Deutscher Bundestag

Ausschuss Digitale Agenda

Ausschussdrucksache
19(23)046

„Resilienz von Demokratien im digitalen Zeitalter im Kontext der Europawahl“

Lisa-Maria Neudert, University of Oxford

Öffentliche Anhörung des Ausschusses Digitale Agenda
10. April 2019

Vielen Dank an Herrn Dr. Jens Zimmermann und die SPD-Bundestagsfraktion für die Einladung heute als Sachverständige vor dem Ausschuss Digitale Agenda zu sprechen.

Mein Name ist Lisa-Maria Neudert. Ich bin Doktorandin und Wissenschaftlerin am Oxford Internet Institute, einem akademischen Department an der University of Oxford. Meine Forschung dort beschäftigt sich mit „Computational Propaganda“, computergetriebener Propaganda, also dem Einsatz von Algorithmen, Automatisierung und Big Data mit dem Ziel der Meinungsbeeinflussung.

Spätestens seit der US-Präsidentschaftswahl 2016 gibt es in Deutschland eine anhaltende Debatte über ausländische Wahlmanipulation, Desinformationskampagnen und Meinungsmache im Internet und im Besonderen in den sozialen Netzwerken. Auch nicht zuletzt, weil Angela Merkel im November 2016 den Bundestag ausdrücklich vor Gefahren durch „Fakeseiten, Bots, Trolle“ in Deutschland gewarnt hat.

Bevor ich in Details gehe, eine grundlegende Einschätzung vorweg: Der Umgang mit Desinformation in Deutschland ist kein Rand-Phänomen und keine Ausnahme, sondern etwas das den Otto-Normal-Bürger, der im Internet unterwegs ist direkt betrifft. Unsere Forschung am Oxford Internet Institute hat ergeben, dass während der Bundestagswahl 2017 rund 20 Prozent der politischen Inhalte, die in den sozialen Medien geteilt wurden von extremistischen, hoch-polarisierenden, verschwörungstheoretischen „Junk News“ Quellen stammten[1]. Doch trotz solcher Forschungsarbeiten — unter anderem von den hier anwesenden Sachverständigen — hängt die Debatte in Deutschland noch immer in der Phase der Problemdefinition und Wirkungsfrage von Desinformation fest.

Natürlich sind Phänomene im Zusammenhang mit digitaler Meinungsmanipulation nur schwer zu quantifizieren — was anlässlich von hunderten oder tausenden Beiträgen, die Bürger jeden Tag im Netz sehen, auch kaum überrascht. Im Nachfolgenden will ich deshalb anhand von konkreten Beispielen über das Wirkungspotenzial von computergesteuerter Propaganda und Desinformation in Deutschland sprechen und aufzeigen, wo sich solche Wirkungen bereits jetzt entfalten und Einfluss auf den öffentlichen Diskurs haben.

[1] Neudert, L.-M., Kollanyi, B., & Howard, P. N. (2017). Junk News and Bots during the German Parliamentary Election: What are German Voters Sharing over Twitter? (Data Memo No. 2017.7). Oxford: University of Oxford.

In meiner Forschung arbeite ich vor allem mit Open Source Data und den öffentlichen Daten, die soziale Netzwerke zugänglich machen. Ich werde meine heutigen Einschätzungen über die Lage in Deutschland auf Forschungsergebnisse stützen, die (1) von unserem Team an der University of Oxford kommen, (2) sowie dem Netzwerk internationaler Akademiker, die sich mit Meinungsmanipulation auf Social Media beschäftigen.

Meine Forschung am Oxford Internet Institute

Am Oxford Internet Institute bin ich seit Sommer 2016 Teil des „Project on Computational Propaganda", das unter anderem durch den Europäischen Forschungsrat finanziert wird. Wir waren eines der ersten akademischen Forschungsprojekte, die sich mit dem Einfluss von digitaler Desinformation und ausländischer Manipulation auf Wahlen und öffentliche Meinung beschäftigt haben. Unsere Forschung hat bisher zum Beispiel die US Präsidentschaftswahl 2016[2], das Brexit-Referendum[3] und die deutsche Bundestagswahl 2017 analysiert. Momentan beschäftigen wir uns mit der Wahl in Indien und der Europawahl.

