Social Bots

Das Phänomen der Social Bots ist noch recht jung. Die Aktivitäten von Social Bots sind insbesondere auf der Plattform Twitter nachzuweisen, ihre Wirkungen auf die (politische) Willensbildung sind jedoch noch kaum bekannt, geschweige denn belegt. Gleichwohl wird Social Bots ein durchaus schadhaftes oder sogar gefährliches Einflusspotenzial unterstellt. Das TAB hat durch seinen Konsortialpartner VDI/VDE-IT im Zeitraum von Oktober bis März 2017 eine TA-Vorstudie zum Thema Social Bots erarbeitet. Im Mittelpunkt stand die Frage nach der Wirkungskraft von Social Bots und den daraus resultierenden möglichen Gefahren für die Gesellschaft, zum Beispiel durch die Manipulation politischer Diskussionen in sozialen Netzwerken oder durch die Beeinflussung des Kaufverhaltens von Konsumenten.

Ziel war es, einen Überblick über den aktuellen Stand der Technik von Social Bots, deren Anwendungsfelder, Anwender und Verbreitung sowie zu den angenommenen und tatsächlichen Risiken dieser Computerprogramme zu erarbeiten. Grundlage bildeten eine Literatur- und Quellenanalyse sowie 24 Experteninterviews mit Fachleuten aus sechs Bereichen: Wissenschaft, Verwaltung, zivilgesellschaftliche Organisationen, Parteien (Social-Media-Beauftragte), Presse/Medien sowie Wirtschaft. Auf dieser Basis wurden Thesen erarbeitet, die in einem öffentlichen Fachgespräch am 26. Januar 2017 im Bundestag diskutiert und validiert wurden.

Was sind Social Bots

Social Bots sind Computerprogramme, die darauf ausgerichtet sind, in sozialen Netzwerken (Facebook, Twitter etc.) Beiträge wie Kommentare, Fragen, Antworten oder Meinungsäußerungen automatisch zu generieren, um Diskurse zu beeinflussen oder gar zu manipulieren. Dabei agieren sie menschenähnlich: Social Bots sind in der Lage, sinnreiche Texte zu erzeugen, die den von Menschen geschriebenen Inhalten ähneln. Sie können Konversationen führen, indem sie auf passende Inhalte aus dem Internet zurückgreifen. Um menschliches Verhalten zu imitieren, sind Social Bots vielseitig und agieren beispielsweise nicht nur politisch, sondern veröffentlichen auch mehr oder weniger Belangloses, etwa Kommentare zu Fußballergebnissen. Auch täuschen sie je nach Tageszeit einen unterschiedlichen Grad an Aktivität vor oder imitieren die Identitäten von realen Nutzern, indem sie realistische Nutzernamen und/oder personenbezogene Informationen wie Bilder oder Links für sich verwenden. Für Internetnutzer ist es selten offensichtlich, dass Beiträge von Social Bots nicht von einem Menschen, sondern von einer Maschine stammen.

Aktionsspielräume

Social Bots werden momentan vorrangig dafür eingesetzt, Diskussionen inhaltlich zu verzerren sowie die Wichtigkeit von Themen oder die Popularität von Personen und Produkten zu beeinflussen. Social Bots wurden bisher in erster Linie auf der Plattform des Kurznachrichtendienstes Twitter nachgewiesen, die eine für Programmierer leicht zugängliche technische Schnittstelle anbietet. Nach Experteneinschätzung bergen Social Bots das Potenzial, die politische Debattenkultur im Internet durch die massenhafte Verbreitung von (Falsch-)Meldungen zu verändern und durch eine »Klimavergiftung« das Vertrauen in die Demokratie zu unterlaufen. Eine wichtige Voraussetzung für den Einfluss von Social Bots auf politische Entscheidungsprozesse sind Kulminationspunkte wie etwa eine knappe Entscheidung bei Wahlen. Über die politische Einflussnahme hinaus bergen Social Bots das Potenzial, das Kaufverhalten von Personen zu manipulieren. Die technischen Möglichkeiten zur Enttarnung von Social Bots sind noch im Entwicklungsstadium und hinken der schnellen Entwicklung von Bots hinterher.

Charakteristische Merkmale 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:

- 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.

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.

Bislang gezeigter Einfluss und Wirkungen

Es gibt lediglich eine Handvoll prominenter Beispiele, in denen Social Bots mit dem Ziel der politischen Meinungsbeeinflussung eingesetzt wurden. Die drei am häufigsten in der Presse und wissenschaftlichen Literatur genannten Beispiele sind Social-Bot-Einsätze während der Protestbewegung in der Ukraine, im Verlauf der Brexit-Kampagne sowie im US-Präsidentschaftswahlkampf 2016.

Dabei wurden Social Bots im Wesentlichen für vier Ziele eingesetzt:

- 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 oder Beleidigung von Personen.

Bisher gibt 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 noch unbekannt.

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.

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. Darüber hinaus stellen Social Bots langfristig eine Bedrohung für das Geschäftsmodell von sozialen Netzwerken dar. Diese basieren überwiegend auf dem Verkauf von Werbung und/oder Nutzerdaten und funktionieren nur, wenn Menschen die Plattformen rege benutzen und dadurch beeinflusst Kaufentscheidungen treffen. Ein Teil der Nutzer könnte sich abwenden, weil sie das Vertrauen in die Echtheit der Beiträge verlieren, und Investoren könnten sich zurückziehen.

Handlungsoptionen

Eine Handlungsoption zur Eindämmung der Bedrohung durch Social Bots besteht in der Stärkung der Medien- und informationstechnischen Kompetenz von Kindern und Erwachsenen. Kinder, Jugendliche, aber 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 in der schulischen Ausbildung vermittelt werden. Eine besondere Zielgruppe entsprechender Maßnahmen sind auch (angehende) Journalisten, da sie als Multiplikatoren zu großer Sorgfalt bei der Auswahl ihrer Quellen verpflichtet sind.

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 problematisch. Stattdessen müssten sich die Anbieter von sozialen Medien stärker selbst verpflichten und Maßnahmen gegen die Verbreitung von Social Bots auf ihren Plattformen umsetzen. 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 derzeit keine technische Lösung des Problems in Sicht. Social Bots nutzen gegenwärtig zum weit überwiegenden Teil den Kurznachrichtendienst Twitter, der sich neben der auch maschinell gut generierbaren einfachen Nachrichtenstruktur durch eine leicht ansteuerbare Schnittstelle (Application Programming Interface [API]) auszeichnet. Diese Eigenschaften bieten zugleich aber auch mögliche Ansatzpunkte für Abwehrmechanismen gegen Social Bots. 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. Dadurch könnte nur erwünschten Algorithmen der Zugang gewährt werden, während unerwünschte Algorithmen geblockt würden. 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. Um eine umfassende Klärung und Einschätzung des Gefährdungspotenzials sowie der technischen und rechtlichen Herausforderungen zu ermöglichen, sind weitere Forschungsarbeit und investigative Ermittlungen gegen die Urheber von Social Bots nötig.

Die TA-Vorstudie »Social Bots« wurde im März 2017 abgeschlossen und wird in Kürze durch den ABFTA als Horizon-Scanning Nr. 3 veröffentlicht.

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