Social Bots

Spätestens seit dem US-Präsidentschaftswahlkampf machen sogenannte Social Bots von sich reden. Gemeinsam mit sogenannten Fake News (Falschnachrichten) sollen sie die Wahl entschieden haben. Doch was steckt genau hinter den Programmen, die auf sozialen Medien in Erscheinung treten? In diesem Dossier werden wir einen Einblick in die Welt der Bots geben und eine Einschätzung der Lage versuchen.

Was sind Social Bots?

Der Begriff „Bot" ist eigentlich eine Kurzform von „Roboter". Grundsätzlich verstehen wir unter Bots Programme, die automatisch sich wiederholende Aufgaben übernehmen, ohne dass sie dafür Kommandos von Benutzer_innen benötigen. Oft ist auch von „Botnetzen" die Rede, wenn mit Malware infizierte PCs gemeint sind, die zum Beispiel zum Versand von Spam genutzt werden. Eine genaue Definition, welche Programme als „Bot" bezeichnet werden und welche nicht, gibt es nicht – hier handelt es sich um sprachliche Konventionen, die sich mit der Zeit eingebürgert haben.

Mit Social Bots sind Bots gemeint, die in sozialen Netzwerken aktiv sind. Das Phänomen ist vor allem auf dem Kurznachrichtendienst Twitter zu beobachten, wo es durch die technischen Begebenheiten und die Öffnung von Entwicklungsschnittstellen (API) relativ einfach ist, Bots einzusetzen. Auch der Fakt, dass es nur eine einzige Art von Accounts gibt und die Begrenzung auf 140 Zeichen sorgen dafür, dass Twitter sich besonders für Bots eignet – es ist technisch viel aufwändiger, ein vollautomatisches Facebook-Profil zu gestalten, während dies auf Twitter sogar mit nur wenigen Programmierkenntnissen funktioniert. Es wird geschätzt, dass 7 Prozent aller Twitter-Accounts Bots sind – die Schätzung ist jedoch enorm schwierig. Wissenschaftler des Londoner University College haben Ende Januar 2017 ein Botnetz ausfindig gemacht, das aus über 350.000 Accounts bestand, die alle ungewöhnlich häufig Zitate aus den „Star Wars"-Filmen getwittert haben. Aktuell scheint dieses Botnetz zu ruhen, aber es könnte theoretisch jederzeit von seinen Erschaffern reaktiviert werden. Im Facebook Messenger bieten bereits einige Firmen Chatbots an, die rudimentären Kundensupport – zum Beispiel Kunden über eine Verspätung eines Fluges informieren – übernehmen können, ähnliche Pläne gibt es auch für WhatsApp. Der Messenger-Dienst Telegram bietet eine Entwicklungsschnittstelle für Bots an.

In sozialen Netzwerken ähneln Bots in ihrem Verhalten oft Menschen. Somit ist die Verwechslungsgefahr groß und es ist nicht immer leicht, zu erkennen, ob der Gegenüber ein Mensch oder eine Maschine ist. Da die Entwicklungen im Bereich der künstlichen Intelligenz mit großen Schritten vorangeht, werden wir in Zukunft mehr Bots sehen, vor allem in der Dienstleistungsbranche (z.B. Support-Chat).

Sind alle Bots gefährlich?

Die meisten bekannten Bots sind nicht gefährlich – vor allem jene, die Dienstleistungen im Facebook Messenger oder ähnlichen Diensten anbieten, sind klar als Bots gekennzeichnet. Somit ist es nicht möglich, sie mit Menschen zu verwechseln. Auch bei Twitter gibt es viele Bots, die auf den ersten Blick als solche zu erkennen sind. Allerdings sind diese kleinen Programmierprojekte oft auch nicht sehr nützlich und für manche Nutzer_innen eher ärgerlich: So gibt es zum Beispiel Twitter-Bots, die nach häufigen Rechtschreibefehlern suchen und die Verfasser_innen der Tweets belehren. Andere Twitter-Bots sind eher artistische Projekte und generieren aus einer vorgefertigten Liste von Satzbauteilen kleine Geschichten in Form von Ein-Satz-Tweets. Andere Bots retweeten Tweets, in denen bestimmte Begriffe vorkommen – ob solche Accounts wirklich einen praktischen Nutzen haben, sei dahingestellt.

