IMPLIKATIONEN AUS DEM EINSATZ VON SOCIAL BOTS FÜR DIE ÖFFENTLICHE MEINUNGSBILDUNG

Lisa Fink

Masterandin, Hochschule Bonn-Rhein-Sieg, Fachbereich Informatik, Fraunhofer Institut für Intelligente Analyse- und Informationssysteme, Abteilung Knowledge Discovery
Hahnbitzenweg 4, 53757 Sankt Augustin, DE
lisa.fink@smail.inf.h-brs.de / lisa.fink@fraunhofer.iais.de

Schlagworte: ***Social Bots, Öffentliche Meinungsbildung, E-Democracy***

Abstract: *Der Beitrag von Social Media zur öffentlichen Meinungsbildung wurde bereits mehrfach untersucht. Von besonderem Interesse waren dabei Social Bots, die als menschliche Nutzer wahrgenommen werden können. Die Analyse von Twitter-Nachrichten zur Landtagswahl in Nordrhein-Westfalen zeigt, dass (1) Social Bots an der öffentlichen Meinungsbildung beteiligt waren, (2) diese vornehmlich Inhalte von «Die Piraten Partei», «DIE LINKE» und «Alternative für Deutschland» verbreiteten und (3) deren Aktivität so gering war, dass eine Manipulation der öffentlichen Meinungsbildung ausgeschlossen werden kann.*

1. Motivation und verwandte Arbeiten

«Social Media» wie Facebook, Twitter und Instagram bieten Nutzern vielfältige Möglichkeiten, miteinander zu kommunizieren, Inhalte einzeln oder gemeinsam zu erstellen, zu bearbeiten und auszutauschen. In Kollektivprojekten, Content Communities, Blogs und Microblogs, sozialen Netzwerken und sozialen virtuellen Welten wird die Kommunikation und Kollaboration der Nutzer gefördert. Der Beitrag von Social Media zur öffentlichen Meinungsbildung wurde in jüngerer Vergangenheit in mehreren Studien untersucht. [Bessi/Ferrara, 2016, Hegelich, 2016, Howard/Kollanyi, 2016, Ferrara et al. 2016, Faas/Sack, 2016; zitiert in: Kind et al. 2017] Von besonderem Interesse war dabei der Einsatz sogenannter «Social Bots», also «[…] Computerprogramme[n], die eine menschliche Identität vortäuschen und zu manipulativen Zwecken eingesetzt werden […].» [Bilton 2014, Fuchs 2016, Woolley 2016, Voss 2016; zitiert in: Kind et al.] Dass Social Bots bereits in der Vergangenheit bei Wahlen und Abstimmungen im Einsatz waren ist mittlerweile gut belegt, die folgenden Beispiele können davon einen Eindruck vermitteln:

- 2010 haben Bots bei den U.S. Midterm Elections bestimmte Kandidaten unterstützt und andere gezielt angegriffen, indem sie tausende Tweets mit Links zu Webseiten verbreiteten, auf denen Falschmeldungen publiziert wurden. [Ferrara et al., 2016] Bei den Special Elections in Massachusetts wurde im selben Jahr ein ähnliches Vorgehen beobachtet. [Ferrara et al., 2016]
- 2016 waren bei der Präsidentschaftswahl in den USA ca. 400’000 Bots aktiv. Sie setzten ca. 3,8 Millionen Twitter-Kurznachrichten ab und hielten damit einen Anteil von 20% an der gesamten politischen Debatte. [Bessi/Ferrara, 2016]
- Während der Protestbewegungen in der Ukraine wurden von 15’000 Twitter-Accounts etwa 60’000 Tweets pro Tag verbreitet, die zwischen Fußball und sexistischen Witzen versteckt auch Propaganda-Nachrichten des «Rechten Sektors» enthielten und gezielt junge, ukrainische Männer ansprechen sollten. [Hegelich, 2016, S. 5]
- Während des EU-Austrittsreferendums in Großbritannien wurden von Bots Twitter-Kurznachrichten abgesetzt, die für einen Austritt Großbritanniens aus der EU warben. [Howard/Kollanyi, 2016]

Darüber hinaus konnte der Einfluss von Bots auch im Zusammenhang mit wirtschaftlichen Ereignissen nachgewiesen werden. So trieb 2014 ein Bot-Netzwerk den Marktwert der bis dato unbekannten, Ein-Mann-Firma «Cynk» derart in die Höhe, dass diese binnen weniger Wochen einen Marktwert von 5 Milliarden US-Dollar erzielte. Der Wert der Aktie stieg von 0.1 US-Dollar auf 20 US-Dollar an. [Fiegerman, 2014]

Auch bei gesellschaftlichen Ereignissen traten Social Bots schon in Erscheinung. So wurden beispielsweise kurz nach dem Anschlag auf den Boston Marathon im Jahr 2013 ungeprüfte Informationen und Gerüchte über den Anschlag durch Social Bots verbreitet. [Ferrara et al., 2016]

