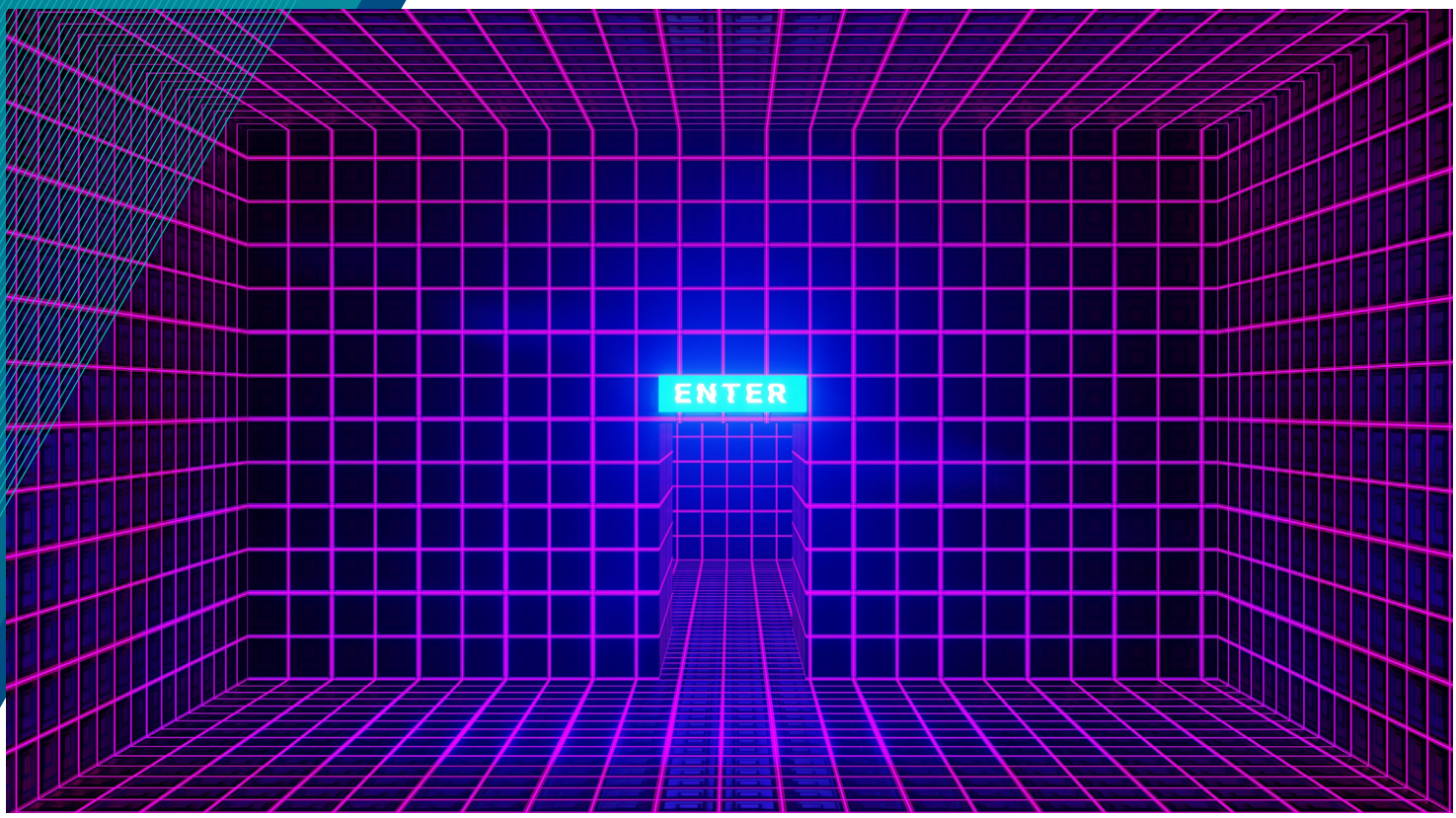
Nr. 499 / März 2023
Analysen & Argumente

KONRAD ADENAUER STIFTUNG



Manipulation und Desinformation im Metaverse

Welche Herausforderungen gibt es und wie ist ihnen zu begegnen?

