahme (sogenannte Counter-Speech-Kampagnen) zur Bekämpfung von Falschnachrichten einzusetzen. Ferner könnten sie für eine positive Beeinflussung menschlichen Verhaltens (Nudging) eingesetzt werden. Im letzteren Fall wäre dies jedoch nur ethisch unbedenklich, wenn die Prinzipien der informationellen Selbstbestimmung berücksichtigt würden.

Handlungsoptionen

Die bisher vorliegenden Erkenntnisse legen nahe, dass für einen souveränen Umgang mit Propaganda- oder Falschmeldungen das Wissen um die Qualität und Zuverlässigkeit von Quellen einerseits sowie Grundkenntnisse informationstechnischer Zusammenhänge andererseits entscheidend

sind. **Kinder, Jugendliche und auch Erwachsene** sollten **in ihrer Medienkompetenz** im Sinne einer Digital Literacy **gestärkt werden**. Ein grundlegendes Verständnis informationstechnischer Funktionsweisen und Zusammenhänge – etwa dazu, wie Nachrichten zum Trend werden – sollte unbedingt in der schulischen Ausbildung vermittelt werden. Ob das Thema Social Bots in einem größeren Rahmen zur richtigen Nutzung vernetzt-digitaler und sozialer Medien edukativ behandelt werden kann oder spezifisch adressiert werden muss, wäre zu klären.

Eine besondere Zielgruppe entsprechender Maßnahmen sind auch **Journalisten**, da sie **als Multiplikatoren** zu großer Sorgfalt bei der Auswahl ihrer Quellen verpflichtet sind. Auch etablierte Medien greifen zunehmend auf Inhalte aus sozialen Medien zurück und orientieren sich bei der Bewertung der Relevanz von Themen und Nachrichten an diesen. Aufgrund der leichten Manipulierbarkeit sollten sich Journalisten nicht allein auf die in sozialen Medien gebräuchlichen Indikatoren, wie z. B. die Anzahl der Retweets, stützen, sondern diese Quellen – ähnlich wie bei der Bewertung von Bildmaterial – auf Glaubwürdigkeit und Echtheit hin prüfen.

Der bestehende Rechtsrahmen bietet keine Handhabe, um Social Bots und deren manipulativen Einsatz zu unterbinden. Eine **Kennzeichnungspflicht von Bots** erscheint zum jetzigen Zeitpunkt u. a. aufgrund der Schwierigkeiten bei der zuverlässigen Detektion von Bots, mangelnder Sanktionierungsmöglichkeiten sowie von Konflikten mit dem Datenschutz eher ungeeignet. Stattdessen müssten sich die **sozialen Medien stärker selbstverpflichten** und Maßnahmen gegen die Verbreitung von Social Bots auf ihren Plattformen umsetzen. Bei rechtswidrigen Praktiken durch Social Bots wäre zu erwägen, die Auftraggeber oder Programmierer strafrechtlich zu belangen. Nur in Ausnahmefällen dürfte es möglich sein, die international und von Drittländern aus agierenden Initiatoren von Social Bots zu identifizieren. Durch **Selbstverpflichtungen von Unternehmen und zivilgesellschaftlichen Organisationen** wäre es möglich, zumindest einer weiteren Verbreitung von Social Bots Einhalt zu gebieten.

Wenngleich die Entwicklung von **Enttarnungssystemen** unerlässlich ist, ist gegenwärtig keine definitive technische Lösung des Problems in Sicht. Da Social Bots zum weit überwiegenden Teil im Kurznachrichtendienst Twitter eingesetzt werden, der sich neben der auch maschinell gut generierbaren einfachen, inhaltlichen Nachrichtenstruktur durch eine leicht ansteuerbare Schnittstelle (Application Programming Interface [API]) auszeichnet, stellt diese einen möglichen Abwehrmechanismus gegen Social Bots dar. So gibt es Überlegungen, dass an der Schnittstelle eine Identifikation des zugreifenden Algorithmus erfolgt. Auf diese Weise könnte ermittelt werden, wie der Algorithmus funktioniert, was er bewirkt etc. Durch eine derartige Maßnahme würde nur erwünschten Algorithmen der Zugang gewährt, während unerwünschte Algorithmen abgeblockt werden könnten. Ob ein solcher Mechanismus jedoch tatsächlich wirksam sein kann und eine Chance auf Realisierung hat, wird auch in Expertenkreisen angezweifelt.

Die Beschäftigung mit dem noch recht jungen Phänomen Social Bots zeigt, dass noch viele Fragen offen sind. In den seltensten Fällen konnte eine direkte Wirkung der Social Bots und ihrer Nachrichten nachgewiesen werden. Um eine umfassende Klärung und Einschätzung des Gefährdungspotenzials, der technischen und rechtlichen Herausforderungen zu ermöglichen, sind **weitere Forschungen und investigative Ermittlungen** nötig. Nur mit einer erweiterten Wissensbasis kann die Frage beantwortet werden, ob Social Bots potenziell demokratiegefährdend oder nur eine lästige Randerscheinung sind.

Horizon-Scanning Nr. 3
Social Bots
Sonja Kind, Tobias Jetzke, Sebastian Weide, Simone Ehrenberg-Silies, Marc Bovenschulte

Projektinformation
www.tab-beim-bundestag.de/de/untersuchungen/uV005.html

Projektleitung und Kontakt
Dr. Sonja Kind
+49 30 310078-283
sonja.kind@vdivde-it.de

Das Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag (TAB) ist eine selbstständige wissenschaftliche Einrichtung, die den Deutschen Bundestag und seine Ausschüsse in Fragen des wissenschaftlich-technischen Wandels berät. Das TAB wird seit 1990 vom Institut für Technikfolgenabschätzung und Systemanalyse (ITAS) des Karlsruher Instituts für Technologie (KIT) betrieben. Hierbei kooperiert es seit September 2013 mit dem Helmholtz-Zentrum für Umweltforschung GmbH – UFZ, dem IZT – Institut für Zukunftsstudien und Technologiebewertung gGmbH sowie der VDI/VDE Innovation + Technik GmbH. Der Ausschuss für Bildung, Forschung und Technikfolgenabschätzung entscheidet über das Arbeitsprogramm des TAB, das sich auch aus Themeninitiativen anderer Fachausschüsse ergibt. Die ständige »Berichterstattergruppe für TA«, besteht aus je einem Mitglied der Fraktionen: Dr. Philipp Lengsfeld (CDU/CSU), René Röspel (SPD), Ralph Lenkert (Die Linke), Harald Ebner (Bündnis 90/Die Grünen) und der Ausschussvorsitzenden, Patricia Lips (CDU/CSU).