Diese Ereignisse mit Beteiligung von Social Bots werfen die Frage auf, inwiefern Social Bots eine Gefahr für die politische, wirtschaftliche und gesellschaftliche Meinungsbildung in Deutschland darstellen. Mit dieser Frage beschäftigte sich auch der Deutsche Bundestag Anfang des Jahres 2017, da befürchtet wurde, dass Social Bots die öffentliche Meinungsbildung bei Wahlen und damit den Wahlausgang beeinflussen, indem sie Diskussionen inhaltlich verzerren und die Wichtigkeit von Themen oder die Popularität von Personen künstlich überhöhen. In zwei Ausschüssen wurden daraufhin Experten zu ihrer Einschätzung der von Social Bots ausgehenden Gefahren befragt. Grundlage für die Diskussion war ein Thesenpapier des Büros für Technikfolgen-Abschätzung beim Deutschen Bundestag, das Social Bots trotz schwacher empirischer Grundlage ein großes Gefahrenpotential zuschreibt: «Social Bots tragen zur Veränderung der politischen Debattenkultur im Internet bei und können durch die massenhafte Verbreitung von (Falsch-)Nachrichten zu einer Desinformation und «Klimavergiftung» im öffentlichen Diskurs führen. Social Bots bergen das Potenzial, das Vertrauen in die Demokratie zu unterlaufen.» [Kind et al., 2017]

2. Fallstudie: Landtagswahlen in Nordrhein-Westfalen

Das folgende Kapitel fasst die Analyseergebnisse der Nachrichten des Kurznachrichtendienstes Twitter zur Landtagswahl in Nordrhein-Westfalen (NRW) zusammen. Ziel der Analyse war es, den Einsatz von Social Bots bei der Landtagswahl in NRW zu untersuchen, um ausgehend davon Implikationen aus dem Einsatz von Social Bots für die öffentliche Meinungsbildung abzuleiten.

2.1. Grundlage der Datenerhebung

Twitter bietet Entwicklern über verschiedene Programmierschnittstellen, sogenannte «Application Programming Interfaces» (kurz API), die Möglichkeit, Tweets und zugehörige User-Daten abzufragen. Die Abfragen der Twitter Search API ermöglichen es unter anderem, nach Tweets mit bestimmten «Hashtags» zu suchen. Ein Hashtag ist ein Schlagwort, das Nachrichten in sozialen Netzwerken klassifiziert. Um Tweets für die Landtagswahl über die Search API sammeln zu können, musste zunächst eine Liste an relevanten Hashtags erstellt werden. Grundlage für die Hashtag-Auswahl waren Wahlslogans, Spitzenkandidaten, Parteinamen, einschlägige Talkshows und Informationsformate der Nachrichtensender ARD, ZDF und WDR sowie die meist verwendeten Hashtags auf Twitter im Vorfeld der Landtagswahl. Auf Basis der identifizierten Hashtags konnten im Zeitraum zwischen dem 5. und 22. Mai täglich automatisiert Abfragen über die Search APIs abgesetzt und insgesamt 341’957 Datensätze mit Informationen zu Tweets und Usern gesammelt werden.

Der Datensatz wurde zunächst dahingehend untersucht, wie sich die Verteilung von Tweets und Retweets im Untersuchungszeitraum darstellt. Mit einem Retweet kann ein User die Tweets eines anderen Users in der Timeline des eigenen Twitterkanals anzeigen lassen und mit einem Kommentar versehen. Die Reichweite eines Tweets kann so über mehrfaches Retweeten im Sinne des Schneeballeffekts deutlich erhöht werden. Die Verteilung war wie erwartet: Das Nachrichtenaufkommen stieg bis zum Wahltag leicht an, erreichte dort seinen absoluten Höhepunkt und fiel danach wieder deutlich ab. Die Anzahl Retweets war an den einzelnen Tagen fast immer größer als die Anzahl Tweets, demzufolge schienen die User zur NRW-Wahl mehr von anderen Usern zu retweeten als Tweets originär zu verfassen. Da die Anzahl Tweets und Retweets sowohl vor, als auch nach dem Wahltag niedriger war als die Anzahl der aktiven User, kann außerdem festgehalten werden, dass das allgemeine Interesse an der Landtagswahl eher gering war.

2.2. Netzwerkanalyse

Charakteristisch für vor allem einfache Social Bots ist, dass sie überwiegend Tweets anderer User retweeten und weitaus seltener eigene Tweets verfassen. Um herauszufinden, ob unter den gesammelten Usern solche sind, die eine hohe Anzahl an Retweets vorweisen und deshalb Social Bots sein könnten, wurde in der Folge das Retweet-Verhalten der User untersucht. Die Ergebnisse wurden in einem Netzwerkgraphen visualisiert, wobei die Punkte einzelne User darstellen. Die gerichteten Linien zwischen zwei Punkten zeigen den Nachrichtenfluss vom Urheber einer Nachricht zu dessen Retweeter.

Abbildung 2–1 zeigt die Ergebnisse der Netzwerkanalyse für die aktivsten fünf Retweeter von Nachrichten zur NRW-Wahl und die Existenz sogenannter «Echokammern». Als Echokammern werden Kommunikationsräume bezeichnet, in denen jene Meinungen besonders laut widerhallen, die zum eigenen Weltbild passen. Sie sind deshalb gefährlich, weil diametrale Ansichten kaum mehr wahrgenommen und reflektiert werden können. Die fünf im Rahmen der Netzwerkanalyse identifizierten Echokammern stellen sich als kreisförmige Ansammlungen von Punkten dar und sind, mit Ausnahme der Echokammern am rechten Bildrand, klar voneinander abgegrenzt. Der Punkt im Zentrum jeder Echokammer repräsentiert einen User, der alle User, die über Linien mit ihm verbunden sind, retweetet. Die zentralen User sind von besonderem Interesse, da sie sich aufgrund der hohen Retweetaktivität als potenzielle Social Bots empfehlen. Ein weiteres Charakteristikum für Social Bots ist ihre Neigung, andere Social Bots zu retweeten. Im Folgenden wird die Echokammer am rechten unteren Bildrand näher untersucht. Ein besonderes Augenmerk wird dabei auf die Frage gelegt, welche NRW-Tweets und politische Inhalte in ihr verbreitet wurden und ob Verbindungen zwischen Usern bestehen, die sich als Social Bots empfehlen.