Christopher Nehring

- Die neuen virtuellen Kommunikationsräume sind die bislang immersivste Form der digitalen Welt. In dieser Umgebung findet eine noch stärkere Vermischung von Unterhaltung und Information statt. Daher können Desinformation sowie Manipulation *realer* und *intensiver* aufgenommen werden.
- Zudem können neue technologische Entwicklungen (zum Beispiel Deepfake-Technologien oder virtuelle Influencer) die Wirkung von Desinformation verstärken.
- Zwar haben die einzelnen Anbieter und Betreiber der virtuellen Räume die Autorität und Kontrollbefugnis, doch werden diese nur unzureichend ausgeübt. Um der Dezentralität gerecht zu werden, braucht es zusätzliche internationale Standards und Regeln, die von unabhängigen Stellen überwacht und durchgesetzt werden.
- Medien, Journalistinnen und Journalisten, Behörden und Anbieter seriöser Informationen sind bislang noch nicht oder nur unzureichend in den virtuellen Kommunikationsräumen präsent. Sie sollten die Kommunikationsräume proaktiv besetzen („Prebunking“ und strategische Kommunikation) und Informationsangebote schaffen.

Inhaltsverzeichnis

Statt „flacher", zweidimensionaler Oberflächen haben einige Anbieter, wie Meta, Rockstar Games oder Decentraland Foundation, virtuelle Kommunikationsräume geschaffen, die bis auf den Geschmacks- und Geruchssinn alle Sinne ansprechen und den Nutzerinnen und Nutzern realitätsnahe, dreidimensionale Erfahrungen bieten. Die Räume werden als „Metaversum"[1] bezeichnet. Partizipation, Interaktion, an die Realität angenäherte Erfahrbarkeit und Sozialität sind grundlegende Eigenschaften dieser technologischen Entwicklung. Sehr stark zielen diese Räume auf Emotionen und Wahrnehmungen ab. So ermöglichen sie unter anderem eine stärkere Vermischung von Inhalten und Unterhaltung (*Gamefication und Infotainment*).

Doch bergen diese immersiven Räume Herausforderungen und Risiken für die Gesellschaft: Manipulierte oder falsche Informationen und Inhalte lassen sich nicht nur schnell und nahezu unkontrolliert verbreiten, sondern wirken viel realistischer auf konsumierende Personen als im zweidimensionalen Raum. Ein frühzeitiges Gegensteuern ist besonders wichtig, um Fehler, wie sie beim Umgang mit den Sozialen Medien gemacht wurden, zu vermeiden.

1. Zu wenig regulierte Kommunikationsräume

Für ein besseres Verständnis dieser Technologie gilt es grundsätzlich zu verstehen, dass es nicht das *eine* Metaverse gibt. Stattdessen gibt es unzählige immersive Räume und Nutzungsmöglichkeiten. „Altspace VR", eine von Microsoft betriebene Plattform virtueller Räume, ist ein Beispiel: In einem Raum findet ein Livekonzert statt, in einem anderen gibt es Weiterbildungsangebote und in einem dritten werden Bibelkreise angeboten.[2] Jede Nutzerin und jeder Nutzer kann – vergleichbar mit Facebook-Gruppen, Whatsapp-Gruppen oder Chat-Räumen – eine eigene „Welt" kreieren oder eine bestehende kopieren. Diese sind zunächst nur für die Person selbst sichtbar und werden erst durch Einladung für andere zugänglich. So besteht die Möglichkeit, versteckte beziehungsweise geheime virtuelle Räume zu schaffen, die für private, kommerzielle, kriminelle oder politische Zwecke gebraucht beziehungsweise missbraucht werden können. Bis auf vereinzelte Community-Standards[3] üben die Anbieter ihre Autorität und Kontrollbefugnis bisher nur unzureichend aus. Meta oder Microsoft lehnen beispielsweise die alleinige Verantwortung für Sicherheitsfragen rund um die immersiven Kommunikationsräume ab und verweisen bei der Regulierung auf ihre Standards[4] und die einschlägige Gesetzgebung der Europäischen Union (*Digital Services Act*[5] und den *Strengthened Code of Practice on Disinformation* von 2022[6]). Der Digital Services Act trat erst am 16. November 2022 in Kraft und wird derzeit in Kommunikationsräumen noch nicht umgesetzt. Zudem erfasst der örtliche Anwendungsbereich der Verordnung lediglich

