

Manipulation im Netz:

(Medien-) Pädagogik zwischen Fake Accounts, Social Bots, und Propaganda

Handreichung für Pädagog*innen

erstellt im Rahmen eines Workshops beim Medienkompass NRW 2018

Dr. Lena Frischlich & Dr. Christian Grimme

Zusammenfassung

Das Projekt PropStop und die Forschungsgruppe DemoRESILdigital der Universität Münster beschäftigt sich mit verdeckt und automatisiert betriebener Online-Propaganda, Extremismus, Hass und Mobbing in Online-Medien. Dabei stehen einerseits die technischen Möglichkeiten zur Nutzung von Fake-Profilen und Social Bots zur strategischen Manipulation im Fokus. Andererseits werden die zentralen kommunikativen und psychologischen Mechanismen zur Ausnutzung von Desinformation, Hass- und Angstrede in dieser Umgebung erforscht.

Christian Grimme und Lena Frischlich stellen im Workshop Ergebnisse zu aktuellen technischen und sozialwissenschaftlichen Fragestellungen vor: Wie funktionieren Social Bots in sozialen Netzwerken? Können sie tatsächlich manipulieren? Wer wird über Online-Medien eigentlich angegriffen?

In diesem Zusammenhang soll diskutiert werden, warum es wichtig ist, Medienkompetenz bereits bei Schülerinnen und Schülern anzulegen und warum die Beschäftigung mit Algorithmen nicht nur etwas für Nerds ist.

Ausgangslage

Wir leben in einer zunehmend digitalisierten Gesellschaft. Gerade für junge Menschen sind Online-Medien selbstverständlicher Bestandteil ihrer Lebenswelt. Die JIM Studie 2017 (s. weiterführende Literatur) zeigt, dass 93% der Jugendlichen, das Smartphone täglich nutzten. Neben den vielen Möglichkeiten zu gesellschaftlicher Partizipation, gehen damit auch vermehrte Möglichkeiten einher, online auf manipulative Inhalte, gefälschte Accounts, Hass und Propaganda zu stoßen.

So berichtet Jugenschutz.net von extremistischer Propaganda in nahezu allen sozialen Netzwerken, die Befragung der Landesanstalt für Medien zeigte 2017 dass 54% der Deutschen zwischen 14-24 Jahren häufig Hasskommentare im Netz sehen. Spätestens seit der US-Wahl 2016 werden zudem fingierte Nachrichten in politischen pseudo-Presseangeboten (sogenannte „Fake news“) und (semi-) automatisierte Fake-Accounts (sogenannte „Social Bots“) verdächtig zu gesellschaftlicher Polarisierung beizutragen und sogar Wahlen zu beeinflussen. Tatsächlich verbreiten sich Inhalte in

sozialen Netzwerken oft von Nutzerkonto zu Nutzerkonto. Irgendwann ist der eigentliche Ursprung von Informationen nur noch schwer nachzuvollziehen und Mediennutzer*innen laufen Gefahr, unbewusst zur Verbreitung von Hass, Fehlinformationen oder Propaganda beizutragen.

Außerdem kann es schwer sein herauszufinden, wer eigentlich hinter einem bestimmten Online-Account steckt oder wer die tausende von „Fans“ sind, die eine bestimmte Seite bei Facebook favorisieren („geliked“) haben. Eine kompetente Überprüfung von Informationen denen man im Netz begegnet wird daher, nicht nur für Jugendliche, immer wichtiger.

Fake Accounts und Social Bots — Im Netz ist man nicht alleine

Nicht hinter jedem Account in sozialen Medien steckt auch ein realer Mensch: Auch unzählige Fake-Accounts, Profile die zu Tarnungszwecken angelegt werden, sind in Online-Medien zu finden. Fake Accounts werden dazu eingesetzt Nutzerbewertungen auf Online-Portalen zu fälschen, auf Instagram Begeisterung zu simulieren, einem Video innerhalb kürzester Zeit hunderte von „Views“ zu verschaffen, oder Inhalte auf Twitter oder Facebook zu teilen.

Fake-Accounts können auch (teil-) automatisiert als sogenannte „Social Bots“ betrieben werden. Der Begriff Social Bot, kurz für „Soziale Roboter“, ist ein Dachbegriff der verschiedene Formen (teil-) automatisierter Accounts in Online-Medien beschreibt, die mit unterschiedlichen Zielsetzungen betrieben werden. Manche dieser Bots sind sehr nützlich, etwa Chat Bots, die bei Kundenanfragen helfen, Assistent Bots, die Termine koordinieren, oder News Bots, wie der Novi-bot der Öffentlich-rechtlichen Medien, der (vor allem junge) Nutzer*innen über das Weltgeschehen informiert. Neben solchen „Nützlingen“ im digitalen Ökosystem gibt es aber auch „Schädlinge“. Etwa Spam Bots, die Werbung versenden oder Propaganda Bots, die dazu eingesetzt werden um Mediennutzer*innen im Sinne einer Ideologie zu manipulieren. Allen diesen Social Bots gemeinsam ist, dass sie menschliches (Kommunikations-) Verhalten im Netz imitieren. Ihnen zu Grunde liegt dabei ein mehr oder weniger komplexer Algorithmus (eine Folge von technischen und formalisierten Handlungsanweisungen). Der Zugriff erfolgt nicht über die menschliche Nutzerschnittstelle, sondern über eine technische Programmierschnittstelle (das Application Programming Interface, kurz API), die die meisten Dienste offen zur Verfügung stellen. Der Algorithmus legt dann zum Beispiel fest, dass wenn immer jemand ein bestimmtes Thema bei Twitter anspricht, also den entsprechenden Hashtag (#) benutzt, der Social Bot diesen Tweet teilt, liked oder darauf mit einem eigenen Tweet antwortet.