Natürlich gibt es auch eine ganze Reihe von Bots, die eher zweifelhafte Ziele verfolgen: Massenhaft angelegte Accounts, die auf den ersten Blick echt wirken sollen, können als Follower gekauft werden. Daneben werden Bots auch zu Werbezwecken eingesetzt, oft versteckt und ohne sich als Bot erkennen zu geben. Ein bekanntes Muster ist die attraktive junge Frau, die sich für ein bestimmtes Thema (z.B. Camping) interessiert und nur darüber twittert und zum Thema retweetet. So wird ein „menschliches“ Interesse und Expertenwissen für ein Thema simuliert. Hat der Account genügend Follower, wird mit Links zu Online-Shops versucht, Geld daraus zu schlagen. Solche Bots sind natürlich nicht per se gefährlich, sie führen unbedarfte User jedoch hinters Licht, weil hier nicht eine menschliche Empfehlung, sondern reine Werbung betrieben wird, die nicht als solche gekennzeichnet wird.

Die Art von Bots, die in letzter Zeit für die meiste Aufmerksamkeit gesorgt hat, sind jedoch jene, die versuchen, politisch Einfluss auszuüben und denen vorgeworfen wird, die Ergebnisse von Wahlen zu manipulieren. Mit diesen Bots werden wir uns in den nächsten Abschnitten genauer beschäftigen.

Politische Einflussnahme

Es gibt verschiedene Methoden, um Social Bots politisch nutzen zu können. Einerseits können die Follower- oder Like-Zahlen eines Accounts unter Zuhilfenahme von Bots relativ einfach nach oben getrieben werden. Bots, die automatisch jeden Tweet eines Kandidaten liken und retweeten, sorgen massenhaft eingesetzt für imposante Zahlen. Eine andere Möglichkeit besteht darin, die Bots auf ein bestimmtes Schlagwort reagieren zu lassen. Klimaleugner in den USA haben beispielsweise einen Bot programmiert, der auf Tweets zum Thema Klimawandel reagiert hat. Wahrscheinlich werden wenige User sich von einem einzigen Satz mit einem Link zu einem Artikel überzeugen lassen. Im Gegensatz zu Bots werden Menschen jedoch müde, können nicht hunderten Usern gleichzeitig schreiben und können nicht den ganzen Tag auf social media verbringen. Bots können außerdem niemals von der gegnerischen Seite überzeugt werden und sind im Vergleich zu anderen Werbeformen sehr billig – der Anreiz, sie im Wahlkampf zu benutzen, ist also sehr groß.

Die Möglichkeiten von Social Bots sind jedoch nicht zu überschätzen: Es ist sehr einfach, einen Bot zu programmieren, der auf bestimmte Stichwörter oder Accounts reagiert und automatisch liked, retweetet oder eine (vordefinierte) Antwort schreibt. Bots, die imstande sind, politische Diskussionen zu führen,

haben jedoch einen sehr hohen Entwicklungsaufwand und sind dementsprechend teuer. Meist werden also relativ „dumme“ Bots eingesetzt, um beispielsweise die Trends bei Twitter zu manipulieren. In einer Zeit, in der jeder Tweet eines Politikers eine potentielle Nachricht ist, beobachten Journalist_innnen Twitter natürlich besonders genau. Somit haben Social Bots das Potential, die Nachrichtenlage zu manipulieren und Schlagzeilen zu generieren, wenn Journalist_innen über die vermeintliche Stimmung auf Twitter schreiben. Natürlich eigenen sich Bots auch hervorragend, um Falschinformationen im Netz zu verbreiten.

USA

Im US-Präsidentschaftswahlkampf 2016 wurden sowohl von republikanischer als auch von demokratischer Seite Social Bots auf Twitter eingesetzt, um Stimmung für den eigenen Kandidaten bzw. die eigene Kandidatin zu machen. Nach der ersten TV-Debatte, bei der sich Hillary Clinton und Donald Trump gegenüberstanden, untersuchte die Oxford University die Tweets, die dazu abgesetzt wurde. Sie kam zu dem – dann doch überraschenden – Ergebnis, dass über ein Drittel der Tweets, die Trump unterstützten, von Bots kamen. Bei Clinton lag die Bot-Quote bei etwas mehr als 22 Prozent. Diese Bots erwecken einerseits den Eindruck, dass es enorm viele Aktivisten gibt, die für ihre Kandidaten twittern und können andererseits durch den gezielten Einsatz von Hashtags die Twittertrends manipulieren. Auch wenn beide Seiten Social Bots als Werbeform eingesetzt haben, könnte es dennoch sein, dass Trump einen Teil seines Wahlerfolges dem Einsatz von Bots zu verdanken hat.

Brexit

Auch das Referendum über den Verbleib des Vereinigten Königreiches in der Europäischen Union war ein heiß umkämpftes Thema auf Twitter und auch hier spielten Bots eine große Rolle. Zumindest, wenn man sich die Zahl der Tweets ansieht. Die Oxford University hat sich 1,5 Millionen Tweets zum Thema Brexit angeschaut und hat festgestellt, dass ein Drittel davon – also eine halbe Million – von weniger als einem Prozent aller Accounts geschrieben wurde. Kein Mensch kann so viele Tweets verfassen, allein die hohe Anzahl der Tweets ließ also eine gewisse Automatisierung vermuten. Auch die beiden aktivsten Accounts waren beide Bots. Wie genau die Verteilung von Bots auf das Leave- bzw. Remain-Lager aussah, ist leider nicht genau bekannt.

