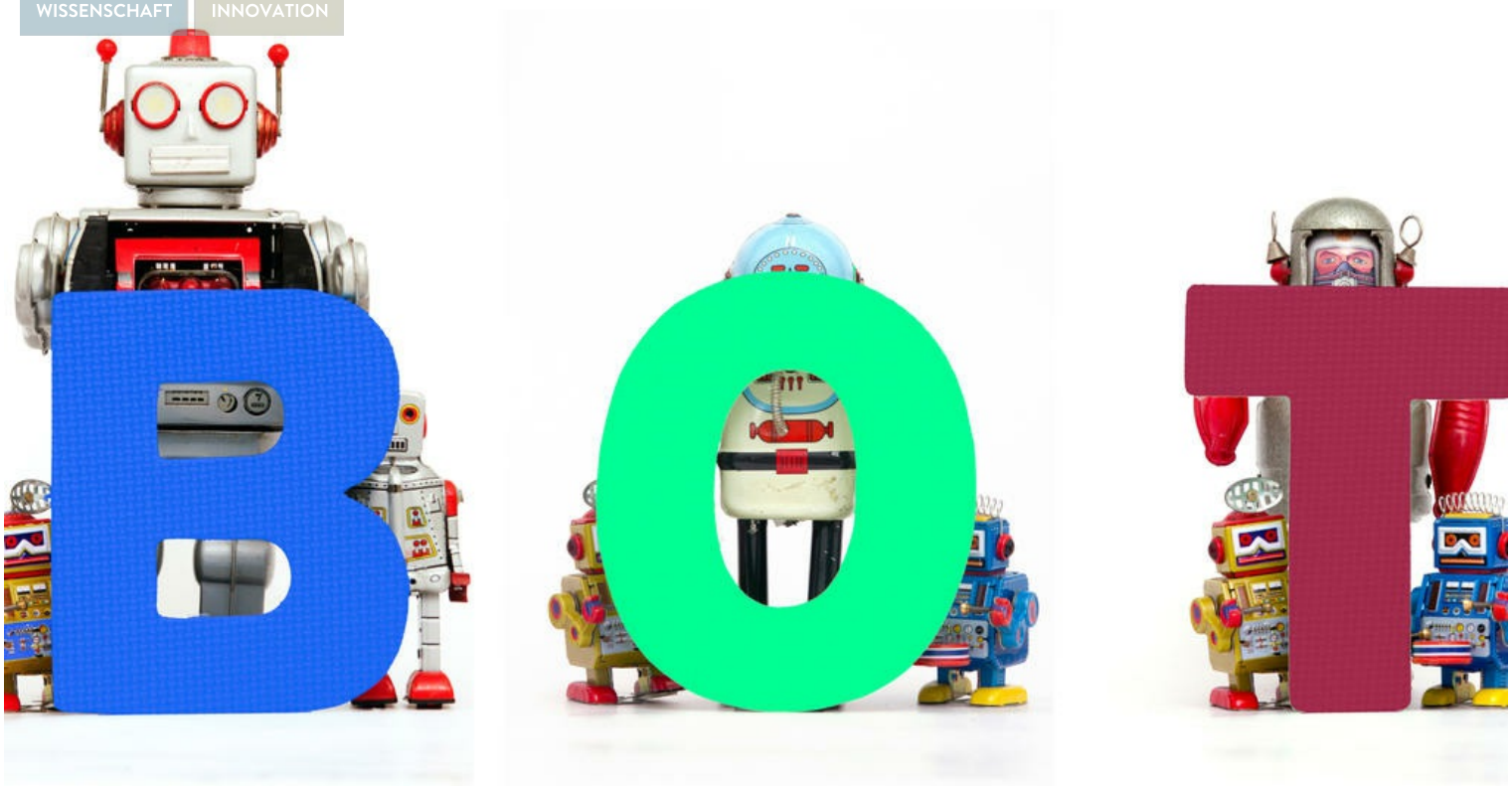
MERTON
Onlinemagazin des *Stifterverbandes*

WISSENSCHAFT INNOVATION



BOT Roboter (Foto: iStock/charles taylor)

Falsche BOT-schaften

VERÖFFENTLICHT AM 06.07.2017

Social Bots, intelligente Computerprogramme, die vorgeben, echte Nutzer zu sein, verzerren das öffentliche Meinungsbild in sozialen Medien. Verschiedene Forschungsprojekte untersuchen, wie gefährlich diese künstlichen Intelligenzen (KI) wirklich sind. Ein Wettbewerb an der TU München will ihnen nun das Handwerk legen.