Der Grad der Automatisierung von Fake-Accounts kann sehr unterschiedlich sei. Die meisten Social Bots, sind aber eher simpel gestrickt und dienen dazu schematische Aufgaben im Netz auszuführen, etwa alle Inhalte einer bestimmten Homepage zu verbreiten, Nachrichten anderer Nutzer zu wiederholen (retweeten) oder alle Nachrichten zu einem bestimmten Thema zu liken. Diese einfachen Bots sind relativ leicht zu programmieren oder können für wenig Geld online erworben werden.

Tatsächliche virtuelle Gesprächspartner*innen wie der experimentelle Microsoft-Bot „Zo“ sind hingegen enorm aufwendig in der Umsetzung und aktuell sind wir noch weit davon entfernt, dass auch Personen mit geringen Programmierkenntnissen vergleichbare Social Bots erstellen könnten. In tatsächlichen Diskussionen mit komplexen Frage-Antwort Mustern sind Menschen Social Bots noch immer weit überlegen.

Manipulation durch Fake Accounts?

Für Manipulationszwecke reichen aber oft auch die „einfachen“ Bots. Wird eine Nachricht von tausenden geteilt oder ein Video von tausenden angesehen, kann man auf den ersten Blick nicht erkennen, ob hinter der Aufmerksamkeit reale Menschen oder Fake Accounts stecken und ob diese als automatisiert (also als Social Bots) betrieben werden. Damit können Fake Accounts in dreierlei Hinsicht dazu eingesetzt werden um Meinungen im Netz zu manipulieren.

(1) Einzelne Mediennutzer*innen können im Sinne der sozialen Bewährtheit, also der Faustregel, „wenn das alle mögen, muss da ja was dran sein“, die wahrgenommene Glaubwürdigkeit von Informationen oder Beliebtheit von Personen oder Parteien falsch einschätzen.

(2) Dadurch, dass viele Internet-Angebote Algorithmen einsetzen, um ihren Nutzer*innen diejenigen Inhalte zu empfehlen, die auch vielen anderen Accounts gefallen haben, können Fake Accounts zur Entstehung sogenannter *Filter-Blasen* beitragen. Dies bedeutet, dass der Auswahlalgorithmus der Plattform Mediennutzer*innen bevorzugt diejenigen Inhalte zeigt, die von vielen Fake Account favorisiert wurden und andere Inhalte als weniger relevant herausfiltert. Außerdem können Fake-Accounts im Rahmen von digitalen Echo-Kammern (Online-Räumen in denen immer und immer wieder dieselbe Meinung bestätigt wird) dazu beitragen, dass bestimmte Meinungen besonders verstärkt werden.

(3) Fake Accounts können dazu eingesetzt werden die „Trends“ in sozialen Medien zu verzerren und damit zu einer verzerrten Wahrnehmung des gesellschaftlichen Meinungsklimas beitragen. Aus Forschung zur sogenannten *Schweigespirale* wissen wir, dass Menschen ihre eigene Meinung im Netz eher dann äußern, wenn sie das Gefühl haben, mit dieser Meinung in der Mehrheit zu sein und eher schweigen, wenn sie sich in der Minderheit wähnen. Das können Propaganda-Bots ausnutzen. Weiterhin besteht das Risiko, dass Politiker*innen oder Journalist*innen die angeblichen „Trends“ kritiklos übernehmen und den Fake Accounts damit auch jenseits sozialer Medien Gehör verschaffen. Viele Fake Accounts folgen gezielt solchen Meinungsführer*innen im Netz — vermutlich auch um von deren Einfluss zu profitieren.

Auch wenn bisher eindeutige Belege für die Wirkung von Fake Accounts auf politische Einstellungen und tatsächliches Wahlverhalten fehlen, ist davon auszugehen, dass die Erfahrung mit manipulativen

Inhalten, Fake Accounts, Social Bots und Online-Propaganda im Netz inzwischen zur Lebenswirklichkeit von Jugendlichen dazu gehört.