Deutschland

Nach der US-Wahl äußerten mehrere Politiker_innen in Deutschland Sorge über Social Bots, Bundeskanzlerin Angela Merkel schlug sogar vor, dass sich alle Parteien darauf einigen sollten, keine Social Bots im kommenden Wahlkampf zu benutzen. Das Projekt „botswatch“ untersucht die Aktivitäten von Bots bei politischen Ereignissen in Deutschland, zum Beispiel bei Diskussionssendungen im Fernsehen. Dabei hat sich gezeigt, dass es bereits deutschsprachige Social Bots gibt, die teilweise zehn Prozent der beteiligten Accounts stellen.

Luxemburg

In Luxemburg gibt es noch keine Berichte über Social Bots. Das wundert auch nicht sehr, denn die Zahl der aktiven Twitternutzer ist im Großherzogtum ziemlich klein. Bis auf Journalist_innen und Politiker_innnen gibt es kaum Menschen, die den Kurznachrichtendienst regelmäßig benutzen. Es würde sich aktuell also wahrscheinlich nicht lohnen, Social Bots als Wahlkampfmaßnahme zu benutzen. Da der Einsatz von Bots auf Facebook um Größenordnungen schwieriger ist, wird der Social Media-Wahlkampf diesbezüglich vorerst wohl noch manuell geführt werden müssen. Durch die Erfolge von Trump und Co. könnten allerdings auch luxemburgische Politiker_innen auf den Geschmack von Twitter kommen – dann wären Social Bots der nächste Schritt.

Gefahren

Die Gefahren von Social Bots, die zur politischen Einflussnahme genutzt werden, sind ganz klar die Manipulation von potentiellen Wähler_innnen. Allerdings dürfen wir nicht vergessen, dass die traditionellen Mittel des Wahlkampfes – Plakate, Flyer, Werbespots, Gadgets – auch eine Form der „Manipulation“ sind. Wir haben uns nur daran gewöhnt, dass es zu Wahlkampfzeiten politische Werbung gibt und haben gelernt, damit umzugehen. Bei Social Bots besteht die Gefahr vor allem darin, dass wir diese Accounts für echte Menschen halten und die Verbreitung von Ansichten falsch einschätzen. Dies ist vor allem bei Hate Speech (Hassrede) gefährlich, da die Hemmschwelle dafür sinkt, wenn wir das Gefühl haben, dass „alle“ so denken. Im Moment sind Social Bots noch relativ rudimentär – wenn sich die Programme weiterentwickeln und zum Beispiel menschenähnlich mit Usern diskutieren können, könnte die Gefahr der Einflussnahme viel größer werden.

Genauso, wie wir bei traditioneller Wahlwerbung die entsprechende Medienkompetenz entwickelt haben, müssen wir auch bei Social Bots lernen, sie zu erkennen und mit den Informationen, die sie verbreiten, umzugehen.

Wie kann ich Social Bots erkennen?

Im Allgemeinen hilft eine kritische Betrachtung jedes Twitter-Accounts, die Informationen, die dieser verteilt, einzuschätzen. Die nachfolgenden Schritte sind also nicht nur dann praktisch, wenn Sie einen Social Bot vermuten, sondern allgemein, wenn Sie einen Twitter-Account auf seine Seriosität einschätzen wollen.

1. Ist der Account vertrauenswürdig?

Lesen Sie einige Tweets des Accounts und beurteilen Sie diese: Sind es extremistische Positionen, wird ein bestimmter Jargon verwendet, lässt sich Hate Speech finden? Desweiteren sollten sie sich anschauen, ob sie Follower des Accounts kennen – dies ist natürlich keine hundertprozentige Sicherheit, gibt ihnen aber einen Anhaltspunkt.

2. Was für ein Profil?

Bots haben oft kein Avatar oder benutzen eins, das sie im Internet geklaut haben – durch eine Bildersuchmaschine können Sie herausfinden, wo das Bild noch überall genutzt wurde. Auch die Profilbeschreibung kann Anhaltspunkte dafür liefern, ob ein Account echt ist oder eine Maschine dahintersteckt. Bots geben oft zufällig ausgewählte Orte in ihrem Profil an – auch dies kann ein Hinweis sein!

