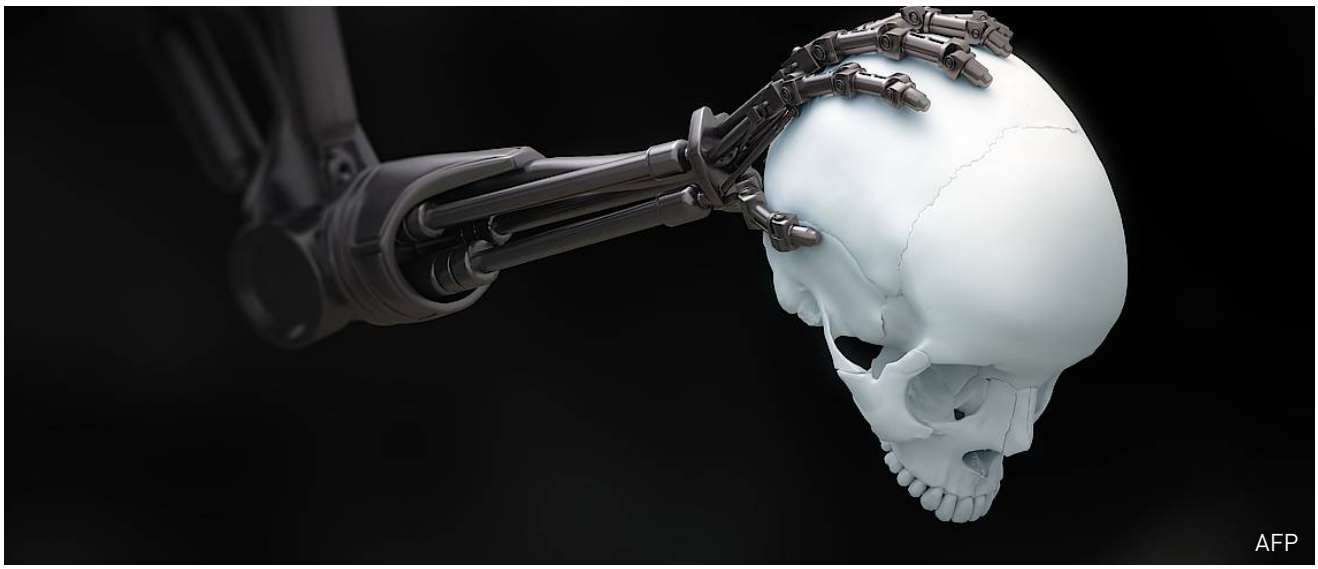
IPG
Internationale Politik
und Gesellschaft

# Die Wahrheit ist tot

Kann die Demokratie die neue Welle künstlicher Intelligenz überleben?

Von Eric Rosenbach, Katherine Mansted | 25.10.2018




Bislang stützten sich Informationsoperationen auf menschliche „Trolle“. Kombiniert mit einfachen automatisierten Algorithmen erzeugten und verbreiteten diese entsprechende Inhalte. Die Social-Media-Konzerne sind heute in der Lage (wenn auch nicht immer gewillt), gegen die meisten Werkzeuge der Informationsgegner einzuschreiten. Viele automatisierte Algorithmen lassen sich identifizieren, weil sie vorhersagbare „botartige“ Muster aufweisen. Entsprechend kündigten – unter öffentlichem und politischem Druck – Facebook, Twitter und Google Anstrengungen an, ihre Algorithmen zu aktualisieren, um gegen „Fake News“ vorzugehen. Dazu führte Facebook Regeln ein, um Wahlwerbung und Werbung zu aktuellen politischen Fragen kennzeichnen zu lassen. Derweil machte sich Twitter dran, Bot-Netzwerke lahmzulegen und gefälschte Nutzerkonten zu löschen. Das sind alles positive Schritte. Doch die  Weiterentwicklung der Künstlichen Intelligenz (KI) könnte in den kommenden Jahren Gegner in die Lage versetzen, ihre Fähigkeiten schneller auszubauen als wir unsere Mittel, um sie zu bekämpfen.