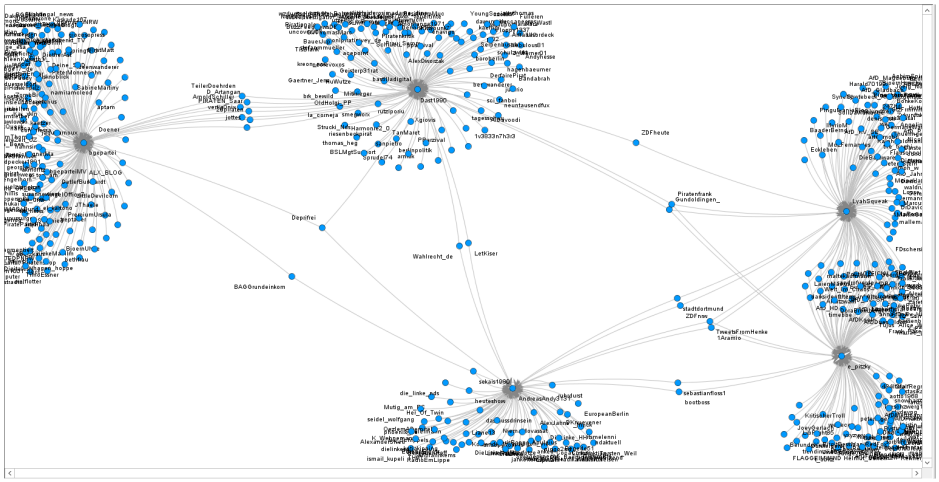

Abbildung 2–1: Netzwerkanalyse top NRW-Retweeter

Im Zentrum der rechten unteren Echokammer steht der User «e_pitzky» (vgl. Abbildung 2–1 unten rechts). Die Parteinamen derjenigen User, deren Inhalte «e_pitzky» retweetete, lassen sich mehrheitlich der Partei «Alternative für Deutschland» zuordnen (vgl. Abbildung 2–2). Der User «Junge_Freiheit», dessen Tweets «e_pitzky» retweetete, wurde im Rahmen einer Analyse des «Project on Computational Propaganda» der Oxford University als Account identifiziert, der als rechtskonservative Zeitung falsche Informationen als Fakten darstellt, der also «Fake News» verbreitet. [Neudert/Kollanyi/Howard, 2017] Betrachtet man den Twitterkanal des Users «e_pitzky» genauer, so fällt auf, dass neben dem hohen Retweetaufkommen weitere Anhaltspunkte dafür existieren, dass es sich bei diesem User-Account um einen Social Bot handeln könnte. So hat «e_pitzky»

in einem Zeitraum von circa zwei Jahren über 96.700 Tweets und Retweets abgesetzt, was durchschnittlich 134 abgesetzten Tweets pro Tag entspricht und die Grenze des «Oxford-Kriteriums» [University of Oxford, 2016] damit um ein Vielfaches überschreitet. Als eines der verbreitesten Kriterien für die Beurteilung der Social-Bot Wahrscheinlichkeit eines Users geht das Oxford-Kriterium davon aus, dass User-Accounts, die (über einen längeren Zeitraum) hinweg durchschnittlich 50 oder mehr (Re-) Tweets täglich veröffentlichen, mit hoher Wahrscheinlichkeit Social Bots sind. [University of Oxford, 2016] Ebenfalls auffällig ist die extrem hohe Anzahl an getätigten «Gefällt mir»-Angaben, denn ca. 58'700 Likes in einem Zeitraum von zwei Jahren sind für einen menschlichen Nutzer mit geregeltem Tagesablauf schwer realisierbar. Während die Anzahl Follower und Freunde eher unauffällig scheint, zeigt das Profilbild kein Bild eines Nutzers, sondern einen Smiley mit verschlossenem Mund. Bilder dieser Art werden als «Stockimages» bezeichnet, sie sind frei zugänglich und oft unentgeltlich nutzbar. Die Verwendung von Stockimages als Profilbild wurde im Rahmen der DARPA Twitter Bot Challenge als ein Indiz für Social Bots genannt. [Subrahmanian et al., 2016]

