Berlin, Mai 2024
Analyse und Beratung

KONRAD ADENAUER STIFTUNG

MONITOR

SICHERHEIT

Der Einfluss von Deep Fakes auf Wahlen

Legitime Besorgnis oder bloßer Alarmismus?

Ferdinand Gehringer, Dr. Christopher Nehring und Mateusz Łabuz

- Die Anzahl der Deep Fakes politischer Natur, einschließlich solcher, die direkt auf die Beeinflussung von Wahlen abzielen, hat signifikant zugenommen.
- Derzeit besteht eine klare Tendenz, Deep Fakes hauptsächlich einzusetzen, um politische Gegner zu diskreditieren und zum Teil auch für politische Werbung
- Die besorgniserregendsten Konsequenzen von Deep Fakes sind ihre kumulativ psychologischen und sozialen Auswirkungen
- Bisher wird die Deep-Fake-Technologie in Deutschland wie auch in vielen anderen Ländern noch nicht zur Einflussnahme auf Wahlprozesse oder während Wahlkampagnen eingesetzt. Aber die Fälle von Deep Fakes im politischen Kontext nehmen zu.
- Maßnahmen zum Schutz vor den negativen Auswirkungen von Deep Fakes sollten darauf abzielen, die Integrität und Authentizität von Informationen zu schützen und die Sicherheit von Wahlprozessen zu stärken.

#KAS4SECURITY

Inhaltsverzeichnis

Das Jahr 2024 kann symbolisch als ein Superwahljahr bezeichnet werden: Etwa die Hälfte der Weltbevölkerung wird aufgerufen, an die Wahlurnen zu treten. Präsidentschaftswahlen finden in etwa 30 Ländern und Parlamentswahlen in etwa 20 anderen Ländern statt. In Taiwan und Indonesien wurde bereits gewählt und auch in einigen der größten demokratischen Länder der Welt, darunter Indien, Mexiko und den USA, werden Wahlen stattfinden. Neben den Landtagswahlen in Thüringen, Sachsen und Brandenburg in Deutschland wird auch das Europäische Parlament im Jahr 2024 gewählt.

Wahlen sind ein wesentliches Element der sozialen Mitbestimmung und der Eckpfeiler der partizipativen Demokratie. Sie bestimmen die zukünftige Verteilung politischer Macht und ermöglichen es den Bürgern, diese Verteilung mitzuprägen. Die Entwicklung moderner Technologien, einschließlich generativer künstlicher Intelligenz, stellt neue Herausforderungen im Zusammenhang mit der Integrität von Wahlen dar. Dazu gehört das manipulative Potenzial von Deep Fakes[1], das als eine der Bedrohungen für die Demokratie betrachtet wird. Die beobachtete Intensivierung des Einsatzes von Deep Fakes zur Beeinflussung des Willensbildungsprozesses in offenen Gesellschaften oder zur Beeinflussung von Wahlergebnissen ist besonders wichtig im Superwahljahr. Insbesondere vor dem Hintergrund der zunehmenden Erosion des Vertrauens in Informationen, politische Institutionen und Prozesse weltweit.

Steigende Zahlen von Deep Fakes

Die Anzahl der Deep Fakes politischer Natur, einschließlich solcher, die direkt auf Wahlen abzielen, hat deutlich zugenommen. Im Jahr 2023 und Anfang 2024 gab es zahlreiche Versuche, den Verlauf von Wahlkämpfen mit Hilfe von Deep Fakes zu beeinflussen. Dies ist ein signifikanter Wandel im Vergleich zu früheren Jahren, in denen solche Fälle isoliert und eher schlecht koordiniert waren.[2] Derzeit gibt es einen klaren Trend, Deep Fakes hauptsächlich einzusetzen, um politische Gegner zu diskreditieren, aber auch für politische Werbung zu nutzen. Die Merkmale des Informationsraums und menschliche Konsumgewohnheiten ändern sich.[3] Bei der Verbreitung von Deep Fakes ist das wichtigste Element die algorithmische Verstärkung, die schädliche Inhalte schnell an Empfänger weiterleitet und eine Moderation von Inhalten, Debunking und die Bekämpfung illegaler Inhalte erschwert.

