ANZEIGE

iq digital In Kooperation mit emetriq

Nutzerbefragung

Nehmen Sie sich 3 Minuten Zeit.

Unterstützen Sie uns mit Ihren Antworten.

Umfrage starten ›

Hinweise zum Datenschutz

DIGITALE REVOLUTION

Warum Deepfakes Demokratien gefährden und sogar Kriege auslösen könnten

Mit KI-Methoden lassen sich täuschend echte Videos und Audiobotschaften produzieren. Experten befürchten, dass die Perfektion der Desinformation die Demokratie gefährdet.

4 Wochen für 1 € 29,99 €

Unbegrenzten Zugang zu allen Artikeln im Web und in der App.

Zum Angebot

X

18.09.2019 - 04:02 Uhr • Kommentieren • 5 x geteilt

Wladimir Putin

Die Angst in den USA ist groß, dass sich Russland mit Deepfakes in den US-Wahlkampf 2020 einmischen könnte.
(Foto: imago/ITAR-TASS)

Düsseldorf, Berlin. Dieser Anruf wird vermutlich in die Kriminalitätsgeschichte eingehen. Es sei ein Notfall, sagte der Chef seinem Mitarbeiter. 220 000 Euro müsse dieser auf ein Konto in Ungarn überweisen, und zwar sofort. Der Mann, angestellt bei der englischen Tochterfirma eines deutschen Energiekonzerns, tat, wie ihm geheißen. Warum hätte er auch zweifeln sollen? Die Stimme klang echt - die Sprachmelodie, der deutsche Akzent. Die Transaktion erfolgte.

Der Mitarbeiter sprach jedoch nicht mit seinem Chef, sondern mit einem Betrüger. Der nutzte eine Software zur Stimmenimitation und produzierte damit eine kaum erkennbare Fälschung. Vor eineinhalb Wochen hat der Versicherer Euler Hermes den Fall öffentlich gemacht - und damit weltweit Schlagzeilen ausgelöst: Womöglich haben Kriminelle erstmals Künstliche Intelligenz (KI) genutzt, um sich als jemand anders auszugeben.

Wenngleich der Versicherer keine Beweise präsentiert hat, ist vom ersten Betrug mittels Deepfake die Rede. Der Begriff spielt darauf an, dass die Technologie im Hintergrund als "Deep Learning" bezeichnet wird - eine Spezialdisziplin der KI: Sie nimmt sich das menschliche Gehirn als Vorbild und verwendet für die Informationsverarbeitung mehrere Schichten künstlicher neuronaler Netze. Das Ergebnis sind Bilder, Videos und Tonsequenzen, die echt wirken, aber künstlich erzeugt wurden.

220 000 Euro - die Schadenssumme, die Euler Hermes übernehmen musste - sind nichts im Vergleich zum destruktiven Potenzial, das Deepfakes entfalten können. Experten warnen, dass eine neue Ära der Desinformation bevorsteht. Gefälschte Videos könnten gesellschaftliche Krisen auslösen oder Panik an den Finanzmärkten schüren.

THEMEN DES ARTIKELS

Big Data | Facebook | USA | Künstliche Intelligenz | Donald Trump | Barack Obama | Nancy Pelosi | Youtube | Microsoft

Allein die Möglichkeit von Fälschungen könnte das Vertrauen in demokratische Institutionen weiter untergraben, Debatten noch stärker polarisieren und soziale Spaltungen vertiefen. "Für Staaten schließt sich das Zeitfenster, sich gegen die potenziellen Bedrohungen durch Deepfakes zu schützen, bevor diese eine Katastrophe auslösen", warnt Charlotte Stanton vom Carnegie Endowment for International Peace.