Die Echokammer des Users «e_pitzky» überschneidet sich mit der des Users «LyahSqueak» (vgl. Abbildung 2–1 rechts oben). Bemerkenswert ist, dass beide Echokammern nicht nur eine Vielzahl von AfD-Partei-Accounts einzelner Bundesländer und Städte retweeten (z.B. »AlternativeBW», AfDDuesseldorf», «AfDKoeln», «AfDPaderborn»), sondern auch AfD-Politiker auf Bundes- und Landesebene (z.B. «Frauke-Petry», «Beatrix_von_Storch», «Bjoern-Hoecke», «MarkusPretzel», «AliceWeidel»). Unter den Usern, die «e_pitzky» und «LyahSqueak» darüber hinaus retweeten, finden sich auch solche, die eine offensichtlich rechtsradikale Gesinnung nahelegen: so retweeten beide Nachrichten des User-Accounts «OFFICIAL_PEGIDA», einer islam- und fremdenfeindlich, völkisch beziehungsweise rassistisch eingestuften Organisation, gegen deren Mitglieder wiederholt Strafverfahren wegen Volksverhetzung anhängig waren beziehungsweise Urteile rechtskräftig wurden. Seit 2012 wird im Auftrag des Generalbundesanwalts gegen einzelne PEGIDA-Mitglieder wegen des Verdachts auf Bildung einer terroristischen Vereinigung ermittelt. [Wikipedia, 2018] Auch werden von «LyahSqueak» und «e_pitzky» Tweets von Usern wie beispielsweise «BonkeKolja», «balleryna», «NSU_LEAKS» oder «stopp_merkel» geteilt, welche ebenfalls islam- und fremdenfeindliche, verschwörungstheoretische beziehungsweise staatsfeindliche Positionen vertreten. Beispielsweise twittert der Autor und Blogger Kolja Bonke, der auf Twitter als User «BonkeKolja» aktiv ist, zur Flüchtlingskrise, Einwanderung und den Ereignissen der Kölner Silvesternacht 2015/16 und stellt in seinen Nachrichten immer wieder den Bezug zwischen Flüchtlingen und dem Anstieg an Kriminalität her. [Grau, 2016] Zwei seiner Tweets führten zur Sperrung seines Accounts durch Twitter: Im ersten Tweet fragte er rhetorisch, ob Bundesjustizminister Heiko Maas noch zu seiner Aussage stünde, es gäbe keine nachweisbare Verbindung zwischen Terroristen und Flüchtlingen. Der zweite Tweet war deutlicher: «Bei Maas stellt sich mir ja die Frage, ob man seine Untätigkeit noch auf Inkompetenz zurückführen kann oder ob er schon kriminell handelt». [Grau, 2016] Der User «balleryna» stand bereits unter dem Verdacht, ein maschinell geführter AfD-Unterstützer-Account zu sein. Die Analysen von Netzpolitik.org deckten auf, dass «balleryna» Teil eines Netzwerks aus anonymen Unterstützer-Accounts ist, welche untereinander und allem Anschein nach auch mit der Parteizentrale in Kontakt stehen. [Reuter, 2017a] Dieses inoffizielle Netzwerk wird dazu eingesetzt, die eigentliche Schwäche der Partei auf Twitter zu kompensieren und ihr so künstlich mehr Präsenz und Gewicht zu verleihen. [Reuter, 2017a] Der User «NSU-Leaks» wurde von Dr. Simon Hegelich, einem Experten auf dem Gebiet, als User-Account mit «[…] sehr Bot-typische[m] Verhalten […]» [Lepies/Brandt, 2017] beschrieben.

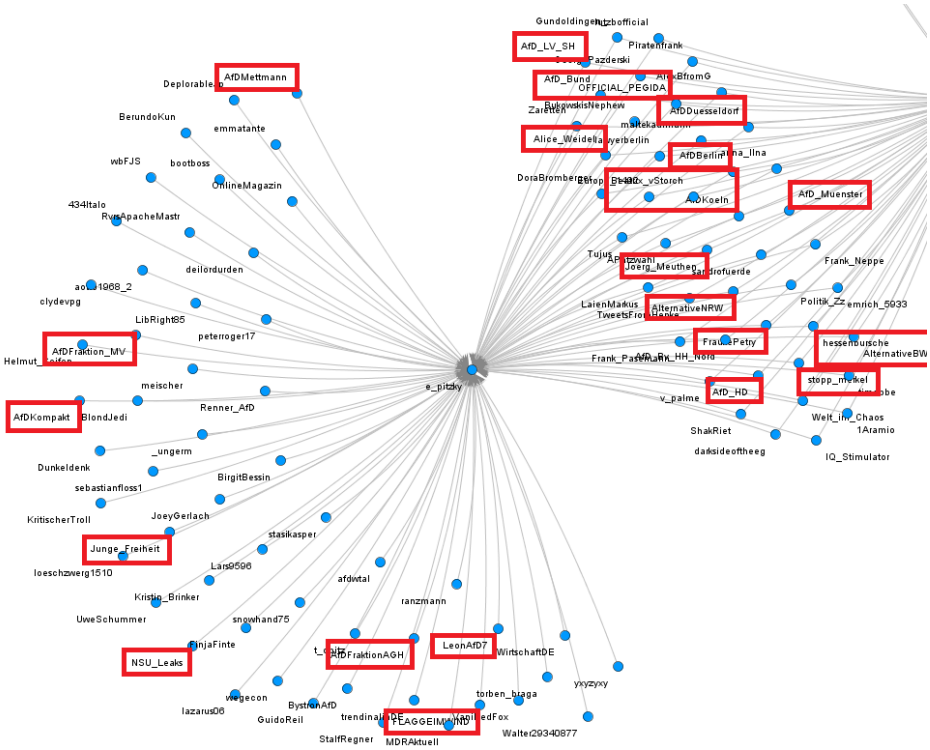

Abbildung 2–2: Echokammer «e_pitzky»

Zusammenfassend kann festgehalten werden, dass die Netzwerkanalyse fünf User identifiziert hat, die aufgrund ihres auffallend hohen Retweetaufkommens bei der NRW-Wahl Kandidaten für Social Bots sein könnten. Neben den beiden Echokammern um die User «jaquearnoux» und «bastilladigital» (vgl. Abbildung 2–1 oben links und mitte), welche vornehmlich Tweets von Unterstützer-Accounts der Piraten Partei weitergeleitet haben, konnte mit der Echokammer um den User «AndreasAndy3131» (vgl. Abbildung 2–1 unten mitte) ein Multiplikator für Unterstützer-Accounts der Partei DIE LINKE identifiziert werden. Die bemerkenswertesten Echokammern sind die der User «LyahSqueak» und «e_pitzky», welche teilweise identische Quellen retweeteten. Von AfD-Partei-Accounts der verschiedenen Bundesländer über Partei-Accounts verschiedener Städte bis zu User-Accounts von AfD-Politikern auf Bundes- und Landesebene wird damit das gesamte Informationsuniversum der AfD verbreitet. Dieser Umstand lässt vermuten, dass es sich bei «LyahSqueak» und «e_pitzky» um einen Teil eines koordinierten Unterstützernetzwerks handelt und nicht um einzelne Personen, die die Partei auf freiwilliger Basis unterstützen. Beunruhigend ist, dass auch Nachrichten von rechtsradikalen Organisationen wie PEGIDA verbreitet werden und in dessen Konsequenz ein User, der einem dieser beiden User folgt, mit mehrheitlich fremdenfeindlichen beziehungsweise rassistischen Nachrichten konfrontiert wird. Weiterhin konnte in der Echokammer von «e_pitzky» ein Social Bot identifiziert werden, dessen Nachrichten von ihm verbreitet wurden.