Deep Fakes werden weit verbreitet im Wahlkampf vor der Präsidentschaftswahl 2024 in den USA eingesetzt.

Neben klassischen Fällen der Diskreditierung politischer Gegner gab es einen sehr beunruhigenden Versuch eines politischen Beraters, die Wahlbeteiligung bei den Vorwahlen in New Hampshire im Januar 2024 zu beeinflussen.

Gefälschte Robo-Anrufe, die die Stimme von Joe Biden imitierten, könnten 5.000–25.000 potenzielle Wähler erreicht haben, obwohl das Ergebnis und die Reichweite der Kampagne noch untersucht werden.[4] Selbst wenn der Einfluss auf das Ergebnis wahrscheinlich überschaubar war, zeigt dieser Prozess, dass das Potenzial hinter der Nutzung von KI leicht für jedermann zugänglich ist und viele Menschen in kurzer Zeit mit einer spezifischen Botschaft erreicht werden können.[5]

Auch die Angriffe in der Slowakei (September 2023) und in Bangladesch (Januar 2024) sind aufgrund der angewandten Strategien bedeutsam. In beiden Fällen wurden unmittelbar vor der Wahl Deep Fake-Desinformationsmaterialien verbreitet, die sich gegen Politiker richteten, die bei den Wahlen antraten. Im Fall der Slowakei soll einer der Kandidaten über Wahlbetrug gesprochen haben (Audio Deep Fake).[6] In Bangladesch kündigte ein Kandidat vermeintlich seinen Rückzug an (Video Deep Fake).[7] Unabhängig von den tatsächlichen Auswirkungen könnte es ein Versuch gewesen sein, die sogenannten Entscheidungszeitpunkte zu testen. *Chesney & Citron*[8] definierten diese als kurze Zeiträume vor einer Wahl, in denen eine Störung der Entscheidungsprozesse irreversible Folgen haben kann. Aufgrund der geringfügigen Zeit bis zum Urnengang ist es zeitlich unmöglich, falsche Informationen wirksam zu entlarven. In der Türkei (Mai 2023) zog sich ein Kandidat in den Präsidentschaftswahlen zurück, nachdem per Deep Fake pornografisches Material, sog. Deep Porn, erstellt und veröffentlicht worden war.[9]

In Argentinien (Oktober 2023) verwendeten beide führenden Kandidaten bei den Präsidentschaftswahlen Deep Fakes, um unter anderem ihre Wahlplakate zu produzieren. Sie erstellten auch Bildmaterial, mit dem politische Gegner lächerlich gemacht werden sollten.[10] In diesem Fall können wir die Umsetzung grundlegender politischer Werbeaktivitäten, aber auch der „Meme-gestützten" Kriegsführung (die Verwendung von Memes zu Desinformationszwecken) im großen Maßstab erkennen.

In Pakistan (Januar 2024) wurden Deep Fake-Aufnahmen des inhaftierten Imran Khan generiert, um seine Anhänger zu mobilisieren. Seine Gegner versuchten dagegen, die Wähler zu demobilisieren, indem sie Aufnahmen von Khan verbreiteten. In diesen Aufnahmen soll er die Bürger davon abgehalten haben, an den Wahlen teilzunehmen.[11]

In Indonesien und Indien (Februar 2024) wurden Deep Fakes von führenden politischen Akteuren weit verbreitet, um ihr Image oder ihr Ansehen zu verbessern.[12] So sangen Politiker in per KI erzeugten Audioaufnahmen populäre Songs. In Indonesien ermöglichte KI die Wiederbelebung von General Suharto, dessen Deep Fake-Avatar politische Werbeaktivitäten durchführen sollte.[13]

Dies sind nur ausgewählte Beispiele von Deep Fakes, die direkt in Verbindung stehen zu Wahlprozessen. Sie sollen das Missbrauchs- und Manipulationspotenzial verdeutlichen. Gleichzeitig wurden Deep Fakes auch für andere politische Zwecke verwendet, was ebenfalls Auswirkungen auf zukünftige Wahlprozesse haben kann. So gab es Fälle unter anderem auch in Polen, Bulgarien, Taiwan, Sambia und Frankreich.