Die Bundesregierung hat die Gefahr erkannt, auch wenn sie sich um eine nüchterne Sprache bemüht. Dass "mittels Deepfakes erzeugte Falschinformationen zur Beeinflussung der Öffentlichkeit" verbreitet werden, sei "grundsätzlich nicht auszuschließen", erklärt das Innenministerium. Darum bereiteten sich die Behörden vor: "Zur Erkennung beziehungsweise Bekämpfung von Kriminalität im Cyberraum unter Nutzung neuer technologischer Methoden" seien die Sicherheitsorgane des Bundes "fortwährend bestrebt, ihre eigenen Analyse-, Ermittlungs- und Strafverfolgungsfähigkeiten weiterzuentwickeln". Die Methoden des maschinellen Lernens, die zur Herstellung von Deepfakes verwendet werden, könnten "auch herangezogen werden, um eine Erkennung sogenannter Deepfakes gezielt zu unterstützen".

Eine Antwort von Innenstaatssekretär Klaus Vitt auf eine schriftliche Frage des FDP-Abgeordneten Konstantin Kuhle weckt allerdings Zweifel daran, dass die Bundesregierung wirklich in der Lage wäre, Deepfakes zu identifizieren. "Ansätze aus Wissenschaft und Forschung zur Erkennung von sogenannten Deepfakes sind den Sicherheitsbehörden des Bundes bekannt, hierbei handelt es sich aber im Wesentlichen um Grundlagenforschung", heißt es in dem Schreiben, das dem Handelsblatt vorliegt.

Nähere Angaben zu ihrem forensischen Instrumentarium will die Bundesregierung nicht machen: Das "Staatswohl" stehe der Offenlegung "polizeilicher und nachrichtendienstlicher Vorgehensweisen zur Gefahrenabwehr" entgegen.

ANZEIGE

Digital Hub I

Um die aktueller
immer mehr mit

Pornovideos als Spielwiese für Deepfaker

Breite öffentliche Aufmerksamkeit erregten Deepfakes erstmals 2017, als auf dem als anarchisch bekannten Portal Reddit Pornovideos mit

prominenten Schauspielerinnen auftauchten – ihre Köpfe montierten Nutzer mithilfe von Software hinein. Die Fälschungen flogen schnell auf, das Unternehmen sperrte das Forum ein paar Monate später, doch die Idee war in der Welt.

Die Kosten für die Manipulation von Videos sinken drastisch. Was früher nur Spezialisten aus Hollywood-Studios konnten, lässt sich heute auf leistungsfähigen PCs zusammenbasteln. Dafür benötigte Programme sind teils frei verfügbar. Wer noch üben muss, kann sich eine Anleitung auf Youtube anschauen. Kaan Sahin von der Deutschen Gesellschaft für Auswärtige Politik (DGAP) spricht daher von einer „Demokratisierung der Desinformation“.

Dieser Fortschritt ist eine Folge der KI-Revolution der vergangenen Jahre. Im Bereich Deep Learning werde zwar schon seit Jahrzehnten geforscht, erläutert der Informatiker Hao Shen, der bei Fortiss, einem Forschungsinstitut des Freistaats Bayern, das Labor fürs maschinelle Lernen leitet: "Aber jetzt sind die Grundlagen vorhanden."

Neben den Algorithmen, die Forscher teils schon vor Jahrzehnten auf Papier entwickelt haben, gibt es heute die gigantischen Datenmengen, die es braucht, um die Systeme zu trainieren, sowie die massive Rechenkraft, um die Arbeit zu bewältigen. Plötzlich werden Anwendungen Realität, die früher als Science-Fiction galten: von Pokerprogrammen, die Profis schlagen, bis zu Autos, die selbstständig über die Straßen fahren.

ANZEIGE

Wie aus Mül kann

Neue Methoden CO2-Emissione und einen ganz zeigt eine McKir aber Milliarden-I

Gleiches gilt für die Bearbeitung von Videos und Audiodateien. "Deepfake ist letztlich eine spezielle Anwendung des Deep Learning", sagt Shen. Auch hier lernen Algorithmen selbstständig, indem sie in großen Datenmengen nach Regeln und Mustern suchen. Beispiel Video: Die Software leitet zunächst ab, welche Merkmale des Gesichts wichtig sind - Augen und Ohren, Lachfalten und Stirnrunzeln. Das erledigt der Computer anhand der Beispiele selbstständig, ohne dass ein Mensch definiert, welche Bestandteile wichtig sind.