Wir haben den Begriff „Computational Propaganda"[4], also computergestützte Propaganda eingeführt, da wir glauben, dass es sich dabei um ein neuartiges Phänomen handelt, das potenziell wirkungsstärker und zielgenauer ist als Desinformation und Propaganda offline. Computergestützte Propaganda nutzt Automatisierung, Algorithmen und Big Data für Meinungsmache im Internet und in den sozialen Medien. Der Begriff umfasst vielseitige Phänomene wie zum Beispiel die virale Verbreitung von Falschinformationen in den sozialen Medien, die Verzerrung von öffentlichen Debatten durch automatisierte Social Bots und Fake Accounts, Meinungskampagnen aus dem Ausland sowie heimische extremistische Outlets, Micro-Targeting und illegale Formen von Data-Mining sowie die Manipulation von Suchmaschinen- und Relevanz-Algorithmen durch Optimierung von Inhalten.

Im Unterschied zu historischen Beispielen von Propaganda und Desinformation ist „Computational Propaganda" im Netz skalierbar, personalisierbar und hat Grenzkosten, die gegen null gehen. Damit hat sich Propaganda demokratisiert und kann nun grundsätzlich auch vom User generiert werden. Dahinter stecken vielseitige Akteure mit politischen oder ökonomischen Motiven[5].

Meinungsmanipulation in Deutschland

Seit 2016 beschäftigte ich mich mit Meinungsmanipulation im Internet in Deutschland. In meiner Forschung habe ich den öffentlichen Diskurs auf Social Media zur Bundespräsidentenwahl 2017[6] sowie zur Bundestagswahl 2017 analysiert und mich außerdem

2 Howard, P. N., Kollanyi, B., Bradshaw, S., & Neudert, L.-M. (2017). Social Media, News and Political Information during the US Election: Was Polarizing Content Concentrated in Swing States? [Data Memo 2017.8). Oxford: University of Oxford.

3 Howard, P. N., & Kollanyi, B. (2016). Bots, #StrongerIn, and #Brexit: Computational Propaganda during the UK-EU Referendum. ArXiv:1606.06356 [Physics]. Retrieved from http://arxiv.org/abs/1606.06356

4 Woolley, S. C., & Howard, P. N. (2016). Political Communication, Computational Propaganda, and Autonomous Agents. International Journal of Communication, 10, 4882–4890. Retrieved from http://ijoc.org/index.php/ijoc/article/view/6298

5 Bradshaw, S., & Howard, P. N. (2017). Troops, Trolls and Troublemakers: A Global Inventory of Organized Social Media Manipulation. The Computational Propaganda Project. Retrieved from http://comprop.oii.ox.ac.uk/research/troops-trolls-and-trouble-makers-a-global-inventory-of-organized-social-media-manipulation/

6 Neudert, L.-M., Kollanyi, B., & Howard, P. N. (2017). *Junk News and Bots during the German Federal Presidency Election: What Were German Voters Sharing Over Twitter* (Data Memo No. 2017.2). Oxford: University of Oxford.

mit Regulierung und politischen Gegenmaßnahmen beschäftigt. Momentan sehe ich für Deutschland drei unmittelbare Gefahren.

1. *Virale Desinformation im politischen Mainstream*. Wir haben in unserer Forschung zur Bundespräsidentschaftswahl 2017 und zur Bundestagswahl 2017 nachgewiesen, dass circa 20 Prozent der politischen Inhalte und Nachrichten, die Wähler auf Twitter geteilt haben manipulative „Junk News" waren. In Deutschland kamen also auf vier Links zu verlässlichen Inhalten über Politik und Nachrichten, je ein Link zu extremistischen, hoch-polarisierenden und verschwörungstheoretischen „Junk News". Kombiniert mit Social Media Algorithmen. Kann man angesichts dieser Menge davon ausgehen, dass der Otto-Normal Internetnutzer, während der Bundestagswahl mit solchen „Junk News" ausgesetzt war. Wer steckt dahinter? Die Top „Junk News" Quellen in Deutschland waren in unserer Untersuchung vor allem heimische Medien, die durchaus nicht nur politisch, sondern auch ökonomisch motiviert sind. Der anti-islamische Blog *Philosophia Perennis*, das rechtsextreme *Zuerst!* und *Politically Incorrect News*, die angeben Nachrichten gegen den Mainstream machen zu wollen. Gesondert hinzu kommen dann noch russische Staatsmedien wie *Russia Today*, *Ruptly* und *Redfish*, die auf Facebook und YouTube Hundertausende Follower und Subscriber haben. Diese Outlets setzen dabei vor allem auf Themen, die im deutschen politischen Mainstream bereits ohnehin hochkontrovers sind, wie zum Beispiel Immigration, falsche Kriminalstatistiken oder die Ausschreitungen in Chemnitz, aber auch Verschwörungstheorien rund um Klimawandel und Wissenschaft. Besonders prekär ist, dass polarisierende Desinformation und „Junk News" immer wieder an die Spitze der Aufmerksamkeitsökonomie schießt. Auf YouTube waren rechtsextremistische, pseudo-wissenschaftliche und *Russia Today* Inhalte unter den erfolgreichsten Videos über Chemnitz[7]. Laut einer Analyse von *Buzzfeed* war eine Falschnachricht der erfolgreichste Facebook-Post 2018 mit mehr als 148.000 Interaktionen[8].