Bisherige Auswirkungen von Deep Fakes

Die Frage der Untergrabung demokratischer Wahlen durch Deep Fakes ist nicht mehr eine Frage des „ob", sondern des „wann", „wie" und „in welchem Ausmaß". Deep Fakes beeinflussen bereits den Verlauf demokratischer Wahlen, aber dieser Einfluss ist weitgehend indirekt und stark vom Informationsraum abhängig.

Alle kommenden Wahlen können potenzielle Ziele von Deep Fakes sein, aber die Methode ihres Einsatzes wird von der Spezifität des Informationsraums und des politischen Kontextes abhängen.

Angriffe könnten auf der Ausnutzung spezifischer Schwachstellen beruhen, einschließlich der Verstärkung kognitiver Vorurteile (z.B. Versuche, unvorteilhafte Gerüchte zu bestätigen)[14] oder der gezielten Ansprache von Themen, die die öffentliche Meinung besonders erregen (z.B. Präsentation eines Kandidaten, der gegen Korruption kämpft, während er eine Bestechung annimmt).

Die tatsächlichen Folgen der Nutzung von Deep Fakes zur Beeinflussung von Wahlen lassen sich nur schwer bewerten. Insbesondere sind das Ausmaß des Phänomens und ihr jeweiliger Einfluss nicht leicht zu quantifizieren. Deep Fakes sind Teil von Desinformationsaktivitäten. Sie tragen zur Störung des Vertrauens in Informationen bei. Es geht nicht nur um direkte Desinformationsangriffe, sondern auch um die langfristigen Folgen der Untergrabung des Vertrauens der Bürger, der Förderung von Unsicherheit oder der Störung des epistemischen Werts von Medien, Informationen und ihrer Überbringer.[15]

In diesem Kontext bestehen die Auswirkungen von Deep Fakes auf Wahlen hauptsächlich in psychologischen und sozialen Aspekten.[16] Dies bedeutet nicht, dass Deep Fakes nicht das Potenzial haben, direkt auf Wahlen und den Wahlprozess einzuwirken. Zentral hierfür scheint das zeitliche Abzielen auf die erwähnten Entscheidungspunkte zu sein,[17] die bereits Teil eines neuen Desinformations-Leitfadens sein könnten.

Das Verständnis der Folgen von Deep Fakes erfordert den Aufbau eines methodischen Rahmens zur Bewertung ihrer Auswirkungen. Entscheidende Berücksichtigung muss die jeweilige Form finden. Es gibt bereits klare Anzeichen dafür, dass Audio-Dateien aufgrund der Schwierigkeiten bei der Entlarvung eine größere Bedrohung darstellen, obwohl ihre tatsächliche Wirkung noch weiter untersucht werden muss.

Wahlen in kleinerem Maßstab (z.B. lokale Wahlen) können ähnlich sensibel sein. Das Risiko der Manipulation hängt auch von der Größe des Wahlkampfes ab. Kandidaten in kleineren Wahlen haben weniger Mittel, um Deep-Fake-Inhalte zu entlarven, während große Wahlkämpfe und Kampagnen von der medialen Aufmerksamkeit stark profitieren.

Die Grenze zwischen den Folgen von Deep Fakes und Desinformation zu ziehen, ist äußerst schwierig. Die fehlende methodische Grundlage und die Schwierigkeiten bei der empirischen Überprüfung lassen den tatsächlichen Einfluss von Deep Fakes nicht messbar erscheinen. Insbesondere da Aktivitäten, die direkt auf Wahlen abzielen, durch Aktivitäten in anderen Bereichen ergänzt werden könnten: Deep Fakes könnten Teil von Desinformationskampagnen, militärischen Informationsoperationen oder hybriden Manipulationsversuchen sein.[18]

Wie aus einer Analyse von Deep Fakes im Zusammenhang mit den Wahlen von 2023 und Anfang 2024 hervorgeht, sind bisher nicht die Effekte messbar, welche viele Beobachter erwartet haben.[19] Nur in zwei Fällen, während der Wahlen in der Slowakei und in der Türkei, hatten Deep Fakes einen messbaren Effekt auf die Wahl selbst. Aber auch dort haben sie die Wahl nicht entschieden.