LESEZEIT: 6 MINUTEN

TEXT:
ALEXANDRA STRAUSH ›

„Politisches Direktmarketing“ nannten Donald Trumps kreative Helfer ihre neue Methode im Onlinewahlkampf: Verschiedene Nutzer erhielten über die Plattform Twitter genau die Information, die sie brauchten, um in Trump den richtigen Mann an der Spitze der Vereinigten Staaten zu sehen. Potenzielle Wähler mit Vorbehalten gegen Muslime bekamen Beiträge zum harten Kurs des Republikaners gegenüber dieser Minderheit zu lesen. Und wer um seinen Arbeitsplatz bangte, konnte auf seinem Smartphone lesen, dass Trump 25 Millionen neue Jobs schaffen würde.

Möglich wurde diese Strategie durch sogenannte Social Bots, intelligente Computerprogramme, die automatisiert im Internet die Meinung ihres Erschaffers verbreiten. Amerikanische Forscher haben bewiesen, dass im US-Präsidentschaftswahlkampf 2016 rund 400.000 Social Bots für ein Fünftel der Twitter-Beiträge zum Thema verantwortlich waren. Ob sie am Ende die Entscheidung an der Urne beeinflusst haben, kann niemand sagen. Aber allein der massenhafte Einsatz dieser elektronischen Meinungsmacher beunruhigt Politiker und Netzbeobachter.

Doch was oder wer steckt eigentlich hinter diesen Social Bots, kurz für Social Robots? Es sind Programme, die automatisch ein oder mehrere Benutzerkonten in sozialen Medien wie Twitter oder Facebook steuern und sich so nach vorher erlernten Regeln zu Wort melden. Dahinter kann ein harmloser Spaß stehen, so wie bei der „**Pfannkuchenpolizei**“, einem Bot, der automatisch auf das Wort „Berliner“ in Tweets reagiert. Er korrigiert die Nutzer, dass das beliebte Gebäck in Berlin Pfannkuchen heißt. Aber häufig stehen hinter diesen Bots eben auch handfeste Interessen: eine Firma, die versteckt Werbung für ihre Produkte platziert, oder eine politische Gruppe, die das öffentliche Meinungsbild beeinflussen will. Der Arabische Frühling wurde von massiver Bot-Diskussion im Netz begleitet. Und die von Edward Snowdon veröffentlichten internen Papiere belegen, dass auch der US-Geheimdienst NSA sich mit den Einsatzmöglichkeiten von falschen, virtuellen Identitäten befasst hat.

RAFFINIERTE TARNUNG

Nun wäre der eine oder andere Roboterbeitrag auf Twitter sicher genauso gut zu ertragen wie die tägliche Spam-Mail im eigenen Postfach. Aber im Gegensatz zur virtuellen Tamara oder Susan, die gerne einen netten Mann kennenlernen möchte, ist die Tarnung von fortgeschrittenen Social Bots viel raffinierter. Simon Hegelich, Professor für Political Data Science an der Hochschule für Politik an der TU München, hat in einem Forschungsprojekt ein Netzwerk von 80 Social Bots in der Ukraine entdeckt. Scheinbar authentische User inklusive Foto chatten miteinander oder reagieren auf Beiträge von echten Nutzern. Zwischen Fußballnachrichten, sexistischen Witzen und Tipps zu illegalen Downloads streuten die computergenerierten Accounts im Februar 2014 auch immer wieder handfeste politische Kommentare zum Sturz von Präsident Wiktor Janukowitsch ein. Social Bots dieser Art sind komplex programmiert: Sie greifen nicht nur standardisiert auf Inhalte zurück, die in Datenbanken hinterlegt sind, sondern lernen aus dem Verhalten echter Nutzer und passen sich ihm an. Wer hinter diesen Meinungsmaschinen steht, können die Forscher nicht genau sagen. „Es ist sehr einfach, sich im Internet eine falsche Identität zuzulegen“, meint Hegelich. Auch massenhaft: Für 500 Dollar könne man in den USA 10.000 gefälschte Twitteraccounts kaufen, für weitere 500 Dollar die Software, die sie steuert. Die Köpfe hinter den Robotern, auch Botmaster genannt, bleiben anonym.

