



Deep Fake: Gefahren, Herausforderungen und Lösungswege

Norbert Lossau

- › Noch mehr als Fake News können manipulierte Videos, sogenannte Deep Fakes, gefährliche Auswirkungen auf Gesellschaft und Demokratie haben.
- › Die Produktion von Deep Fakes gelingt mit Methoden der Künstlichen Intelligenz, sogenannten Neuronalen Netzwerken mit Deep Learning.
- › Eine Gegenstrategie kann das Dokumentieren von Quellen und Verbreitungswegen von Videos sein. Insbesondere „digitale Wasserzeichen“ oder auch die Blockchain-Technologie können dabei eine Rolle spielen.
- › Es gibt Handlungsbedarf in juristischer Hinsicht. Bisher gibt es in Deutschland keine ausreichenden Gesetze zum Umgang mit Deep Fakes. Es gibt sinnvolle Anwendungen der Technik, die für Deep Fakes genutzt werden, in Kunst, Wissenschaft und Bildung. Diese sollten nicht verboten sein.
- › Den klassischen Medien kommt beim Thema Deep Fake eine besondere Rolle und Verantwortung zu, was zu ihrer Stärkung beitragen könnte.

Inhaltsverzeichnis

Was sind Deep Fakes?.....	2
Vom gefälschten Foto zum manipulierten Video.....	2
Anwendungen und Missbrauchspotenziale von Deep Fakes.....	3
Stand der Technik.....	4
Deep Fakes und Cheap Fakes.....	5
Risiken und Handlungsbedarf.....	5
Impressum	9

Was sind Deep Fakes?

Die massenhafte Verbreitung gefälschter Informationen (Fake News) kann gefährliche Auswirkungen auf die Gesellschaft und letztlich sogar die Demokratie haben¹. Diese Problematik wird, insbesondere im Kontext der sozialen Medien, seit einiger Zeit im politischen und wissenschaftlichen Raum diskutiert. Eine befriedigende Strategie im Kampf gegen Fake News ist noch nicht gefunden, da zeichnet sich bereits eine neue, noch größere Gefahr ab: Deep Fakes – perfekt gefälschte Videos, in denen Personen erfundene Aussagen in den Mund geschoben werden oder in denen sie scheinbar Handlungen begehen, die in Wirklichkeit nie stattgefunden haben². Mit leistungsfähigen Verfahren der künstlichen Intelligenz (KI) lassen sich Videos in einer Weise manipulieren, dass zumindest mit bloßem Auge nicht mehr zu erkennen ist, ob sie echt sind oder manipuliert wurden.

Missbräuchliche
Anwendung von KI

Das Kunstwort Deep Fake ist entstanden aus dem Zusammenziehen der Begriffe „Deep Learning“, einer speziellen KI-Technik, und dem „Fake“, also der Fälschung. Zum Erstellen von Deep Fake-Videos werden sogenannte Neuronale Netze verwendet, deren Funktionsmechanismen biologischen Gehirnen nachempfunden sind. Sie zeichnen sich durch eine gewisse Lernfähigkeit aus (*machine learning*) und können aus hinreichend vielen Fotos einer bestimmten Person erlernen, beziehungsweise vorhersagen, wie diese aus einer bestimmten Perspektive oder bei einer anderen Mimik aussehen würde. Die Leistungsfähigkeit eines Neuronalen Netzwerks wächst mit der Zahl der simulierten Schichten aus Neuronen. Experten sprechen dabei auch von der „Tiefe“ des Netzwerks. Mithin erhalten Neuronale Netze das Attribut „Deep Learning“, wenn sie über sehr viele Neuronenschichten verfügen.

Vom gefälschten Foto zum manipulierten Video

Das Nachbearbeiten und Verfälschen von Fotos ist so alt wie die Fotografie selber. Es gibt berühmte historische Beispiele wie das von Stalin verfügte „Verschwinden“ der Revolutionäre Leo Trotzki und Lew Kamenew von einem Foto, das sie als Zuhörer bei einer Rede Lenins zeigte³. Ein modernes Beispiel ist ein in sozialen Medien verbreitetes Fake-Foto, das Wladimir Putin auf dem Hamburger G20-Gipfel im Jahr 2017 zwischen Donald Trump und Recep Tayyip Erdoğan sitzend zeigt. Im Originalbild gab es keinen Putin.