3. Wie aktiv ist der Account?

Bots sind oft sehr aktiv und veröffentlichen viele Tweets am Tag, für Projekte wie „botswatch“ liegt die Schwelle bei mindestens 50 Tweets am Tag. Natürlich gibt es auch Menschen, die eine ähnlich starke Aktivität auf dem Netzwerk haben, dies ist jedoch eher die Ausnahme. Wenn der Account noch nicht alt ist und dennoch schon eine hohe Anzahl an Tweets aufweist, ist das ein starkes Indiz für einen Bot. Bots weisen außerdem oft eine sehr hohe Zahl an Retweets und Likes auf, was beides überprüfbar ist.

4. Wie schreibt der Account?

Accounts, die überhaupt nur retweeten, sind sehr wahrscheinlich Bots. Allerdings verraten sich Bots oft durch ihren Sprachstil – ist die Grammatik schief? werden immer die gleichen Begriffe und Phrasen wiederholt? und antwortet der Account sehr schnell? Dann handelt es sich vermutlich um einen Bot!

Zusätzlich zu ihrem Bauchgefühl gibt es mittlerweile auch Dienste, die sie benutzen können, um Bots zu erkennen: das Projekt Bot or Not? Der University of Indiana untersucht einen Twitter-Account auf mehrere Faktoren hin und versucht einzuschätzen, ob es sich bei dem Account um einen Bot oder einen Menschen handelt. Natürlich ist diese Einschätzung nicht immer sehr akkurat (Donald Trump erhält z.B. eine 52prozentige Chance, ein Bot zu sein), aber sie kann einen ersten Hinweis geben.

Fazit

Die Gefahren und die Einflussmöglichkeiten von Social Bots sollten nicht überschätzt werden. Die Verantwortung liegt bei den Betreibern von sozialen Netzwerken – diese sollten falsche Accounts bzw. Accounts, die falsche Tatsachen vorspiegeln, verbannen. Leider haben alle sozialen Netzwerke durch ihre Geschäftsmodelle ein starkes Interesse an hohen Userzahlen, was der Bekämpfung von Fake-Accounts entgegensteht. Die Möglichkeiten der Politik, reglementierend einzugreifen sind eher gering und Expert_innen sehen solche Versuche als mögliche Eingriffe in die Meinungsfreiheit. Eine interessante Idee hatte Kevin Munger von der New York University. Der Forscher entwickelte vier Bots, die User auf rassistische Sprache hinwiesen. In der Folge sanken die rassistischen Kommentare um 27 Prozent am Tag. Allerdings ist fraglich, wie viele Menschen sich von Bots ermahnen lassen wollen – und wie ethisch der Einsatz ist, wenn die „guten" Bots vorgeben, Menschen zu sein.

Wer nicht von Social Bots manipuliert werden will, kann einerseits versuchen, sie zu erkennen – und andererseits seinen gesunden Menschenverstand einsetzen und Informationen und ihre Quellen überprüfen.

Quellen:

- Heinrich Böll Stiftung über Social Bots: https://www.boell.de/de/2017/02/09/social-bots
- Botswatch: http://botswatch.de/
- WDR-Blog über Social Bots im US-Wahlkampf: https://blog.wdr.de/digitalistan/usa-wahlkampf-mit-propaganda-bots-gefaehrdet-demokratie/
- The Rise of social bots: http://cacm.acm.org/magazines/2016/7/204021-the-rise-of-social-bots/fulltext
- Forbes: Do evil – The Business of social media bots: http://www.forbes.com/sites/lutzfinger/2015/02/17/do-evil-the-business-of-social-media-bots/#6080c2b91104
- tagesschau: Nur die AfD will auf „Meinungsroboter" setzen: https://www.tagesschau.de/inland/social-bots-afd-101.html
- Brexit-Bots: https://qz.com/713980/watch-out-for-the-brexit-bots/
- Bot or Not? http://truthy.indiana.edu/botornot/
- Star Wars Botnetz: https://www.heise.de/newsticker/meldung/Forscher-entdecken-riesiges-Twitter-Botnetz-Star-Wars-3604196.html
- Facebook Messenger-Bots: https://blog.hubspot.com/marketing/facebook-bots-guide
- „Gute" Bots: https://www.heise.de/tr/blog/artikel/Die-guten-Chatbots-3492352.html

Bei Fragen bezüglich des Internetbetrugs
oder der Nutzung des Internet im Allgemeinen,
wenden Sie sich bitte an die BEE SECURE Helpline:

BEE SECURE HELPLINE BERATUNG
Tel: 8002 1234

Herausgeber: BEE SECURE · B.P. 707 · L-2017 Luxemburg
Tel.: (+(+352) 247-86427 · Fax.: Fax: (+ 352) 46 41 86
bee-secure@snj.luwww.bee-secure.lu

THE GOVERNMENT OF THE GRAND DUCHY OF LUXEMBOURG
Co-financed by the European Union Connecting Europe Facility