Angetrieben werden die Fortschritte in der KI hauptsächlich von der steigenden Datenflut. Die weltweiten Massen an Daten wachsen in exponentiellem Tempo. Rund 90 Prozent der heute vorliegenden Daten sind in den beiden letzten Jahren aufgelaufen. Bis 2020 werden ungefähr 20 Milliarden Sensoren des „Internets der Dinge“ Daten sammeln - rund um den Globus, aus Mobil- und Haushaltsgeräten sowie städtischen Infrastrukturen. Parallele Entwicklungen tragen zu immer gewaltigeren Datenmassen bei. Dazu zählen Geotagging durch Smartphone-Apps, intelligente Autos und Finanzdienstleister, eine verbesserte Gesichtserkennung und Affective Computing, bei dem Programme aus Texten, Gesichtsausdrücken und Stimmmustern menschliche Gefühle auslesen. Befeuert wird diese Datenexplosion vornehmlich durch die Wirtschaft. Daten ermöglichen es Unternehmen ihre Kunden zielgenauer ins Visier zu nehmen.

**Es stellt sich womöglich heraus, dass es taktisch am effizientesten und billigsten ist, Menschen aus den Abläufen herauszuhalten.**

Daten sind wertvolle kommerzielle Informationen, können in den Händen von Gegnern aber brandgefährlich werden. Russland hat eine lange Geschichte darin, die gesellschaftliche Spaltung in umstrittenen Fragen zu verschärfen, indem es gezielt empfängliche Gruppen ins Visier nimmt: So posteten russische Agenten strittige Inhalte in Facebook-Gruppen, die Unterstützern von Black Lives Matter und Kritikern nahestanden.

Fortschritte im maschinellen Lernen versetzen Gegner künftig in die Lage, zu fast jedem Bürger ein detailliertes Profil zu erstellen, zu kaufen oder zu stehlen. Und diese Profile beruhen nicht mehr nur auf bekannten eingegebenen Daten, etwa ob eine Person einer Gruppe gegen Rassendiskriminierung angehört. Sie basieren auch auf Auswertungen durch Werkzeuge des maschinelles Lernens, die persönliche Eigenschaften und Vorlieben, politische und religiöse Überzeugungen, Gefühle in Echtzeit sowie Merkmale der Identität wie sexuelle Vorlieben immer genauer vorhersagen können. Schon jetzt ist das Mikrotargeting über Soziale Medien eine der schwieriger abzuwehrenden Taktiken der Informationsoperation. Denn die entsprechenden Botschaften sind nur für die anvisierten Einzelnen oder Gruppen und nur für kurze Zeit sichtbar. Wenn Maschinen uns bald besser kennen als wir uns selbst, erhalten Gegner die Fähigkeit, diejenigen auszumachen und anzusprechen, die für Einflussnahmen besonders empfänglich sind. Dann können sie höchst personalisierte Inhalte erstellen, die maximale Wirkung entfalten - eben indem sie die besonderen Charaktereigenschaften, Überzeugungen, Bedürfnisse und Verletzlichkeiten eines Individuums ausnutzen.

Um Inhalte für Informationsoperationen zu erstellen, braucht es bislang noch Menschen. Mit der nächsten Welle der KI-Forschung könnten allerdings Bots ans Steuer gelangen. Heutige KI-Werkzeuge interagieren nur im sehr begrenzten Umfeld mit Menschen, verbessern dabei aber ständig ihre Fähigkeiten, originelle Inhalte zu generieren, die auf die Stimmung des Adressaten zugeschnitten sind. Wenn die KI ihre Fähigkeit, menschliches Verhalten nachzuahmen, weiter ausbaut, sind automatisch erstellte gefälschte Identitäten im Netz schwieriger aufspüren. KI-Werkzeuge sind lernende Systeme. KI-fähige Bots werden Experimente durchführen können und anhand von Erfolg und Misserfolg in Echtzeit lernen, ihre Methoden bis zur maximalen Wirksamkeit zu verfeinern. Ein mögliches Ergebnis: Es stellt sich womöglich heraus, dass es taktisch am effizientesten und billigsten ist, Menschen aus den Abläufen herauszuhalten.