Kumulative Effekt als größte Bedrohung

Die besorgniserregendsten Konsequenzen von Deep Fakes sind ihre kumulativ psychologischen und sozialen Auswirkungen. Deep Fakes werden eher für destruktive Wahlkämpfe eingesetzt. Sie ermutigen nicht unbedingt dazu, für einen bestimmten Kandidaten oder eine bestimmte Partei zu stimmen, sondern entweder gar nicht zu wählen oder nicht für einen Kandidaten oder eine Partei zu stimmen.

Um dies effektiv zu tun, müssen Deep Fakes nicht besonders überzeugend oder lebensnah sein, solange sie eine klare emotionale Botschaft haben, die haften bleibt. Studien haben gezeigt, dass in diesen Fällen Hinweise, wie „Dieser Inhalt wurde mit KI erstellt", das Publikum nicht davon abhalten, die Inhalte zu teilen und an sie zu glauben.

Allein die Tatsache, dass Deep Fakes und KI-Manipulationstechnologien existieren, reicht nicht aus, um einflussreiche und disruptive Auswirkungen in der realen Welt zu erzeugen. Im Jahr 2019 führte beispielsweise das Gerücht, dass eine Videobotschaft von Präsident Ali Bongo von Gabun ein Deep Fake sei und er tot sei, zu einem Militärputsch im Land.[20] Aber weder war er tot noch war das Video ein Deep Fake. Im Herbst 2023 veröffentlichte die israelische Regierung ein Bild, welches die beim Hamas-Angriff auf Israel getöteten Kinder zeigte. In der Folge wurde dieses als Deep Fake dargestellt und verzerrte die öffentliche Diskussion über die Berechtigung der Reaktion Israels in den darauffolgenden Tagen.[21]

In der Forschung wird dieses Phänomen als „Liar's Dividend" bezeichnet. Diese umfasst Behauptungen, dass eine Information ein Deep Fake ist, um abzulenken, zu verzerren oder zu verteidigen.[22]

Es könnte auch für Gerichtsverfahren verwendet werden und eine Form der „Deep Fake-Verteidigung" annehmen.[23] Im Sommer 2023 nutzte ein Anwalt, der Tesla vor einem Gericht in Los Angeles gegen Anschuldigungen im Zusammenhang eines tödlichen Unfalls mit ihrem autonom fahrenden Programm verteidigte, diese Taktik, um vorsichtig Zweifel und Misstrauen gegenüber einer angeblich von Elon Musk gemachten Aussage zu äußern.[24] Wenn alles ein Deep Fake sein könnte, gibt es immer Grund zur Skepsis. Diese Logik und ihr politischer Missbrauch haben sich als mächtige Einflussmöglichkeit erwiesen.

Außerdem ist es möglich, Ereignisse und Debatten zu beeinflussen, indem behauptet wird, dass ein Deep Fake vorliegt. Der Einsatz der Technologie kann das Vertrauen des Publikums in die Authentizität und Echtheit einer Information untergraben. Wie Studien zeigen, reicht bereits die einfache Angst vor Deep Fakes aus, um das Maß an Unsicherheit über die Echtheit bei den Empfängern zu erhöhen. Wissenschaftler haben dieses Phänomen als „epistemische Apokalypse" bezeichnet, und beschreiben damit die Verschmelzung der Grenzen zwischen Realität und Fälschung.[25] Diese Ängste resultieren in einer häufigeren Infragestellung der Richtigkeit von Informationen. Umfragen in Deutschland, Großbritannien und den USA haben gezeigt, dass mehr als 70 % der Befragten Bedenken hinsichtlich Deep Fakes äußerten und mehr als 40 % der Befragten in den USA angaben, dass sie das Gefühl hatten, getäuscht zu werden.[26]

Angst, Misstrauen und Unsicherheit könnten somit die wichtigsten Auswirkungen von Deep Fakes sein. Der Einsatz kann mächtige, jedoch schwer messbare Auswirkungen auf den politischen Prozess, die politische Kommunikation und die Wahlen haben. In einer Welt, in der alles ein Deep Fake sein könnte, sind die Integrität der Wahlen und der Informationen in Gefahr, unabhängig von der tatsächlichen Menge oder Qualität der Deep Fakes.