2. *Automatisierung und Social Bots als Debattentreiber*. Unsere Studien haben sich auch mit Social Bots befasst. Dazu möchte ich allerdings gleich vorwegnehmen, dass es anhand der Daten, die die sozialen Netzwerke öffentlich zugänglich machen, fast unmöglich ist mit Sicherheit zu sagen, ob eine Debatte durch Bots beeinflusst wird. Die momentan verlässlichsten Methoden evaluieren Automatisierung auf Account Ebene oder nutzen komplexe Machine Learning Verfahren — diese funktionieren allerdings nur, wenn große Mengen an Accounts vorher händisch richtig klassifiziert wurden. Selbst etablierte Systeme wie zum Beispiel *Botometer* der University of Indiana sind durchaus nicht unumstritten. Wir sprechen daher bei unserer Methode von Amplifikations-Accounts, die wir als hochaktive Accounts definieren, die mehr als 50 Mal pro Tag zu ausgewählten Hashtags twittern. Hier haben wir in Deutschland nur sehr geringe Aktivitätslevel nachweisen können. Während der Bundestagswahl wurden 7.4 Prozent des Twitter-Traffics von solchen Amplifikations-Accounts gesteuert. Dennoch gab es in den letzten Monaten in Deutschland immer wieder Berichte, — wie zum Beispiel in der Welt — dass Bots im öffentlichen Diskurs in Deutschland mitmischen.

[7] Cunningham, S. (2018, September 20). How misinformation spread on YouTube after Chemnitz demonstrations - Analysis by Ray Serrato. Retrieved April 8, 2019, from KCRW Berlin website: https://kcrwberlin.com/2018/09/separating-fact-from-fiction

[8] Schmehl, K. (2018). Das sind 8 der erfolgreichsten Falschmeldungen auf Facebook 2018. Retrieved April 8, 2019, from BuzzFeed website: https://www.buzzfeed.com/de/karstenschmehl/falschmeldungen-facebook-2018-fakes-luegen-fake-news

Das hat dann wiederum die politische Debatte über Regulierung und Kennzeichnungspflicht angeheizt und das obwohl die Glaubwürdigkeit dieses Berichts in Frage gestellt wurde. Ich will an dieser Stelle die Gelegenheit nutzen um vor solchen populärwissenschaftlichen Berichten zu warnen und dazu aufrufen deren Methoden zu hinterfragen und Transparenz zu fordern. Selbst führende wissenschaftliche Bot-Erkennungs-Systeme haben Probleme mit falsch-positiven Ergebnissen. Bot-Detection und damit auch Kennzeichnung bleiben komplex, insbesondere auch da Bots selbst immer komplexer werden und zunehmend natürliche Sprache verstehen werden[9].