Fälschungen mit
Vorgeschichte

Seit den 1990er Jahren sind Computerprogramme verfügbar, die es praktisch jedem ermöglichen, digital vorliegende Bilder nachträglich zu verändern. Solange es dabei nur um das Aufhübschen von privaten Urlaubsbildern geht, ist das gewiss unproblematisch. In professionellen Kontexten stellt sich aber durchaus die Frage nach der Beweiskraft einzelner Fotos, mit denen etwas belegt oder dokumentiert werden soll. Längst gibt es hier Techniken und

Ausgefeilte Technik,
geringer Aufwand

Strategien, mit denen die Authentizität und der originale Zustand von Bildern sichergestellt werden soll – zum Beispiel durch digitale Wasserzeichen⁴.

Bewegte Bilder, also Videos, waren bis vor Kurzem noch nicht von dieser Glaubwürdigkeitskrise betroffen. Sie galten gemeinhin als untrüglicher Beweis dafür, dass sich etwas genau so abgespielt hat, wie es im Film zu sehen ist – ausgenommen allenfalls diverse Animationen in aufwendigen und teuren Filmproduktionen. Ein entscheidender Unterschied zu den heutigen Deep Fakes ist der vergleichsweise geringe Aufwand, der mittlerweile für derartige Manipulationen erforderlich ist. Ein handelsüblicher PC und frei verfügbare Software wie das kostenlos erhältliche *DeepFaceLab*⁵ reichen aus, um selber Produzent von Deep Fake-Videos zu werden.

Derartige Fälschungen lassen sich im Web bestaunen. Da erklärt beispielsweise Facebook-Chef Mark Zuckerberg in einem YouTube-Video⁶, dass Facebook Daten sammelt, um Menschen manipulieren zu können. Und die Influencerin Kim Kardashian gibt zu, dass sie es liebt, Menschen zu manipulieren, um damit Geld zu verdienen⁷. Natürlich haben die beiden dies so nicht gesagt. Diese Deep Fakes wurden von Künstlern kreiert, die damit auf die Mächtigkeit und die potenziellen Gefahren der neuen Technik hinweisen wollten. Problematisch wird es indes erst dann, wenn ein Deep Fake nicht mehr als Scherz, Satire oder Parodie erkennbar ist, sondern wenn mit krimineller oder politischer Absicht getäuscht und manipuliert werden soll.

Die Wissenschaftler Shruti Agarwal und Hany Farid von der University of California in Berkeley warnen, dass Staatsoberhäupter in Fake-Videos Dinge sagen oder tun könnten, die zu schweren politischen Verwerfungen, ja Staatskrisen führen könnten. Und militärischen Führern könnten provozierende Aussagen untergeschoben werden, die im schlimmsten Fall sogar einen Krieg auslösen. Auch Börsenmanipulationen oder gezielte Attacken gegen Unternehmen sind vorstellbar. „Von Deep Fakes geht eine signifikante Bedrohung für die Demokratie, die nationale Sicherheit und die Gesellschaft insgesamt aus“, stellen Agarwal und Farid fest⁸. Dass ein Video eine Regierung stürzen kann, hat 2019 der Fall Heinz-Christian Strache in Österreich eindrucksvoll gezeigt – wobei das sogenannte Ibiza-Video kein Fake, sondern ein echtes Video war. Das haben forensische Analysen bestätigt.