Implikationen für Deutschland

Bisher wird in Deutschland, wie in vielen anderen Ländern, die Deep-Fake-Technologie hauptsächlich für Betrug und Pornografie verwendet. In Wahlprozessen oder während Wahlkämpfen wurde sie noch nicht eingesetzt, aber die Fälle von politischen Deep Fakes nehmen zu.

Der prominenteste Fall ist ein von linken Aktivisten erstelltes Deep Fake-Video, welches Bundeskanzler Scholz zeigt, wie er ein AfD-Verbot fordert. Trotz offizieller Entlarvung und des Drängens der Bundesregierung entschieden sich beliebte und reichweitenstarke Plattformen Sozialer Medien dazu, das Video nicht zu löschen, bis sie gerichtlich drei Monate später dazu aufgefordert wurden.[27]

Russische Komiker (mit mutmaßlichen Verbindungen zum Kreml) haben wiederholt deutsche Politiker mit Deep-Fake-Telefonanrufen ins Visier genommen. Im Jahr 2023 sprach Wirtschaftsminister Robert Habeck mehr als vier Minuten lang mit russischen Komikern, die sich als afrikanische Politiker ausgaben.[28]

Von politischen Akteuren scheinen weit rechtsstehende Politiker, Aktivisten und Gruppen am häufigsten KI-Bilder und Audio-Deep Fakes zu verwenden. Politiker der AfD haben KI verwendet, um symbolische und rassistische Bilder von Migranten zu erstellen[29], und gegen das bestehende System Demonstrierende haben diskreditierende Audio-Deep Fakes der ARD Tagesschau bei Demonstrationen verwendet.[30] Als diese Politikerinnen und Politiker sowie andere Beteiligte sich mit massiven nationalen Demonstrationen gegen Rassismus konfrontiert sahen, verwendeten sie ebenfalls die „Deep-Fake- Verteidigung" und behaupteten, dass Bilder der Demonstrationen mit KI erstellt wurden, um die Anzahl der Demonstranten zu übertreiben.[31]

KI-generierte Bilder wurden auch während der Welle von Bauernprotesten seit Ende 2023 verwendet. Einige KI-Bilder waren rein symbolisch, andere sollten das Ausmaß der Proteste übertreiben. In einem besonders bemerkenswerten Fall von rechtsgerichteten Politikerinnen und Politikern sowie Aktivistinnen und Aktivisten, die versuchten, die Stimmung der Proteste einzufangen, wurde ein Bild von aufgehäuften Heuballen vor dem Eiffelturm geteilt und kommentiert.[32] Dieses Bild erwies sich als KI-manipuliert.

Während Deutschland sich auf die Europawahlen im Juni 2024, die Landtagswahlen in drei Bundesländern und die Bundestagswahl 2025 vorbereitet, scheint es, dass die meisten politischen Akteure die Nutzung und Vorteile der Deep-Fake-Technologie derzeit erst noch erkunden. Die bisher aufgetretenen Fälle von Deep-Fake-Angriffen haben jedoch gezeigt, dass politische Akteure noch relativ unvorbereitet und sich der Bedrohung nicht vollständig bewusst sind. Angemessene Reaktionsmechanismen fehlen bisher.

Systemische Bedrohung und notwendige Maßnahmen

Anstatt auf einen „Game-Changer-Moment" zu warten, einen einzelnen Deep Fake, der massive Verwirrung stiftet und allein wichtige politische Ereignisse entscheidend beeinflusst, sollten Deep Fakes eher als kumulative, systemische Bedrohung betrachtet werden. Der Aufbau von Schutzmaßnahmen gegen die negativen Auswirkungen von Deep Fakes sollte Maßnahmen umfassen, die darauf abzielen, die Integrität von Informationen und Wahlen zu schützen sowie die Resilienz zu stärken.