Simon Hegelich (Foto: Uni Siegen)

Simon Hegelich, Professor für Political Data Science in München

Aber zumindest den Bots selbst können Forscher und Programmierer auf die Schliche kommen. Einfache Faustregeln reichen dazu inzwischen nicht mehr aus. Zum Beispiel die Masse der geposteten Beiträge oder die Eigenschaft von Fake-Accounts, sich in Netzwerken um viele Freunde zu bemühen, aber meist keine

Follower zu haben. Die Bots haben dazugelernt: Sie posten nur noch sparsam, um von den Betreibern der sozialen Netzwerke nicht geblockt zu werden. Und sie folgen sich gegenseitig. Aber in jedem Tweet steckten neben dem geposteten Text bis zu 1.400 zusätzliche Variablen, erklärt Simon Hegelich. Diese könne man mit digitalen Verfahren der Mustererkennung untersuchen. Er selbst habe zum Beispiel die Erfahrung gemacht, dass ein Computer anhand der Farbwerte ein aus dem Internet geklautes Profilbild von einem echten, mit dem Smartphone aufgenommenen unterscheiden könne. Eine ähnliche Aufgabe stellt die TU München jetzt im Rahmen der Munich Bot Challenge (siehe Kasten): Programmierer, Wissenschaftler oder interessierte Laien sollen automatisierte Verfahren zur Bot-Erkennung entwickeln. Zwar habe die Indiana University mit BotOrNot schon ein weitverbreitetes Werkzeug zur Verfügung gestellt – aber da es sprachbasiert sei, sagt Hegelich, funktioniere es für deutsche Twitteraccounts nur mäßig. Von der Munich Bot Challenge versprechen sich die Initiatoren neue Ansätze zur Bot-Enttarnung, die in Zukunft vielleicht einmal in eine Art Filterlösung für soziale Netzwerke einfließen könnten. Ein genereller Ausschluss von Fake-Accounts bleibt jedoch problematisch. „Es gibt keinen Beweis, dass ein Bot ein Bot ist“, sagt Hegelich. „Wir sprechen immer nur von Wahrscheinlichkeiten.“

MUNICH BOT CHALLENGE

Social Bots im Netz auf die Spur kommen: Wettbewerb für Jugendliche, Studierende und Videomacher.

INFOS ZUM WETTBEWERB

Wahrscheinlichkeiten prägen auch die öffentliche Diskussion um die Meinungsroboter. Laut einer Onlineumfrage von Mai dieses Jahres durch die Beraterfirma Fittkau & Maaß Consulting befürchten 59 Prozent der 1.200 Teilnehmer, dass durch Social Bots in Zukunft immer öfter Menschen und Entscheidungen manipulieren werden. Forscher bescheinigen den Bots, ideale Propagandamaschinen zu sein, weil sie massenhaft und viel schneller posten als ein Mensch – und weil allein die Masse der Beiträge in sozialen Medien durch Aufmerksamkeit belohnt werden würde. „Sie führen zu Verzerrung bei der Meinungsbildung und im öffentlichen Diskurs, tragen zu Fake News und Desinformation bei“, meint Professor Dirk Helbing von der Eidgenössischen Technischen Hochschule (ETH) Zürich.

Social Bots, so wie sie im US-Wahlkampf eingesetzt wurden, würden zum Filterblaseneffekt beitragen: Jeder liest, sieht und hört nur noch, was er sowieso schon weiß oder glauben will. Die Folge sei Polarisierung, meint Helbing. Der Gesellschaft gehe die gemeinsame Basis und Konsenzfähigkeit verloren. Nicht ganz so dramatisch sieht das Linus Neumann vom Chaos Computer Club. In einem Fachgespräch im Bundestag argumentierte er, dass Social Bots wohl kaum die Ergebnisse der anstehenden Bundestagswahl beeinflussen könnten, wenn es die etablierten Medien seit Jahrzehnten nicht geschafft hätten. Dagegen spräche schon die in Deutschland verhältnismäßig kleine Anzahl der Twitter-Nutzer. Viele Studien, so auch die des Büros für Technikfolgen-Abschätzung des Bundestages, kommen zu dem Ergebnis, dass die Wirkung der Existenz von Social Bots nicht nachweisbar sei. „Aber wir haben auch keinen empirischen Nachweis dafür, dass TV-Werbung wirkt“, gibt Simon Hegelich zu bedenken. „Und trotzdem geben die Auftraggeber sehr viel Geld dafür aus.“

QUELLE: HTTPS://MERTON-MAGAZIN.DE/FALSCHE-BOT-SCHAFTEN