Gefährdungen für
Gesellschaft und
Demokratie

Anwendungen und Missbrauchspotenziale von Deep Fakes

Bislang wurde Deep Fake-Technik vorwiegend zur Produktion von Pornofilmen genutzt. Da werden die Gesichter von prominenten Schauspielerinnen, so geschehen etwa mit Scarlett Johansson oder Emma Watson, nachträglich in die mit Pornodarstellerinnen gedrehten Filme montiert. Bewegung und Mimik der Köpfe und Lippen werden dabei von der KI so perfekt angepasst, dass alles täuschend echt aussieht. Für solche Produkte gibt es offenbar einen Markt, und einmal mehr ist es also die Pornografie, die eine technologische Innovation befördert – wie bei der Einführung der VHS-Kassette, der DVD oder sogenannten VR-Brillen zur dreidimensionalen Darstellung von virtuellen Realitäten. Es dürfte nur noch eine Frage der Zeit sein, bis VR- und Deep Fake-Technik miteinander kombiniert werden.

Diskreditierung von
Personen

Doch nicht nur Prominente werden Opfer von Deep Fake-Pornofilmen. Als die Australierin Noelle Martin im Internet nach eigenen Bildern suchte, stieß sie auf Pornofilme, in die ihr Gesicht eingefügt worden war. Der Fall sorgte für Aufsehen und führte dazu, dass es in Australien seit 2018 ein Gesetz gibt, das den Urhebern derartiger Fakes mehrjährige Haftstrafen androht. Der Jurastudentin Noelle Martin reicht dieser Erfolg nicht. Sie fordert eine globale Initiative auf UN-Ebene gegen diese Form der Menschenrechtsverletzung⁹. Zudem

gehe es darum, in einer Welt leben zu können, in der man davon ausgehen darf, dass die von Medien verbreiteten Nachrichten wahr sind.

Das Verwenden des Gesichts einer bestimmten (unbeteiligten) Person für die Produktion eines Fake-Pornofilms kann unterschiedlich motiviert sein. Zum einen kann es darum gehen, jemandem zu schaden oder Rache zu üben. Es soll auch schon vorgekommen sein, dass mit Fake-Videos Geldbeträge erpresst wurden. Derartige Fälle sind naturgemäß nicht gut belegt. Plausibel erscheint diese neue Form von Kriminalität durchaus. Und die Fallzahlen dürften mit der immer leichteren Verfügbarkeit und einfacheren Nutzbarkeit von Deep Fake-Technik wachsen.

Klar ist auch, dass es bei kriminellen Anwendungen von Deep Fakes keineswegs nur um Pornografie gehen wird. Sie dürfte relativ an Bedeutung verlieren. Deep Fake-Videos können eine konkrete Person in vielfacher Hinsicht diskreditieren. Zum Beispiel könnte man sie beim Begehen einer strafbaren Handlung zeigen oder etwas Volksverhetzendes sagen lassen.

Kriminelle Potenziale

Stand der Technik

Bislang lassen sich Deep Fakes in vielen Fällen noch mit aufwendiger Technik enttarnen. Das gilt insbesondere für die jedermann zugänglichen Programme zur Herstellung von Video-Fälschungen. Bei professionell erstellten Deep Fakes stellt sich die Lage nach Einschätzung von Experten ähnlich dar wie beim Wettlauf zwischen Hackern und der Abwehr von Cyber-Angriffen. Es ist ein Rüstungswettlauf, bei dem mal die eine und mal die andere Seite die Nase vorn hat. Ganz ähnlich dürfte es sich beim immer perfekteren Erstellen und dem immer raffinierteren Enttarnen von Deep Fakes verhalten. Auf der einen Seite ermöglicht künstliche Intelligenz das Aufspüren von verräterischen Spuren, die bei der Produktion von Deep Fakes entstehen können. Auf der anderen Seite wird künstliche Intelligenz lernen, genau diese Spuren künftig zu verwischen. Ob es hier in den kommenden Jahren zu einer systematischen Überlegenheit bei der Produktion oder dem Enttarnen von Deep Fakes kommen wird, lässt sich nicht voraussagen.