Anschließend ist es möglich, bestimmte Gesichtsausdrücke auf eine andere Person zu übertragen. So entstand ein Video von Ex-US-Präsident Barack Obama, der auf seinen Nachfolger Donald Trump schimpft. Oder ein Video von Facebook -Gründer Mark Zuckerberg, der von der totalen Kontrolle faselt. Oder eins von Nicolas Cage, dessen Gesicht in Blockbustern wie „Indiana Jones“ und „James Bond 007“ auftaucht.

Noch sieht man den Unterschied zwischen Original und Fälschung: Die Akteure in Deepfake-Videos wirken zumeist künstlich, der Mund ist seltsam geöffnet, die Kopfbewegungen sind steif. Intuitiv erkennen viele Menschen, dass etwas nicht stimmt. Doch das ist eine Momentaufnahme. "In der nahen Zukunft werden Menschen nicht mehr in der Lage sein, ein echtes von einem gefälschten Bild zu

unterscheiden", ist Shen überzeugt. "Vermutlich werden wir den Kampf gegen die Technologie verlieren."

Für solche Systeme gibt es legitime Anwendungen, wie Forscher in ihren Veröffentlichungen stets betonen. Ein Beispiel ist die Medienbranche: Spezialeffekte werden noch realistischer, Studios und TV-Sender können die Gesichtsausdrücke von echten Schauspielern auf digitale Avatare übertragen. Oder Fehler bei den Dreharbeiten ausbessern, ohne dass es auffällt.

Auch andere Bereiche profitieren von der Simulation. "Wir können mit der Technologie realistische Szenarien erschaffen, in denen autonome Fahrzeuge virtuell trainieren", erläutert Shen. Das System lerne, mit unerwarteten Situationen umzugehen, ohne Menschenleben auf der Straße zu riskieren. Auch in der Medizin gibt es potenzielle Anwendungen: "Wir können simulieren, wie sich seltene Krebsarten entwickeln, und so die Diagnose und Behandlung verbessern", erklärt der Ingenieur.

Dabei bleibt es aber nicht. „Es handelt sich um eine großartige Technologie“, sagt Shen. Das Problem sei, dass sie zum Missbrauch einlade „und die Regierungen noch nichts dagegen tun“. Besonders die USA sind für die Gefahr sensibilisiert – die russische Einmischung in den Präsidentschaftswahlkampf 2016 beschäftigt die amerikanische Politik noch immer.

Die Gegner von US-Präsident Donald Trump fürchten, dass Russland 2020 erneut in den Wahlkampf eingreifen könnte – und dieses Mal nicht mit verhältnismäßig primitiven Facebook- und Twitterbotschaften, sondern dem Versuch, mit Deepfakes die Wahl zu Trumps Gunsten zu entscheiden.

Hinweis an die Redaktion >>

NÄCHSTE SEITE Der Mittelfinger von Varoufakis

Seite 1 2 Alles auf einer Seite anzeigen

E-MAIL POCKET FLIPBOARD

Auch interessant

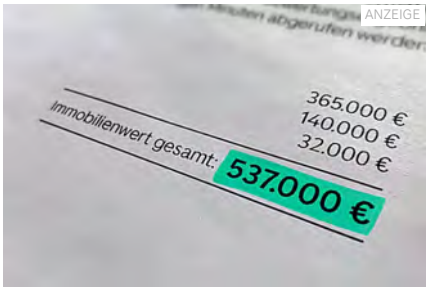
Empfohlen von outbrain

Care by Volvo

Einen Volvo online abonnieren. Nur eine transparente Monatsrate.

Forge of Empires

Das beste Strategiespiel aller Zeiten für PC-Spieler. Kein Download.



Immobilienscout24.de

Unfassbar: Rechner zeigt in 3 Minuten Wert deines Hauses!