3. *Unwirksame (Selbst)-Regulierung und Gesetzgebung.* In meiner Forschung habe ich zuletzt regulatorische und andere staatliche Maßnahmen gegen Desinformation untersucht, die seit 2016 eingeführt worden sind[10]. Insgesamt hat unser Team 42 Länder weltweit und ihre Maßnahmen analysiert. Auch Deutschland mit dem Netzwerkdurchsetzungsgesetz ist natürlich eines davon. Im Rahmen dieser Arbeit haben wir viele Resilienz- und Medienkompetenz-Programme untersucht, Maßnahmen im Zusammenhang mit Datenschutz und Transparenz von politischer Werbung, aber auch neue Löschpflichten, Inhaltszensur und Akkreditierungsvorschriften, Kriminalisierung und Re-Definition von illegalen Inhalten evaluiert. Dabei sind uns eine Reihe an beunruhigenden Phänomenen aufgefallen und die zentralsten möchte ich kurz ansprechen. (A) Autoritäre Regime nutzen Regulierung in demokratischen Ländern als Anlass für Zensur und Inhaltskontrolle. (B) Die Beurteilung über die Legalität von Inhalten im Netz ist privatisiert worden und hat sich auf soziale Netzwerke verlagert, wobei es bei deren Content Moderation an Transparenz mangelt. (C) Maßnahmen adressieren oftmals symptomatische Erscheinungen anstatt grundlegender Probleme im Zusammenhang mit Aufmerksamkeits-Ökonomien und Geschäfts-Modellen von sozialen Netzwerken. Grundsätzlich fehlt für wirksame Gegenmaßnahmen noch immer eine Wissensbasis über Phänomene im Zusammenhang mit Desinformation, politischem Micro-Targeting und Social Bots deren Ausprägung und quantitativen Vorkommen. Mehr Transparenz von sozialen Netzwerken durch Reporting von grundlegenden Metriken, zugängliche APIs und Werbeanzeigen Archive wären wichtige Schritte.

Ausblick

Es bleibt schwer zu demonstrieren wie viele Menschen in Deutschland manipulativen, politischen Inhalten und computergesteuerter Propaganda ausgesetzt waren, davon beeinflusst worden sind oder gar ihr Wahlverhalten geändert haben. Nur den sozialen Netzwerken selbst liegen Daten vor anhand derer solche Aussagen gemacht werden können. Aber es ist bereits jetzt evident, dass Desinformation im politischen Mainstream in Deutschland etabliert ist. Abschließend ein kurzer Ausblick.

Erstens, computergestützte Propaganda erfährt momentan einen „Pivot to Privacy“. Die nächste Generation von Desinformation sind nicht etwa glaubwürdige „Deep Fakes“, sondern

[9] Neudert, L.-M. (2018, August). Future elections may be swayed by intelligent, weaponized chatbots - MIT Technology Review. Retrieved from https://www.technologyreview.com/s/611832/future-elections-may-be-swayed-by-intelligent-weaponized-chatbots/

[10] Bradshaw, S., Neudert, L.-M., & Howard, P. N. (2018). Government Responses to Malicious Use of Social Media (p. 19). Retrieved from https://www.stratcomcoe.org/government-responses-malicious-use-social-media

viel eher die Verbreitung von Falschnachrichten auf encrypted Chat-Applikationen wie Messenger, WhatsApp und Discord.

Zweitens, eine zumindest teilweise technische Lösung ist angesichts der schieren Masse an Content in sozialen Netzwerken unvermeidbar. Aber Künstliche Intelligenz kann momentan noch nicht zuverlässig illegale Inhalte und Automatisierung erkennen und sollte daher nicht als ein Wundermittel behandelt werden.

Drittens, Maßnahmen gegen Desinformation und computergestützte Propaganda werden oftmals in einem komplizierten Spannungsverhältnis zur freien Meinungsäußerung und Freiheit im Netz stehen. „Overblocking" sowie Instrumentalisierung durch autoritäre Regime werden sich als grundlegende Probleme manifestieren.

Meinungsmanipulation und Desinformation im Netz sind eine anhaltende Gefahr für die Demokratie in Deutschland. Um diesen Problemen entgegenzuwirken müssen Soziale Netzwerke Daten und grundlegende Metriken über Aktivitäten auf ihren Plattformen veröffentlichen. Und so eine transparente Wissensbasis für politische Willensbildung schaffen.

Relevante Literatur

Bradshaw, S., Neudert, L.-M., & Howard, P. N. (2018). *Government Responses to Malicious Use of Social Media* (p. 19). NATO StratCom Centre of Excellence. Retrieved from https://www.stratcomcoe.org/government-responses-malicious-use-social-media

Neudert, L. M. (2017). Computational Propaganda in Germany: A Cautionary Tale. In S. Woolley & P. Howard (Series Ed.), *Computational Propaganda: Political Parties, Politicians, and Political Manipulation on Social Media* (p. 31). Oxford: University of Oxford. Retrieved from http://blogs.oii.ox.ac.uk/politicalbots/wp-content/uploads/sites/89/2017/06/Comprop-Germany.pdf

Neudert, L. M., & Marchal, N. (2019). *Polarisation and the use of technology in political campaigns and communication*. European Parliament. Retrieved from http://www.europarl.europa.eu/RegData/etudes/STUD/2019/634414/EPRS_STU(2019)634414_EN.pdf