Die Community-Standards der Anbieter können nur der Anfang der Kontrolle sein.

das EU-Hoheitsgebiet. Bisher gibt es weder auf EU-Ebene noch auf Ebene der Nationalstaaten spezifische Regeln und Richtlinien, die auf die Besonderheiten der dreidimensionalen virtuellen Kommunikationsräume eingehen.

Nick Clegg, Leiter der Unternehmenskommunikation von Meta, verglich solche privat erstellten, nur auf persönliche Einladung betretbaren Räume mit privaten Abendessen in der physischen Realität.[7] Dabei gehe es, so Clegg, hauptsächlich darum, Privatsphäre und Datenschutz zu garantieren; ein Selbstversuch von Buzzfeed-Journalistinnen und -Journalisten in den USA zeigte jedoch, dass diese Räume ohne jegliche Intervention von Meta für die Verbreitung von Desinformation und Verschwörungstheorien genutzt werden können. Buzzfeed erstellte einen privaten Raum und postete in diesem strafrechtlich relevante Inhalte. Selbst nachdem sie diese bei Meta meldeten, wurden die Inhalte als unbedenklich eingestuft.[8]

Um den Herausforderungen in den immersiven Kommunikationsräumen begegnen zu können, muss die Frage, wer die **Autorität und Kontrolle** ausübt beziehungsweise durchführt **(„Governance-Frage“)**, geklärt werden. Wie bei den Plattformen sozialer Medien erfordert vor allem die Dezentralität der immersiven Kommunikationsräume neben einheitlicher internationaler Standards und Regulierung auch international abgestimmte und organisierte Kontrollen, Rechtsfolgenregelungen und zugleich deren Durchsetzung.

Interpol und Europol haben die Risiken der immersiven Räume auf die Gesellschaft erfasst und eine Aufklärungskampagne initiiert. Interpol richtete eine Repräsentanz in einem Meta versum ein, in dem Trainings, Weiterbildungen und ein gezielter Austausch zwischen Strafverfolgungsbehörden weltweit stattfinden soll.[9] Noch einen Schritt weiter ging Europol und veröffentlichte im Oktober 2022 den Bericht *Policing in the metaverse: what law enforcement needs to know*, der nicht nur eine Gefahrenanalyse des Metaverse, sondern unter anderem einen expliziten Aufruf zur Einrichtung von Präsenzen europäischer Polizeibehörden enthält.[10] Es sind demnach **klare Regeln** und von den Herstellern **unabhängige Kontrollen** erforderlich. So könnte für die Überwachung, Regulierung und Gestaltung globaler digitaler Informationsräume wie dem Metaverse eine **internationale Organisation** eingerichtet oder auf eine bestehende Organisation wie die Internationale Fernmeldeunion derartige Kompetenzen übertragen werden.

Die Strafverfolgungsbehörden erkennen die Gefahrenpotentiale.