Die Netzwerkanalyse der User beschränkte sich auf den Zeitraum vom 5. bis zum 22. Mai 2017, was einer Zeitspanne von 18 Tagen entspricht, und berücksichtigte nur Retweets zur NRW-Landtagswahl von Usern, die mehr als 10 (Re-)Tweets pro Tag verschickten. Die Analyse stellt also nur einen Ausschnitt aller Tweets dar. Um das Oxford-Kriterium anwenden zu können, müssen jedoch alle Tweets eines Users betrachtet werden. Aus diesem Grund wurde im Folgenden die Social Bot-Wahrscheinlichkeit der User mit den meisten allgemeinen

(Re-)Tweets mit der Social-Bot Wahrscheinlichkeit der User mit den meisten (Re-)Tweets zur NRW-Wahl verglichen.

Abbildung 2–3 zeigt die Wahrscheinlichkeitsverteilung einer Stichprobe der jeweils 90 aktivsten User, die Social Bots sein könnten. Auf der Y-Achse finden sich fünf farblich markierte Bereiche, welche die Social-Bot-Wahrscheinlichkeit eines User-Accounts abbilden. Diese Wahrscheinlichkeiten wurden mit Hilfe des «Botometer» berechnet, einem Bot Detection Framework der Indiana University, welches über 1'000 Attribute in die Schätzung der Bot-Eigenschaft eines Twitter-Accounts einbezieht. User-Accounts im blauen Bereich sind mit sehr geringer Wahrscheinlichkeit Social Bots, wohingegen User-Accounts im roten Bereich mit sehr hoher Wahrscheinlichkeit Social Bots sind. Bereits ab dem orangenen Bereich (ab 60%) kann von einem hinreichenden Verdacht auf einen Social Bot ausgegangen werden. [Indiana University, 2017]

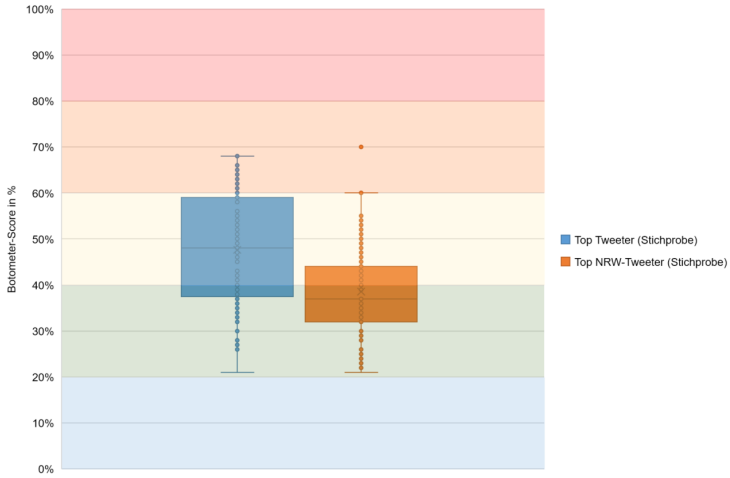

Abbildung 2–3: Wahrscheinlichkeit für Social Bots (Stichprobe)

Der linke Boxplot zeigt die Verteilung der Social-Bot-Wahrscheinlichkeit für die aktivsten 90 User-Accounts, die 200 oder mehr allgemeine Tweets pro Tag abgesetzt haben und damit das Oxford-Kriterium eindeutig erfüllen. Es fällt auf, dass der Median der Verteilung in etwa bei 48% liegt, was bedeutet, dass die Hälfte der User eine Social-Bot-Wahrscheinlichkeit kleiner als ca. 48% aufweist. Entsprechend wird der anderen Hälfte eine Social-Bot-Wahrscheinlichkeit größer als ca. 48% zugeschrieben. Interessant ist, dass ca. 25% der User-Accounts eine Social-Bot-Wahrscheinlichkeit aufweisen, die größer als 60% ist und damit ein hinreichender Verdacht auf Social Bots vorliegt.

Der rechte Boxplot zeigt die Social-Bot-Wahrscheinlichkeit für die aktivsten 90 User-Accounts, die zwei oder mehr NRW-Tweets abgesetzt haben und damit deutlich unter dem Oxford-Kriterium geblieben sind. Es fällt auf, dass die Hälfte der User-Accounts eine Social-Bot-Wahrscheinlichkeit unter ca. 36% hat. Weitere 25% der User-Accounts haben eine Social-Bot-Wahrscheinlichkeit, die zwischen 45% und 60%, also noch im gelben Bereich, liegt. Es gibt einen Ausreißer, dessen Social-Bot-Wahrscheinlichkeit vom Botometer mit 70% berechnet wurde. Für das Gros der anderen User, die zur NRW-Wahl getwittert haben, kann jedoch festgehalten werden, dass kein hinreichender Verdacht auf Social Bots vorliegt.