**Fortschritte in KI ermöglichen, Audio- und Videomaterial billiger und schwerer erkennbar zu manipulieren. Forscher sind nur noch wenige Jahre, wenn nicht Monate davon entfernt, realistische Fälschungen von Videos herzustellen, die jedes menschliche Auge täuschen.**

Fortschritte in KI ermöglichen zudem, Audio- und Videomaterial billiger und schwerer erkennbar zu manipulieren. Derzeit gelten Tonaufnahmen, Bilder oder Videos von hoher Qualität als besonders beweiskräftig, wenn um Fakten gestritten oder vor Gericht prozessiert wird. Wie Experten allerdings voraussagen, sind Forscher nur noch wenige Jahre, wenn nicht Monate davon entfernt, realistische Fälschungen von Videos herzustellen, die jedes menschliche Auge täuschen. Schon jetzt kursiert im Internet nutzerfreundliche Software, mit der sich absolut echt wirkendes Hörmaterial fälschen lässt,

wenn zu einer Stimme nur ein ausreichend großer Trainingsdatensatz vorliegt. Gegner sind bald in der Lage, vollständig gefälschte audiovisuelle Inhalte zu erstellen. Oder sie werden - noch heimtückischer - bestehende Inhalte manipulieren, um hochwirksame Informationsoperationen auf den Weg zu bringen. Manche Analysten verweisen auf eine noch größere Gefahr für die Demokratie: Wer vermehrt auf digitale Fälschungen setzt, untergräbt damit auch das Vertrauen in absolut glaubwürdige Informationen.

Was dieses Risiko angeht, sind wir optimistischer. So wie sich das Internet weiterentwickelt hat und vertrauenswürdige Websites inzwischen mit einem Sicherheitszertifikat ausgestattet sind, so dürften auch Systeme weiter ausreifen, mit denen sich audiovisuelles Material zertifizieren lässt. Blockchain-Technologien könnten ebenso dazu dienen, sicherzustellen, dass entsprechende Zertifikate echt sind. Kurzfristig werden Gegner allerdings aus der Lücke zwischen verbesserten Fälschungstechniken und neuen Regeln zur Authentifizierung Kapital schlagen können. Und selbst wenn sich diese Lücke dereinst schließt: Bei besonders strittigen Themen wie internationalen Krisen werden gefälschte audiovisuelle Inhalte wahrscheinlich weiterhin erhebliche Probleme bereiten. Ebenso bei Meldungen, die schnell die Runde machen und rasche Entscheidungen erfordern.

Die Informationstechnologien haben nicht nur die Leben, Gesellschaften und Wirtschaften revolutioniert. Sie verändern auch die Natur des politischen Geschäfts und der Konflikte im 21. Jahrhundert. In vielerlei Hinsicht haben unsere Gegner aus dieser Realität schneller die Lehren gezogen und sich angepasst. Deshalb sollten sich Demokratien auf immer raffiniertere und aggressivere Angriffe dieser Art gefasst machen. Auch müssen ihre Führer erkennen, dass sich nationale Interessen nicht mehr durch konventionelle militärische, wirtschaftliche und diplomatische Mittel vertreten und verteidigen lassen. Für Amerika bleibt ein kleines Zeitfenster, um eine gesamtstaatliche kohärente Strategie zu entwickeln, mit der sich die Gefahren des Informationszeitalters abwehren lassen.

Davon hängt womöglich die Integrität und Legitimität unseres Regierungssystems ab.

*Dies ist ein Auszug aus dem Paper „Can Democracy Survive in the Information Age?“ von Eric Rosenbach und Katherine Mansted, Belfer Center for Science and International Affairs, Harvard Kennedy School, Oktober 2018.*