Politische und öffentliche Institutionen sollten klare Verteidigungs- und Reaktionsstrategien entwerfen und einführen, um die Integrität von Wahlen und Informationen sicherzustellen. Darüber hinaus sollten spezialisierte Institutionen regelmäßig über die neuesten Entwicklungen im Informationsraum in verschiedenen Medien berichten und aktuelle Erzählungen, Desinformationskampagnen und verwendete Deep Fakes veröffentlichen. Die Kommunikation mit der Gesellschaft über aktuelle Bedrohungen und Kampagnen schafft zusätzliches Bewusstsein.

Des Weiteren sollten politische und Medienakteure gemeinsame ethische Standards für die Verwendung von KI in politischer Kommunikation, Wahlkampf, Werbung und Berichterstattung entwickeln, veröffentlichen und durchsetzen. Ein Verhaltenskodex sollte auch klare Grenzen festlegen, wann KI-unterstützte Tools im Wahlprozess verwendet werden können und wann nicht mehr.

Maßnahmen zur grundlegenden und KI-spezifischen Medienkompetenz müssen dringend gestärkt werden. **Programme und Bildungsmaßnahmen zur Erhöhung des Bewusstseins und der Widerstandsfähigkeit sollten Teil eines Wahlvorbereitungscurriculums für Entscheidungsträger, Kandidaten, aber auch Beamte, Journalisten, Influencer und die breite Öffentlichkeit werden.** Zugleich sollte der Bildungsaspekt ein Element des Schulcurriculums werden.

Regeln und Vorschriften, d. h. Bestimmungen des EU-KI-Gesetzes oder Bedingungen und Community-Standards von Social-Media-Plattformen, müssen mit "Deep Fake-Response-Einheiten" und speziellen Ressourcen für sehr kurzfristige wahlbezogene Deep Fakes durchgesetzt werden. Gesetzgeber könnten auch die Ausgabe zusätzlicher (d. h. wahlbezogener) Vorschriften in Betracht ziehen.

Öffentlich-private Partnerschaften und die Zusammenarbeit zwischen politischen Akteuren, sozialen Medienunternehmen, traditionellen Medien und Forschungseinrichtungen können dazu beitragen, ein erhöhtes Bewusstsein für das Problem zu schaffen, sowie entsprechende Inhalte rechtzeitig zu entlarven und zu löschen.

Der öffentliche und der private Sektor sollten zusammenarbeiten, um Methoden zur Erkennung von Deep Fakes zu stärken und ihre Verfügbarkeit zu erhöhen. Strafverfolgungsbehörden sollten auch in angemessene Maßnahmen in diesem Zusammenhang investieren und die digitalen Kompetenzen entwickeln, die erforderlich sind, um schädliche Inhalte zu erkennen und somit schneller zu reagieren.

Das Verständnis der Konsequenzen von Deep Fakes erfordert den Aufbau eines methodischen Rahmens zur Bewertung ihrer Auswirkungen. Auch wenn der manipulative Einsatz von Deep Fakes noch keine Wahl entschieden hat, ist es nur eine Frage der Zeit, bis der Einfluss von Deep Fakes auf Wahlen und den Wahlprozess zunimmt.

Besonders in einem Super-Wahljahr wie 2024 ist es an der Zeit, die notwendigen Maßnahmen einzuleiten und umzusetzen, um auf zukünftige Wahlen vorbereitet zu sein.

---

[1] Gemäß dem von der EU verabschiedeten Gesetz über Künstliche Intelligenz werden Deep Fakes als von KI erzeugte oder manipulierte Bild-, Audio- oder Videoinhalte definiert, die bestehenden Personen, Objekten, Orten oder anderen Entitäten oder Ereignissen ähneln und für eine Person fälschlicherweise authentisch oder wahrhaftig erscheinen würden.

[2] Łabuz M. Nehring C. (2024). On the way to deep fake-democracy? Deep fakes in election campaigns in 2023. European Political Science. Accepted.

[3] Huijstee van M. et al. (2021). Tackling deepfakes in European policy. European Parliamentary Research Service. Brussels.