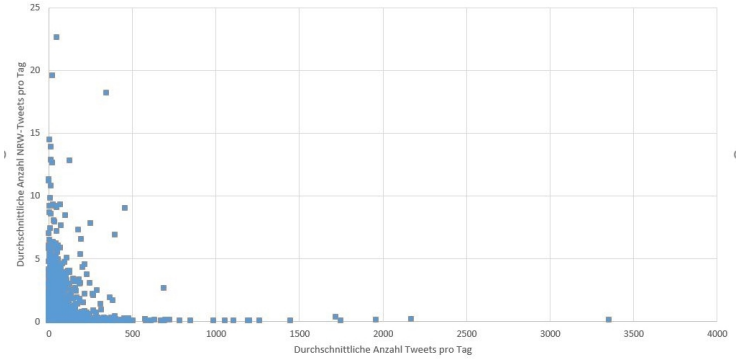

Abbildung 2–4: Durchschnittliche Anzahl Tweets vs. NRW-Tweets pro Tag

In einem nächsten Schritt wurde nun die Aktivität der beiden Gruppen direkt gegenübergestellt, Abbildung 2–4 zeigt die Ergebnisse. Auf der X-Achse ist die durchschnittliche Anzahl allgemeiner Tweets pro Tag und User abgetragen, auf der Y-Achse die durchschnittliche Anzahl an NRW-Tweets pro Tag und User. Deutlich erkennbar ist, dass die Mehrheit der User weniger als 500 Tweets pro Tag abgesetzt hat. User, die zwischen 0 und 250 Tweets pro Tag abgesetzt haben, äußerten sich am meisten zur NRW-Wahl. Deren durchschnittliche Anzahl NRW-Tweets pro Tag ist jedoch vergleichsweise gering, in der Regel weniger als 10 Tweets pro Tag.

Die Analyse der Twitter-Daten zur Landtagswahl in NRW hat gezeigt, dass Social Bots an der öffentlichen Meinungsbildung beteiligt waren. Die Wahrscheinlichkeit für Social Bots unter den User-Accounts mit höherem Tweet-Aufkommen war dabei niedrig und deren (Re-)Tweet-Aufkommen war vergleichsweise gering. Um Einfluss auf die Landtagswahl in NRW nehmen zu können, hätte deren Aktivität auf Twitter bedeutend höher sein müssen.

3. Fazit und aktuelle Entwicklungen

Am Beispiel der Kommunikation über den Kurznachrichtendienst Twitter konnte für den Analysezeitraum nachgewiesen werden, dass mit sehr hoher Wahrscheinlichkeit Social Bots an der politischen Diskussion beteiligt waren. Gleichzeitig hat die Analyse der Twitter-Kommunikation gezeigt, dass die User-Accounts mit höherem Tweet-Aufkommen und Bezug zur NRW-Wahl überwiegend keine Social Bots waren. Dies wird auch durch die Beobachtung bestätigt, dass die Anzahl NRW-spezifischer Tweets weit unter der Schwelle liegt, die als einschlägig im Hinblick auf eine Beteiligung von Social Bots angesehen wird (vgl. Kapitel 2). Eine Beeinflussung der politischen Meinungsbildung rings um die NRW-Wahl durch Social Bots kann damit nahezu ausgeschlossen werden. Untersuchungen der Twitter-Kommunikation bezüglich der Bundestagswahl im Zeitraum vom 1. bis zum 10. September von Neudert et al. [Neudert/Kollanyi/Howard, 2017] kommen zu einem ähnlichen Ergebnis: «The impact of political bots was minor overall, with highly automated accounts generating a small fraction of the Twitter traffic about the election, and most of the bots working in the service of the far-right AfD». [Neudert/Kollanyi/Howard, 2017]

Trotz der Tatsache, dass eine Beeinflussung der öffentlichen Meinungsbildung durch Social Bots bei der Landtags- und Bundestagswahl nicht nachgewiesen werden konnte, hat die öffentliche Diskussion in Wissenschaft, Politik und Presse ein Bewusstsein für die Gefahren geschaffen, die von Social Bots ausgehen können. In Deutschland tritt insbesondere der Politologe und Lehrstuhlinhaber für Political Data Science Dr. Simon Hegelich in Erscheinung. Er konstatiert, dass «[…] Social Bots jeden relevanten Hashtag bei Facebook, Twitter und Co. bevölkern […]» [Rebiger, 2017], wenngleich der empirische Nachweis, dass jemand seine Meinung in Folge von Social-Bot-Nachrichten ändere, schwierig zu erbringen sei. Von seinen Forschungsergebnissen berichtete er unter anderem dem Ausschuss für Bildung, Forschung und Technikfolgenabschätzung

und dem Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag (TAB). Noch vor der Bundestagswahl verabschiedete der Deutsche Bundestag das sogenannte «Netzwerkdurchsetzungsgesetz», das Betreiber von Internet-Plattformen verpflichtet, offensichtlich rechtswidrige Inhalte innerhalb von 24 Stunden nach Eingang einer Beschwerde zu löschen. Bei Zuwiderhandlung drohen Bußgelder von bis zu fünf Millionen Euro [Deutscher Bundestag, 2017]. Mit diesem Gesetz sollen Hetze und Fake News in den sozialen Netzwerken bekämpft werden. Kritiker sehen eine Gefährdung der Meinungsfreiheit, da im Zweifelsfall auch rechtmäßige Inhalte gelöscht werden könnten, um eine Zahlung von Bußgeldern zu vermeiden. [Reuter, 2017b]