2. Desinformation in neuen virtuellen Kommunikationsräumen wirkt realistischer und intensiver

Informationen und Erfahrungen, die Nutzerinnen und Nutzer in den virtuellen Kommunikationsräumen aufnehmen beziehungsweise machen, werden nicht nur als realistisch, sondern als besonders intensiv wahrgenommen. Seit über 20 Jahren forschen Expertinnen und Experten im Bereich der kognitiven Psychologie an und mit virtuellen Realitäten (VR). Studien zeigen, dass VR im menschlichen Gehirn Emotionen und Eindrücke auslösen kann, die sich nicht von jenen der physischen Realität unterscheiden.[11] So können zum Beispiel im Extremfall Traumata oder Angstzustände durch VR-Erlebnisse hervorgerufen werden.[12] Versuche mit exzessiver VR-Nutzung zeigten außerdem, dass die Konsumentinnen und Konsumenten nach stundenlangem Aufenthalt in einer virtuellen Realität Probleme hatten, zwischen Erlebnissen, Erinnerungen und Wahrnehmung in virtuellen und physischen Realitäten zu unterscheiden.[13] In einem Experiment an der Universität Stanford konnten Kleinkindern mithilfe von VR erfolgreich falsche Erinnerungen suggeriert werden.[14] Im Vergleich zu heutiger digitaler Desinformation in sozialen Medien wirkt Desinformation in den neuen immersiven Kommunikationsräumen intensiver und kann somit gefährlicher werden.[15]

Um das Gefahrenpotenzial zu minimieren, sollten Nutzerinnen und Nutzer über die technologischen Aspekte und die Wirkungen beziehungsweise die Wirkmöglichkeiten immersiver Kommunikationsräume sowie deren Risikoeffekte aufgeklärt und geschult werden. **Frühzeitige Medienbildung** ist besonders wichtig. Es empfiehlt sich, die Medienbildung über diese Kommunikationsräume auch in diesen Räumen stattfinden zu lassen, um die speziellen technischen Eigenschaften und Wirkungen aktiv erfahrbar zu machen. Erste Schritte in diese Richtung geht derzeit die XR Foundation[16], die unter anderem Kurse zu Medienbildung über das Metaversum unterstützt.[17] Diese Initiativen sollten von **unabhängigen Stellen**, zum Beispiel zivilgesellschaftlichen Akteuren, Medienanstalten und wissenschaftlichen Institutionen, aufgegriffen und weiterentwickelt werden. Die proaktive Besetzung der Kommunikationsräume **(strategische Kommunikation)** ist ein geeignetes Instrument, um gegen die Verbreitung von Desinformation vorzugehen.

Durch proaktive Maßnahmen kann Desinformation vermieden werden.