Technischer Wettlauf zwischen Täuschen und Enttarnen

Unabhängig davon wird allein schon die schiere Masse an zu erwartenden Deep Fake-Videos große Probleme bereiten. Wenn in wenigen Jahren praktisch jedermann mit geringem zeitlichem und finanziellem Aufwand Fake-Videos in guter Qualität produzieren kann, dürften die sozialen Netze geradezu von Deep Fakes überflutet werden. Sie werden in vielen Fällen nicht sofort als unecht auffallen und eine automatische Kontrolle aller Inhalte erscheint von vornherein als aussichtslos. Die meist nur geringe Auflösung von solchen im Netz verbreiteten Videos erschwert überdies den Nachweis von Spuren, die auf einen Deep Fake hindeuten könnten.

Vertrauensverlust im Netz

Mittlerweile sind Deep Fakes sogar in Echtzeit möglich – zumindest wenn es allein um das Fälschen gesprochener Texte geht. Das Programm *Lyrebird*¹⁰ kann beispielsweise die Stimmen von realen Personen täuschend echt nachahmen und beliebige Texte unmittelbar als Fake sprechen. Vorangehen muss allerdings auch hier eine Trainingsphase, in der das Neuronale Netz die betreffende Stimme erlernen muss.

Deep Fakes und Cheap Fakes

Beachtliche Fälschungserfolge lassen sich auch schon mit sogenannten Cheap Fakes erzielen, deren Produktion deutlich weniger aufwendig ist als die eines Deep Fakes. Ein Beispiel: Ein Internetvideo zeigt Nancy Pelosi, die Sprecherin des US-Repräsentantenhauses, wie sie scheinbar angetrunken in ein Mikrofon lallt. Diesen Effekt haben die Fälscher allein durch geschicktes Verändern der Abspielgeschwindigkeit erzielt. Eine einfache, aber gleichwohl sehr wirksame Methode, denn dieser Cheap Fake löste in den USA tatsächlich eine Debatte aus, ob Pelosi für ihr Amt geeignet ist.

Einfach, billig und
wirkungsvoll

Es gibt Forschungsarbeiten, die auch das Deep Learning deutlich einfacher und damit „cheaper“ machen könnte. Es geht darum, Neuronale Netzwerke so zu konstruieren, dass sie mit weniger Bildern beziehungsweise Daten trainiert werden müssen, um trotzdem ihre jeweilige Aufgabe valide bewältigen zu können. Das ist für alle kommerziellen Anwendungen von Neuronalen Netzen wünschenswert, weil eine kürzere Trainingsphase Zeit und Kosten spart. Die Vision der Forscher lautet „single shot learning“, auch wenn es wohl niemals reichen wird, ein Neuronales Netz nur mit einem Bild oder Datensatz zu füttern. Hierzulande arbeiten unter anderen Fraunhofer-Forscher an der Entwicklung schneller lernender Netze¹¹. Sollten sie Erfolg haben, würde das leider auch die Produktion von Deep Fake-Videos erleichtern. Bis auf Weiteres gilt jedoch, dass man über sehr viele Fotos von einer Person verfügen muss, wenn man sie in ein existierendes Video integrieren will und es echt aussehen soll. Es ist nicht absehbar, wie schnell „single shot learning“ verfügbar sein wird und ob es sich auch für Deep Fake-Produktionen eignet.

Technisch brillant
und preiswert

Risiken und Handlungsbedarf

Was würde es für eine Gesellschaft bedeuten, in der bei jeder veröffentlichten Aussage eines Politikers, Wissenschaftlers oder Wirtschaftsführers stets der Vorbehalt im Raum stünde, dass es sich dabei um einen Deep Fake handeln könnte? Umgekehrt könnte jeder ein ihn belastendes Video mit dem Hinweis in Frage stellen, dass es sich hier um einen Deep Fake handelt. Unbequeme Wahrheiten lassen sich leicht anzweifeln, wenn in einer Gesellschaft ohnehin nichts mehr als verlässlich gilt. Der Wissenschaftler Aviv Ovadya bezeichnet dieses Szenario der allgegenwärtigen Desinformation als „Infocalypse“¹². Allein die Manipulierbarkeit von Wahlen würde demokratische Systeme an den Rand ihrer Stabilität bringen. „Das Schlimmste wäre, wenn die Menschen angesichts der sich abzeichnenden Entwicklungen das Interesse an der Wahrheit verlieren“, sagt Maschinenethiker Oliver Bendel von der Hochschule für Wirtschaft FHNW¹³.