Medienkompetenz wird entsprechend immer wichtiger. Neben der Fähigkeit zum technischen Umgang mit Medien ist dabei vor allem ihre kritische Medienkompetenz, kurz ihre Medienkritikfähigkeit, von Bedeutung. Aufbauend auf dem CONTRA-Projekt zur Förderung von Medienkritikfähigkeit als Präventionsarbeit gegen Extremismus von Rieger, Schmitt, Ernst, Winkler und Roth (2017) kann unter Medienkritikfähigkeit die *analytische*, *reflexive* und *ethische* Einordnung von Online-Inhalten und Akteur*innen verstanden werden, wobei sich drei Teilaspekte unterscheiden lassen: *Awareness*, das Bewusstsein für die Existenz und Wirkungsweise manipulative Inhalte und Akteure. *Reflection*, die kritische Reflektion des eigenen Nutzungsverhaltens. *Empowerment*, die Befähigung aktiv am Diskurs über manipulative Inhalte und Akteure teilzunehmen. Darüber hinaus geht es auch darum, Jugendliche dabei zu unterstützen vertrauenswürdige Quellen zu identifizieren (*Trust*). Angesichts der Vielzahl an Informationen im Netz, ist eine gewisse „Vorauswahl“ unumgänglich, kein*e Nutzer*in kann alles lesen, ansehen oder anhören. Pädagogische Ansätze müssen daher auch aufzeigen, wem Jugendliche online (wenn auch nicht blind) vertrauen können. Medienpädagogik entlang eines solchen *TARE*-Modells („to tare“ = englisch, abwägen, tarieren, erwägen) kann einen wichtigen Beitrag zur Resilienz (junger) Mediennutzer*innen in Zeiten manipulativer Online-Inhalte und Akteur*innen liefern.

Quellen

- Frischlich, L. (*im Druck*). III. Fake News und Social Bots: Erkennung, Wirkung, Bekämpfung. In B. Holznagel & W. Steul (Hrsg.), *Öffentlich-Rechtlicher Rundfunk in Zeiten des Populismus* (S. 27–60). Berlin, Deutschland.
- Frischlich, L., Boberg, S., & Quandt, T. (2017). Un-menschlicher Hass: Die Rolle von Empfehlungsalgorithmen und Social Bots für die Verbreitung von Cyberhate. In K. Kaspar, A. Riffin, & L. Gräser (Hrsg.), *Online Hate-speech* (S. 71–80). München: Deutschland.
- Grimme, C., Preuss, M., Adam, L., & Trautmann, H. (2017). Social bots: Human-like by means of human control. *Big Data*, pp. 279–293. <https://doi.org/https://doi.org/10.1089/big.2017.0044>
- Grimme, C., Assenmacher, D & Adam, L. (2018, *im Druck*). Changing perspectives: Is it sufficient to detect social bots? In *Proceedings of the Conference on Human Computer Interaction International* (HCII), LNCS, Las Vegas, US. Springer.
- Feierabend, S., Plankenhorn, T., & Tathgeb, T. (2017). JIM 2017 Jugend, Information, (Multi-) Media. Medienpädagogischer Forschungsverbund Südwest. Stuttgart; Germany.

Jugendschutz.net, aktuelle Jahresberichte lassen sich unter

<http://www.jugendschutz.net/jahresberichte/> abrufen (zuletzt am 01.03.2018).

Rack, S., & Woldemichel, D. (2017). Fakt oder Fake: Wie man Falschmeldungen im Internet entlarven kann. Berlin, Germany.

Rieger, D., Schmitt, J. B., Ernst, J., Winkler, J., & Roth, H.-J. (2017). Förderung von Medienkritikfähigkeit als Präventionsarbeit gegen Extremismus: Propaganda als Unterrichtsthema. Praxis Schulpsychologie, (12), 4–5.

Weiterführende Informationen und Materialien

Generell ist bei allen Materialien zu beachten, dass es sich noch um ein recht neues Forschungsfeld handelt. Viele Fragen, etwa zur Erkennung und Wirkung von Social Bots, sind bisher ungeklärt. Das merkt man auch daran, dass viele Materialien sich vor allem auf bestimmte politische Orientierungen konzentrieren. Generell lassen sich derartige „Propaganda-Werkzeuge“ aber in allen möglichen nationalen, religiösen und weltanschaulichen Kontexten beobachten. Nicht zu vergessen: Oft geht es auch um kommerziellen Betrug oder den Versuch persönliche Daten zu ergaunern.

- Arbeitsblätter für die Unterrichtsgestaltung stellen u.a. folgende Anbieter zur Verfügung:
- EU-Initiative Klicksafe (<http://www.klicksafe.de/materialien/>)
- Land Niedersachsen (http://www.nibis.de/uploads/1chaplin/files/FakeNews_SekII.pdf)
- Einen (englischsprachigen) Bericht zum Umgang mit manipulativen Inhalten im Klassenzimmer bietet das RAN (Radicalisation Awareness Network) zum Download an <https://tinyurl.com/RAN-fakenews>
- Informationen zu Social Bots gibt es auch bei der Bundeszentrale für politische Bildung (<http://www.bpb.de/252585/was-sind-social-bots>)
- Den Microsofts Chat-bot „Zo“ kann man unter <https://www.zo.ai/> selber testen (Englischsprachiges Angebot)



Dieser Text ist unter einer Creative Commons Lizenz für die nicht-kommerzielle Nutzung lizenziert