3. Neue technologische Entwicklungen wirken effektsteigernd

A) Deepfakes

Kommt Deepfake-Technologie[18] in immersiven Kommunikationsräumen zum Einsatz, können sich negative Effekte und Wirkungen der Technologie verstärken. Ein ohnehin schwer als solches zu erkennendes Deepfake-Video wirkt in einer immersiven Umgebung noch realistischer und intensiver als in zweidimensionalen digitalen Räumen. Darüber hinaus gibt es in der virtuellen Realität bislang keine unabhängigen Überprüfungen und Kontrollen von Authentizität und Identität. Falsche Identitäten sowie Aussagen können uneingeschränkt wirken. Besonders groß ist das schädliche Potenzial der Deepfake-Technologie bei Informationsmanipulation und sogenanntem Mikrotargeting.[19] Politikerinnen und Politiker, Aktivistinnen und Aktivisten, aber auch Werbefiguren können in ihrer Optik, Mimik, Gestik, in ihrem Auftreten und ihren Botschaften an das Verhalten der Zielgruppe angepasst werden, um Sympathien zu erzeugen und deren Wahlverhalten beeinflussen.[20] Die verwendete Software und Hardware für die Nutzung der immersiven Kommunikationsräume setzen auf eine noch extensivere Sammlung von persönlichen Daten (zum Beispiel Augen-, Ohren- oder Fingerscans). Hierdurch stehen mehr Daten und Informationen über die Nutzerinnen und Nutzer zur Verfügung, die das Mikrotargeting verbessern und eine noch größere Individualisierung ermöglichen.[21] Deepfake-Technologie ist für Mimikry-Strategien[22] das wirksamste Instrument. Bereits Anfang der 2000er-Jahre zeigten Studien, dass sich Gesichter von Politikerinnen und Politikern mithilfe von Software bis zu 40 Prozent an die ihrer Betrachterinnen und Betrachter anpassen lassen, ohne dass es diesen auffällt. Die unbewusste Anpassung (Mimikry) verleitete dazu, den Politikerinnen und Politikern aufgrund der Ähnlichkeit zu den Betrachtenden mehr Sympathie entgegenzubringen.[23] Andere Studien mit KI-basierter VR zeigen, dass Studierende einem Professoren-Avatar, der den Nutzenden visuell angepasst war und Augenkontakt hielt, größere Aufmerksamkeit schenkten und mehr Sympathie entgegenbrachten.[24] So ermöglicht der technologische Einsatz den jeweiligen Akteurinnen und Akteuren, sich zeitgleich und zudem individuell an jedes einzelne Mitglied der Veranstaltung anzupassen, während sie sich an ein unbegrenzt großes Publikum richten können, ohne dass das Publikum dies wahrnimmt.[25]

B) KI-Influencer

Menschen („Trolle“) oder Computerprogramme („Bots“) sind ein effektives Mittel zur Verbreitung von Desinformation in digitalen Räumen. Die nächste Entwicklungsstufe sind in diesem Kontext sogenannte „virtuelle Influencer“ oder „virtuelle Meinungsmacher“ (*virtual*

key opinion leaders, V-KOLs). Dabei handelt es sich um fiktive virtuelle Wesen, die mithilfe von künstlicher Intelligenz geschaffen werden und ein realistisch anmutendes, menschliches Äußeres samt dazugehöriger Lebensgeschichte haben. In vielen Ländern, wie China, den USA, Indien, Japan, Südkorea oder Brasilien, sind virtuelle Influencerinnen und Influencer in den vergangenen Jahren überaus erfolgreich und ziehen Millionen Follower an.[26] Auch Meta hat ihnen bereits den Zugang zu und dadurch den Auftritt auf Instagram ermöglicht, was sie für Werbekunden attraktiv macht.[27] In China gab die virtuelle Influencerin „Luo Tianyi" als Hologramm ein Livekonzert mit dem weltbekannten Pianisten Lang Lang[28] und in Japan bewarb „Imma" die Eröffnung einer Ikea-Filiale.[29] Diese Persönlichkeiten lassen sich ebenso für politische Kampagnen und die Verbreitung von manipulierten Informationen einsetzen. Sie können jedwede Botschaft verbreiten, haben keine eigene Moral, Meinung, Haltung oder Gefühle und können an jedem Tag 24 Stunden lang tätig sein. Wie Expertinnen und Experten bestätigen, interessieren sich Regierungen und Staaten für den politischen Einsatz KI-basierter, virtueller Wesen.[30] Welche Botschaften sie verbreiten, hängt allein von den Programmiererinnen und Programmierern sowie der Lernumgebung der KI ab. 2021 kam es während einer Messe in Barcelona zu einem Eklat, als der für immersive Welten konzipierte Bot „David" der Firma Sensorium bei einer Demonstration Corona-Verschwörungstheorien verbreitete, die die KI offensichtlich beim automatisierten Lernen im Internet aufgenommen hatte.[31]