Allgegenwärtige
Desinformation

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat im Jahr 2019 gemeinsam mit dem französischen ANSSI (Nationale Agentur für Sicherheit der Informationssysteme) in einer Stellungnahme davor gewarnt, dass „demokratische Prozesse wie Wahlen“ durch Deep Fakes manipuliert werden können¹⁴. In den USA werden solche Befürchtungen im Hinblick auf die kommenden Präsidentschaftswahlen diskutiert. Die amerikanische DARPA (Defence Advanced Research Projects Agency) hat 70 Millionen US-Dollar an Forschungsmitteln bereitgestellt, um Abwehrstrategien gegen Deep Fakes zu entwickeln. In erster Linie geht es dabei um Systeme, die Fälschungen automatisch erkennen sollen.

Manipulation
von Wahlen

Lars Buttler von der Organisation AI Foundation¹⁵ hat ein Programm namens *Reality Defender* entwickelt oder Matthias Nießner, Professor an der Technischen Universität München, ein Programm namens *FaceForensics*. In einer Studie¹⁶ konnte Nießner zeigen, dass *FaceForensics*

Technische
Gegenwehr

Deep Fakes mit einer Trefferquote von 78 Prozent erkannte, wo Menschen dies nur in wenig mehr als 50 Prozent schafften.

Jeder Kamerachip hat eine eigene Charakteristik, gleichsam ein „Fingerabdruck“, weil sich die Eigenschaften der einzelnen Pixel minimal voneinander unterscheiden können. Dies führt zu charakteristischen, nachweisbaren Artefakten in den Bildern. Werden Videos aus Sequenzen zusammengesetzt, die mit verschiedenen Kameras aufgenommen wurden, kann es zu entsprechenden Inkonsistenzen kommen, die Fakes verraten.

Deep Fakes können sich aber nicht nur durch winzige Artefakte im Bildsignal verraten. Auch die Analyse der Tonspur kann sehr aufschlussreich sein. Wissenschaftler des Fraunhofer Instituts für Digitale Medientechnologie in Ilmenau¹⁷ befassen sich seit Jahren mit der forensischen Auswertung von Audiosignalen und können zum Beispiel klären, ob eine gesprochene Nachricht authentisch oder etwa aus Bausteinen zusammengesetzt und mithin gefälscht ist. Oft ist es sogar möglich, aus einem Audiosignal zu rekonstruieren, zu welchem Zeitpunkt es aufgenommen worden ist. Die Netzfrequenz von 50 Hertz ist nämlich nicht konstant, sondern schwankt innerhalb gewisser Grenzen. Schon heute archivieren Forensiker den zeitlichen Verlauf der Netzfrequenz über Jahre hinweg, um den Zeitpunkt der Aufnahme eines Audiosignals bei Bedarf ermitteln zu können. Bei der Herstellung von Deep Fake-Videos kann es zu Inkonsistenzen bei dem im Tonsignal versteckten Zeitstempel kommen. Kurzum: Neben der Analyse der Videobilder kann insbesondere auch die Auswertung des Tonsignals Deep Fakes enttarnen.

Das Enttarnen von Deep Fakes ist ein Ansatz. Möglicherweise erfolgversprechender ist es, mittelfristig ein System zu etablieren, das die Produktion von Videos und die Wege ihrer Verbreitung lückenlos dokumentiert und damit Fälschungen ausschließt. Eine vergleichbare Technologie wie das digitale Wasserzeichen bei Bildern sollte auch bei Videos einsetzbar sein. Möglicherweise lässt sich dazu auch die Blockchain-Technologie¹⁸ nutzen, mit der sich nachträgliche Manipulationen an Dokumenten aller Art, mithin auch Videos, ausschließen lassen.