[4] Matza M. (2024). Fake Biden robocall tells voters to skip New Hampshire primary election. https://www.bbc.com/news/world-us-canada-68064247.

[5] H. Ramer (2024). Political consultant behind fake Biden robocalls says he was trying to highlight a need for AI rules. https://apnews.com/article/ai-robocall-biden-new-hampshire-primary-2024-f94aa2d7f835ccc3cc254a90cd481a99.

[6] Meaker M. (2023). Deepfake Audio Is a Political Nightmare. https://www.wired.co.uk/article/keir-starmer-deepfake-audio.

[7] Pieal J. N. (2024). AI in politics: How lines between reality and 'deepfake' are blurring. https://www.tbsnews.net/features/panorama/ai-politics-how-lines-between-reality-and-deep-fake-are-blurring-779066.

[8] Chesney B., Citron D. (2019). Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security. California Law Review. Vol. 107(18). pp. 1753-1820.

[9] Michaelson R. (2023). Turkish presidential candidate quits race after release of alleged sex tape. https://www.theguardian.com/world/2023/may/11/muharrem-ince-turkish-presidential-candidate-withdraws-alleged-sex-tape.

[10] Nicas J. (2023). Is Argentina the First A.I. Election?. https://www.nytimes.com/2023/11/15/world/americas/argentina-election-ai-milei-massa.html.

[11] Shahzad A. (2024). Pakistan's jailed Imran Khan uses AI-crafted speech to lure votes. https://www.reuters.com/world/asia-pacific/pakistans-jailed-imran-khan-uses-ai-crafted-speech-call-votes-2023-12-18.

[12] Christopher N. (2023). AI Modi started as a joke, but it could win him votes. https://restofworld.org/2023/ai-voice-modi-singing-politics.

[13] Ware G. (2024). Deepfakes and disinformation swirl ahead of Indonesian election – podcast. https://theconversation.com/deepfakes-and-disinformation-swirl-ahead-of-indonesian-election-podcast-223119.

[14] Brown N. (2020). Deepfakes and the Weaponization of Disinformation. Virginia Journal of Law & Technology. Vol. 23(1).

[15] Esselink J. (2021). Deepfakes and extreme beliefs. An ethical assessment. Vrije Universiteit Amsterdam. Amsterdam; Fallis D. (2021). The Epistemic Threat of Deepfakes. Philosophy & Technology. Vol. 34(4). pp. 623-643; Farid H. (2022). Creating, Using, Misusing, and Detecting Deep Fakes. Journal of Online Trust and Safety. Vol. 1(4).

[16] Thus, an increasingly polarized society provides a fertile ground for fueling polarization through social media and algorithms. Algorithms tend to favor emotional and oversimplified content, hence why greater responsibility of platform operators through regulation is opportune. Emotional outrage and social validation play a significant role in this context.

[17] Chesney B., Citron D. (2019). Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security. California Law Review. Vol. 107(18). pp. 1753-1820.

[18] Byman D. L., Gao C., Meserole C. (2023). Deepfakes and international conflict. The Brookings Institution. Washington.

[19] Łabuz M. Nehring C. (2024). On the way to deep fake-democracy? Deep fakes in election campaigns in 2023. European Political Science. Accepted.

[20]Delcker J. (2019). Welcome to the age of uncertainty. https://www.politico.eu/article/deepfake-videos-the-future-uncertainty.

[21] Maiberg E. (2023). AI Images Detectors Are Being Used to Discredit the Real Horrors of War. https://www.404media.co/ai-images-detectors-are-being-used-to-discredit-the-real-horrors-of-war.

[22] Chesney B., Citron D. (2019). Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security. California Law Review. Vol. 107(18). pp. 1753-1820.

[23] Delfino R. (2023). The Deepfake Defense - Exploring the Limits of the Law and Ethical Norms in Protecting Legal Proceedings from Lying Lawyers. SSRN Electronic Journal.

[24] The Guardian (2023). Elon Musk's statements could be 'deepfakes', Tesla defence lawyers tell court. https://www.theguardian.com/technology/2023/apr/27/elon-musks-statements-could-be-deepfakes-tesla-defence-lawyers-tell-court.