Effektive Maßnahmen gegen die negativen Folgen im Zusammenhang mit dieser neuen Technologie und der gezielten Verbreitung von Desinformation in immersiven Kommunikationsräumen beruhen wiederum auf **technologischen Lösungsansätzen** und gleichen den Maßnahmen, die im zweidimensionalen Raum gefordert werden. Einerseits kann der Einsatz bestimmter Technologien, zum Beispiel Deepfakes, **verboten und unter Strafe** gestellt werden.[32] Alternativ bedarf es einer **Kennzeichnungspflicht (beispielsweise digitale Wasserzeichen oder Signaturen) und klaren Regeln** für den Einsatz solcher Technologien, ganz gleich ob für politische oder für kommerzielle Zwecke. Zudem braucht es **Software-Lösungen zur (automatisierten) Erkennung** der eingesetzten Deepfake-Technologie.[33]

4. Fazit

Die neuen virtuellen und immersiven Kommunikationsräume stecken hinsichtlich ihrer Entwicklung noch am Anfang und bergen ein großes Potenzial an Chancen und Risiken. Unzureichende Regulierung und Aufsicht aber auch technologische Entwicklungen wie Deepfakes oder KI-Bots machen diese Räume anfällig für eine noch tiefgreifendere Informationsmanipulation und deren Wirken auf das Individuum als es bisher ohnehin schon der Fall ist. Um dieser Gefahr zu begegnen, müssen allen Schwachstellen frühzeitig Lösungsansätze gegenübergestellt werden.

1 Vgl.: Matthew Ball, 2022: The Metaverse. And How It Will Revolutionize Everything, New York.

2 Microsoft, 2023: Altspace VR. https://account.altvr.com/channels/popular (zuletzt geprüft: 15.3.2023).

3 Microsoft verwies in Bezug auf „Altspace VR" zum Beispiel auf geltende Community Standards (https://learn.microsoft.com/en-us/windows/mixed-reality/altspace-vr/community/community-standards), die hauptsächlich auf Belästigung und Hate Speech abzielen. Bei Verstoß können User gemeldet und/oder gesperrt werden. Für die Etablierung und Durchsetzung von Standards sind derzeit ausschließlich die Betreiberfirmen zuständig.

4 Siehe z. B. das Statement von Microsoft: https://blogs.microsoft.com/blog/2022/03/28/the-metaverse-is-coming-here-are-the-cornerstones-for-securing-it/; von Meta: https://about.fb.com/news/2021/09/building-the-metaverse-responsibly/.

5 Julian Jaursch, 2022: Der DSA gilt auch „im Metaverse". In: Tagesspiegel.de, 14.12.2022. https://background.tagesspiegel.de/digitalisierung/der-dsa-gilt-auch-im-metaverse (zuletzt abgerufen: 15.3.2023).

6 European Commission, 2022: 2022 Strenghened Code of Practice on Disinformation. https://digital-strategy.ec.europa.eu/en/library/2022-strengthened-code-practice-disinformation (zuletzt abgerufen: 15.3.2023).

7 Nick Clegg, 2022: Making the metaverse: What it is, how it will be built, and why it matters. https://nickclegg.medium.com/making-the-metaverse-what-it-is-how-it-will-be-built-and-why-it-matters-3710f7570b04 (zuletzt abgerufen: 15.3.2022).

8 Emily Baker-White, 2022: Meta Wouldn't Tell Us How It Enforces Ist Rules in VR, So We Ran A Test To Find It Out. In: Buzzfeednews.com, 11.2.2022. https://www.buzzfeednews.com/article/emilybakerwhite/meta-facebook-horizon-vr-content-rules-test (zuletzt abgerufen: 15.3.2022).

9 Interpol, 2022: Interpol launches first global police Metaverse: https://www.interpol.int/News-and-Events/News/2022/INTERPOL-launches-first-global-police-Metaverse, 20.10.2022.

10 Europol, 2022: Policing in the metaverse. What lawinforcement needs to know. https://www.europol.europa.eu/cms/sites/default/files/documents/Policing%20in%20the%20metaverse%20-%20what%20law%20enforcement%20needs%20to%20know.pdf (zuletzt abgerufen: 15.3.2022).