Auch die Presse berichtete vermehrt über die von Social Bots ausgehenden Gefahren. So zeigten Recherchen der FAZ zur Struktur von AfD-Gruppen auf Facebook, dass ein großes Netzwerk von Facebook-Gruppen von wenigen, zentralen User-Accounts gesteuert wird. Diese machen durch fehlende persönliche Angaben und Profilbilder, sowie der hohen Anzahl Freunde und Follower einen anonymen und nicht menschlichen Eindruck, was die Nutzung von Computerprogrammen nahelegt. Gemeinsam mit den von ihnen administrierten Gruppen können diese User-Accounts mehr als 70'000 User erreichen [Bender/Oppong, 2017], wobei die tatsächliche Reichweite dieses Netzwerks wesentlich größer sein dürfte. Dass die AfD Kenntnis von diesen Facebook-Gruppen hat, kann angenommen werden − Parteigrößen wie Frauke Petry und Alice Weidel, die sich im vergangenen Herbst von der Nutzung von Social Bots distanziert hatten [Stern, 2017], sind selbst Mitglieder in diesen vermutlich von Social Bots administrierten Gruppen. [Bender/Oppong, 2017]

Die beschriebenen Akteure und Maßnahmen zeigen, dass eine Auseinandersetzung mit Social Bots und deren Gefahren stattfindet. In drei wesentlichen Punkten stimmen die Akteure überein: Social Bots sind bereits heute in den sozialen Netzwerken aktiv und entsprechende Strukturen, um ihre Themen zu verbreiten, sind vorhanden. [Deutscher Bundestag 2017, Rebiger 2017] Auch sind sich Experten einig, dass die empirische Evidenz für ein Beeinflussungspotenzial von Social Bots aktuell noch nicht ausreichend ist, um Regulierungen auf Bundesebene zu verabschieden. [Deutscher Bundestag 2017, Rebiger 2017] Sie warnen außerdem davor, von dem gehäuften Auftreten von Social Bots auf eine Beeinflussung der öffentlichen Meinung zu schließen. Bei der Frage nach politischen Handlungsmöglichkeiten herrscht unter den Experten Uneinigkeit, während einige eine Kennzeichnungspflicht für Social Bots fordern, geben andere Experten zu bedenken, dass eine solche Kennzeichnung nur schwer umsetzbar sei. Es müsse schließlich gerichtsfest nachgewiesen werden, dass es sich bei einem User-Account um einen Social Bot handele. Weiterhin würde eine solche Kennzeichnung immer zeitlich verzögert sein und eventuell zu Ausweichbewegungen führen. [Deutscher Bundestag, 2017] Auch wurde der Einführung eines kostenpflichtigen und parallelen Internet teils vehement widersprochen, da es den grundlegenden Prinzipien des Internets zuwiderlaufe. [Rebiger, 2017] Konsens bestand vor allem in dem Punkt, dass die Medien- und Internetkompetenz der Nutzer gestärkt werden müsse, denn Social Bots können ihr Ziel der Beeinflussung der öffentlichen Meinung nur dann entfalten, wenn sie von Internetnutzern als Menschen wahrgenommen werden. [Rebiger, 2017]

Die von den Experten ausgesprochene Handlungsempfehlung, die Medien- und Internetkompetenz der Nutzer zu stärken, wird vollumfänglich unterstützt. Die Stärkung dieser Kompetenz sollte bereits im Schulalter beginnen und langfristig verfolgt werden. Eine aktuelle Studie, bei der 1.000 Bürger zu Fake News und Social Bots befragt wurden [PWC, 2017], stützt diese Empfehlung. Demnach gaben die Hälfte der befragten Bürger an, «relativ gut» über Fake News informiert zu sein, über Social Bots hingegen waren nach eigenen Angaben nur 14% der Befragten «relativ gut» informiert. 39% der Befragten kannten den Begriff Social Bot «gar nicht», bei Fake News waren es nur 7%. Insgesamt haben 64% der Befragten kein fundiertes Wissen über Social Bots. Diese Ergebnisse zeigen, dass Aufklärungsbedarf besteht.

Eine weitere Handlungsempfehlung, die im Rahmen dieser Arbeit evident geworden ist, ist die Erarbeitung eines deutschen Bot Detection-Frameworks. Der Botometer der Indiana University bezieht über 1'000 Attribute in seine Schätzung der Bot-Eigenschaft eines Twitter-Accounts ein. Dabei haben Analysen gezeigt, dass Content- und Sentiment-Attribute den höchsten Erklärungsbeitrag aufweisen [Varol et al., 2017] Die

Content-Attribute des Botometer enthalten beispielsweise Informationen über die Häufigkeit und grammatikalische Anordnung von Wörtern in Tweets, während Sentiment-Attribute darüber Auskunft geben, ob die geäußerte Haltung in einem Tweet, positiv, neutral oder negativ ist. [Varol et al., 2017] Damit sind diese Attribute stark von der verwendeten Sprache abhängig, in der die Tweets verfasst wurden. Da der Botometer für die englische Sprache optimiert wurde [Indiana University, 2017], ist bei deutschen Tweets mit Ungenauigkeiten bei der Schätzung der Social Bot-Wahrscheinlichkeit ihrer User zu rechnen. Diese These wird dadurch unterstützt, dass der Twitter-User «e_pitzky» von Dr. Hegelich als Social Bot identifiziert wurde [Löbl/Onneken, 2017], seine Social Bot-Wahrscheinlichkeit vom Botometer jedoch nur mit 29% berechnet wird. Diese Beobachtung unterstreicht die Notwendigkeit eines Botometers für den deutschen Sprachraum, welches sprachabhängige Attribute in seine Berechnung der Social Bot-Wahrscheinlichkeit einbeziehen kann.