Neben der technischen Abwehr von Deep Fakes besteht in jedem Fall auch Handlungsbedarf in juristischer Hinsicht. Es gibt zwar keinen rechtsfreien Raum, denn Fälschungen, etwa von Fotos, haben eine lange Tradition, auf die der Rechtsstaat bereits reagieren musste. Bislang fehlt es jedoch in Deutschland an gesetzlichen Regelungen, die eindeutig eine Grenze zwischen einer zulässigen Bearbeitung von Videos und deren Verbreitung und unzulässigen Täuschungen ziehen. Mit Blick auf die wachsende Problematik ist es notwendig, dass der Gesetzgeber sich diesem Thema zuwendet.

Gesetzlicher
Regelungsbedarf

Ein wichtiger Ansatzpunkt sind die Verbreitungsmechanismen, da die gesellschaftliche Wirkung von Manipulationen mit wachsendem Verbreitungsgrad zunimmt. Durch entsprechende gesetzliche Regelungen sollten Social Media-Betreiber in die Pflicht genommen werden, stärker auf Manipulationen zu kontrollieren.

Deep Fakes können offensichtlich ein scharfes Schwert in der Hand von Satirikern sein. Wie weit darf aber Satire hier gehen? Welche Formen von Deep Fakes werden durch die Freiheit der Kunst garantiert? Und wie steht es um die Freiheit der Wissenschaft? Ein lebensecht wirkender Albert Einstein, der im Video eine Vorlesung über die Relativitätstheorie hielt, wäre ein didaktischer Knaller, Politikern verfälschte Aussagen in den Mund zu legen jedoch ein erhebliches Risiko für die politische Stabilität.

Es sollte eine kluge Grenzlinie gezogen werden, die den Einsatz von Deep Fakes in Kunst, Bildung und Wissenschaft ermöglicht und transparent macht, andererseits Missbrauch unter

Strafe stellt. Weitere offene Fragen sind, ob Deep Fake-Software ab einem bestimmten Grad der Perfektion reglementiert werden sollte und wie die Interessen von durch Deep Fakes geschädigten Privatpersonen gewahrt werden können.

Im Übrigen kann jeder Einzelne einen, wenn auch kleinen Beitrag im Kampf gegen Deep Fakes leisten – durch Zurückhaltung beim Hochladen eigener Fotos ins Netz.

Bei den Deep Fakes ist das Rennen zwischen Täuschen und Enttarnen offen. Doch wenn es technisch möglich sein sollte, Fälschungen von Videos nachzuweisen, dann dürfte gleichwohl der Aufwand dafür so groß sein, dass er nicht von jedem Einzelnen geleistet werden kann. Hier könnte sich für klassische Medienunternehmen die Chance eröffnen, als Trustcenter im digitalen Informationszeitalter aufzutreten und dafür zu garantieren, nur Videos (und natürlich ebenso Textnachrichten) zu verbreiten, die garantiert keine Fakes sind. Neben der technischen Analyse können hier auch Expertenwissen, Quellenanalyse und weitergehende journalistische Recherchen eine Rolle spielen, um die Authentizität von Videomaterial zu garantieren.

Und für eine solche Garantie wären möglicherweise mehr Menschen als heute bereit, einen Obolus zu entrichten. Nicht zuletzt können und sollten Medien auch durch die Produktion eigener, authentischer Videos am Ort des Geschehens dafür sorgen, dass sie journalistisch hochwertiges und garantiert unverfälschtes Material verbreiten. Die Deep Fake-Problematik könnte also letztlich das Vertrauen in die Medien stärken – das ist die optimistische Perspektive. Wenn allerdings der zu befürchtenden Welle von Deep Fakes nicht rechtzeitig und wirksam begegnet wird, könnte es auch zu einer weiteren Schwächung der Glaubwürdigkeit von Medien kommen. Deep Fakes sind also in gewisser Weise die Gretchenfrage für die Zukunft unabhängiger Medien.

Eine Kontrolle der Authentizität von relevantem Videomaterial durch unabhängige Institutionen wie die Medien wäre jedenfalls gegenüber der durch staatliche Stellen zu bevorzugen. Diese wird es jedoch in gewissem Umfang ebenfalls geben, insbesondere im Bereich der Forensik und Strafverfolgung. Je nach Aufwand und Höhe der Kosten für das Enttarnen von Deep Fakes sollte darüber nachgedacht werden, ob und wie sich der Staat bei Medien an der Finanzierung dieser für die Gesellschaft und das demokratische System überaus wichtigen Aufgabe beteiligt.