[25]Schick N. (2020). Deep Fakes and the Infocalypse. Octopus Books. Ottawa; Fallis D. (2021). The Epistemic Threat of Deepfakes. Philosophy & Technology. Vol. 34(4), pp. 623-643; Habgood-Coote J. (2023). Deepfakes and the epistemic apocalypse. Synthese. Vol. 201.

[26] Home Security Heroes (2023). AI deepfakes in 2024 election. https://www.homesecurityheroes.com/ai-deepfakes-in-2024-election; Luminate (2023). Bots versus ballots: Europeans fear AI threat to elections and lack of control over personal data. https://www.luminategroup.com/posts/news/bots-versus-ballots-europeans-fear-ai-threat-to-elections-and-lack-of-control-over-personal-data.

[27] Hanfeld, M (2024): Bundesregierung lässt Deepfake-Video mit Olaf Scholz verbieten, in: FAZ, 22.2.2024 (https://www.faz.net/aktuell/feuilleton/medien/bundesregierung-laesst-fake-video-mit-olaf-scholz-verbieten-19538916.html).

[28] N.N. (2023): Fake-Anruf beim Wirtschaftsminister Russische Trolle legen Habeck rein, in: Spiegel, 6.12.2023 (https://www.spiegel.de/politik/deutschland/robert-habeck-russische-trolle-legen-ihn-mit-fake-anruf-rein-a-5bfc1066-a1ba-4bae-8f3b-7506d4b37c00).

[29] N.N (2024).: So nutzt die AfD KI-Fotos für Propaganda, in: Watson, 3.4.2024 (https://www.watson.ch/digital/afd/174644994-so-nutzt-die-afd-ki-fotos-fuer-propaganda).

[30] N.N. (2024): Demonstrationen in Dresden Justiz ermittelt wegen tagesschau-Fakes, in: Tagesschau, 27.2.2024 (https://www.tagesschau.de/inland/justiz-ermittlungen-tagesschau-audiodateien-100.html).

[31] Pascal Siggelkow (2024): Massenproteste gegen rechts Falsche Behauptungen über Demo-Bilder, in: Tagesschau Faktenfinder, 22.1.2024 (https://www.tagesschau.de/faktenfinder/demonstrationen-rechtsextremismus-bilder-100.html).

[32] Thomas Laschyk (2024): AfD-Fans fallen auf KI-Fake über Bauernproteste in Paris herein, in: Volksverpetzer Faktenfinder, 5.2.2024 (https://www.volksverpetzer.de/faktencheck/afd-ki-fake-bauernproteste-paris/).

Impressum

Die Autoren

Ferdinand Gehringer – Politikberater für interne und Cybersicherheit, Abteilung Internationale Politik und Sicherheit, Bereich Analyse und Beratung der Konrad-Adenauer-Stiftung in Berlin.

Christopher Nehring – Doktor der Geheimdienststudien, Experte für KI, Desinformation und Geheimdienste. Fellow und Gastdozent für das Medienprogramm Südosteuropa der Konrad-Adenauer-Stiftung. Schreibt regelmäßig für den Tagesspiegel, die Deutsche Welle, TableMedia, die NZZ und andere Medien.

Mateusz Łabuz – Diplomat im Karrieredienst des polnischen Außenministeriums; Promotionsstudent an der Technischen Universität Chemnitz (Deutschland); Dozent für Cybersicherheit und KI an der Universität der Nationalen Bildungskommission in Krakau (Polen); Dozent für Cybersicherheit an der Päpstlichen Universität Johannes Paul II. in Krakau (Polen).

Konrad-Adenauer-Stiftung e. V.

Ferdinand Gehringer
Abteilung Internationale Politik und Sicherheit
Hauptabteilung Analyse und Beratung

T +49 30 / 26 996-3460
ferdinand.gehringer@kas.de

Herausgeberin: Konrad-Adenauer-Stiftung e. V.
Gestaltung: yellow too Pasiek & Horntrich GbR

Hergestellt mit finanzieller Unterstützung der Bundesrepublik Deutschland.