4. Literatur

Bender, Justus, Oppong, Marvin, Frauke Petry und die Bots, FAZ.NET, http://www.faz.net/aktuell/politik/digitaler-wahlkampf-frauke-petry-und-die-bots-14863763.html (alle Websiten zuletzt aufgerufen am 2. Januar 2018), 2017.

Bessi, Alessandro, Ferrara, Emilio, Social bots distort the 2016 U.S. Presidential election online discussion, First Monday, http://firstmonday.org/ojs/index.php/fm/article/view/7090/5653a, 2016.

Deutscher Bundestag, Bundestag beschließt Gesetz gegen strafbare Inhalte im Internet, Deutscher Bundestag, https://www.bundestag.de/dokumente/textarchiv/2017/kw26-de-netzwerkdurchsetzungsgesetz/513398, 2017.

Faas, Thorsten, Sack, Benjamin, Politische Kommunikation in Zeiten von Social Media, Bonner Akademie für Forschung und Lehre Praktischer Politik, http://www.bapp-bonn.de/files/BAPP_Politische_Kommunikation_in_Zeiten_von_Social_Media_Web_Final.pdf, 2016.

Ferrara, Emilio et al., The rise of social bots, Communications of the ACM, volume. 59, no. 7, 2016, S. 96-104.

Fiegerman, Seth, The Curious Case of Cynk, an Abandoned Tech Company Now Worth $5 Billion, Mashable, http://mashable.com/2014/07/10/cynk/#cyc8T1Ng6gq1, 2014.

Gathmann, Florian, Teevs, Christian, Nordrhein-Westfalen, Warum diese Landtagswahl so wichtig ist, Spiegel Online, www.spiegel.de/politik/deutschland/nrw-die-wichtigste-landtagswahl-deutschlands-a-1147190.html, 2017.

Grau, Alexander, Wo endet Meinungsfreiheit?, Cicero Magazin für politische Kultur, http://cicero.de/kultur/der-fall-bonke-gegen-twitter-meinungsfreiheit/60491, 2016.

Hegelich, Simon, Invasion der Meinungs-Roboter, Analysen & Argumente, 2016, Heft 221.

Howard, Philip, Kollanyi, Bence, Bots, #StrongerIn, and #Brexit: Computational Propaganda during the UK-EU Referendum, Computing Research Repository, https://arxiv.org/abs/1606.06356, 2016.

Indiana University, FAQ, Indiana University, https://botometer.iuni.iu.edu/#!/faq, 2017.

Kind, Sonja et al., Social Bots, Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag, Berlin 2017.

Lepies, Jennifer, Brandt, Mathias, Statistik der Woche: Wenig Bots bei Merkel und Schulz, Technology Review Das Magazin für Innovation, https://www.heise.de/tr/artikel/Statistik-der-Woche-Wenig-Bots-bei-Merkel-und-Schulz-3773369.html, 2017.

Löbl, Diana, Onneken, Peter, Infokrieg im Netz-Trolle, Hacker und Fake News im Wahlkampf, ARD, http://www.ardmediathek.de/tv/die-story/Infokrieg-im-Netz-Trolle-Hacker-und-F/WDR-Fernsehen/Video?bcastId=7486242&documentId=45887556, 2017.

Neudert, Lisa-Maria, Kollanyi, Bence, Howard, Philip, Junk News and Bots during the German Parliamentary Election: What are German Voters Sharing over Twitter?, Data Memo 2017.7. Oxford, UK: Project on Computational Propaganda, http://comprop.oii.ox.ac.uk/wp-content/uploads/sites/89/2017/09/ComProp_GermanElections_Sep2017v5.pdf, 2017.

PWC, Bevölkerungsbefragung: Social Bots und Fake News, PWC, https://www.pwc.de/de/technologie-medien-und-telekommunikation/social-bots-berichtsband.pdf, 2017.

Rebiger, Simon, Fachgespräch im Bundestag: Experten halten Einfluss von Social Bots für überschätzt, Netzpolitik.org, https://netzpolitik.org/2017/fachgespraech-im-bundestag-experten-halten-einfluss-von-social-bots-fuer-ueberschaetzt/, 2017.

Reuter, Markus, Bundestag beschließt Netzwerkdurchsetzungsgesetz, Netzpolitik.org, https://netzpolitik.org/2017/bundestag-beschliesst-netzwerkdurchsetzungsgesetz/, 2017b.

Reuter, Markus, Twitter-Datenanalyse bei der AfD: Die falsche Balleryna, Netzpolitik.org, https://netzpolitik.org/2017/twitter-datenanalyse-bei-der-afd-die-falsche-balleryna/, 2017a.

Stern, Jenny, AfD verzichtet auf Meinungsroboter-oder nicht?, Das Erste, http://faktenfinder.tagesschau.de/social-bots-bundestag-wahl-101.html, 2017.

Subrahmanian, Venkatramanan et al., The DARPA TWITTER BOT CHALLENGE, IEEE Computer, 2016, volume 6, no. 49, S. 38-46.

University of Oxford, Pro-Trump highly automated accounts «colonised» pro-Clinton Twitter campaign, University of Oxford, http://www.ox.ac.uk/news/2016-11-17-pro-trump-highly-automated-accounts-%E2%80%98colonised%E2%80%99-pro-clinton-twitter-campaign, 2016.

Varol, Onur et al., Online Human-Bot Interactions: Detection, Estimation, and Characterization, International AAAI Conference on Web and Social Media, Nord America 2017.

Wikipedia, Pegida, Wikipedia, https://de.wikipedia.org/wiki/Pegida#Strafverfahren_gegen_Pegida-Organisatoren_und_Redner, 2017.