Trustcenter im
digitalen Zeitalter

Zukunft unab-
hängiger Medien

Staatliche Kontrolle

- 1 Norbert Lossau, Konrad-Adenauer-Stiftung (2017): <https://www.kas.de/de/analysen-und-argumente/detail/-/content/gefahrden-fake-news-die-demokratie>
- 2 Ian Goodfellow, Yoshua Bengio, Aaron Courville: Deep Learning. Cambridge, Massachusetts: MIT Press. (2016)
- 3 Sven Felix Kellerhoff, WELT (2012): <https://www.welt.de/kultur/history/article13794477/Wie-Stalin-und-Ulbricht-Fotos-retuschieren-liessen.html>
- 4 <https://watermarking.sit.fraunhofer.de/de/wasserzeichen.html>
- 5 <https://mixed.de/ki-deepfake-selbst-erstellen-so-geht-es-so-lange-dauert-es/>
- 6 <https://www.youtube.com/watch?v=oXr2FwbE0nUh>
- 7 <https://www.youtube.com/watch?v=6xVKyBdXUCM>
- 8 http://openaccess.thecvf.com/content_CVPRW_2019/papers/Media%20Forensics/Agarwal_Protecting_World_Leaders_Against_Deep_Fakes_CVPRW_2019_paper.pdf
- 9 <https://www.youtube.com/watch?v=PctUS31px40>
- 10 <https://www.descript.com/lyrebird-ai?source=lyrebird>
- 11 <https://www.bigdata.fraunhofer.de/content/dam/bigdata/de/documents>
- 12 <https://www.buzzfeednews.com/article/charliwarzel/the-terrifying-future-of-fake-news>
- 13 Norbert Lossau/Oliver Bendel, WELT (2019): <https://www.welt.de/wissenschaft/plus197745219/Deep-Fakes-Wie-erkennt-man-gefaelschte-Videos-im-Internet.html>
- 14 <https://www.ssi.gouv.fr/en/actualite/the-anssi-and-the-bundesamt-fur-sicherheit-in-der-informationstechnik-bsi-present-the-second-edition-of-the-common-situational-picture/>
- 15 <https://aifoundation.com/>
- 16 <https://arxiv.org/abs/1901.08971> und <https://arxiv.org/abs/1812.02510>
- 17 <https://www.idmt.fraunhofer.de/>
- 18 <https://www.opendemocracy.net/en/democraciaabierta/c%C3%B3mo-usar-el-poder-de-blockchain-para-combatir-videos-deepfake-en/>

Letzter Abruf für die genannten Internet-Links: 2.1.2020.

Impressum

Der Autor

Dr. Norbert Lossau

Wissenschaftsjournalist, Mitglied des Beirats der Wissenschaftspressekonferenz WPK

Konrad-Adenauer-Stiftung e. V.

Dr. Norbert Arnold

Hauptabteilung Analyse und Beratung

T: +49 30 / 26 996-3504

norbert.arnold@kas.de

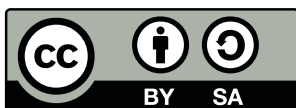
Postanschrift: Konrad-Adenauer-Stiftung e. V., 10907 Berlin

Herausgeberin: Konrad-Adenauer-Stiftung e. V., 2020, Berlin

Gestaltung: yellow too Pasiek Horntrich GbR

Satz: Janine Höhle, Konrad-Adenauer-Stiftung e. V.

ISBN 978-3-95721-626-7



Der Text dieses Werkes ist lizenziert unter den Bedingungen von „Creative Commons Namensnennung-Weitergabe unter gleichen Bedingungen 4.0 international“, CC BY-SA 4.0 (abrufbar unter: <https://creativecommons.org/licenses/by-sa/4.0/legalcode.de>).

Bildvermerk Titelseite

© Soryn, stock.adobe.com