11 Vgl. z. B.: Jeremy Bailenson, 2018: Experience on Demand. What Virtual Reality Is, How It Works, and What It Can Do, New York.

12 Vgl.: Nilufar Baghaei / Vibhav Chitale / Andrej Hlasnik / Lehan Stemmet / Hai-Ning Liang / Richard Porter, 2021: Virtual Reality for Supporting the Treatment of Depression and Anxiety: Scoping Review. https://pubmed.ncbi.nlm.nih.gov/34554097/ (zuletzt abgerufen: 15.3.2022).

13 Franck Steinicke / Gerd Bruder, 2014: A Self-Experimentation Report about Long-Term Use of Fully-Immersive Technology. https://dl.acm.org/doi/10.1145/2659766.2659767 (zuletzt abgerufen: 15.3.2022).

14 Kathyn Segovia / Jeremy Bailenson, 2009: Virtually True: Children's Acquisition of False Memories in Virtual Reality. https://www.tandfonline.com/doi/abs/10.1080/15213260903287267 (zuletzt abgerufen: 15.3.2022).

15 Vgl.: Jeremy Bailenson / Jim Blasovich, 2011: Virtual Reality and Social Networks Will Be a Powerful Combination. https://hci.stanford.edu/courses/cs047n/readings/bailenson-ieee.pdf (zuletzt abgerufen: 15.3.2022).

16 XR Association: https://xra.org/about/.

17 Z. B.: Everfi, o. D.: Get Digital: Safety in the Metaverse. https://everfi.com/courses/k-12/get-digital-safety-in-the-metaverse/ (zuletzt abgerufen: 15.3.2022).

18 Unter Deepfakes sind durch künstliche Intelligenz generierte Manipulationen oder Fälschungen von Bild- und Tondateien zu verstehen. Für die menschliche Wahrnehmung sind diese praktisch nicht mehr zu erkennen. Für Aufsehen sorgten beispielsweise Deepfakes, die mutmaßlich von russischen Geheimdiensten im Zuge des Krieges gegen die Ukraine erstellt wurden, etwa als ein falscher Präsident Selenskyj seine Truppen zur Aufgabe aufrief und ein falscher Vitali Klitschko mit Bürgermeistern in ganz Europa zoomte oder ein falscher ukrainischer Premierminister Schmyhal beim türkischen Drohnenhersteller Bayraktar Lieferungen abbestellen wollte; vgl. ausführlich: Hany Farid / Hans-Jakob Schindler, 2020: Deepfakes. Eine Bedrohung für Demokratie und Gesellschaft. Konrad-Adenauer-Stiftung e. V. (Hrsg.), Berlin. https://www.kas.de/documents/252038/7995358/Deepfakes+-+Eine+Bedrohung+f%C3%BCr+Demokratie+und+Gesellschaft.pdf/c4c7bc69-a5b6-8141-dca1-bb1f6869f806?version=1.3&t=1597323975005 (zuletzt abgerufen: 15.3.2022).

19 Mikrotargeting bezeichnet den Einsatz von zielgerichteten, auf einzelne Zielgruppen maßgeschneiderten Kommunikationsstrategien, die durch Datensammlung und Analyse (insbesondere von über Social Media gewonnenen Informationen), erstellt werden; z.B.: Fabian Prietzel, 2020: Big Data is watching you: Persönlichkeitsanalyse und Microtargeting auf Social Media. In: Markus Appel (Hrsg.), 2020: Die Psychologie des Postfaktischen, Berlin, S. 81-90.

20 Rand Waltzman, 2022: Facebook Misinformation is Bad Enough. The Metaverse Will Be Worse. In: Rand.org, 22.8.2022. https://www.rand.org/blog/2022/08/facebook-misinformation-is-bad-enough-the-metaverse.html (zuletzt abgerufen: 15.3.2022).

21 Vgl.: Europol, 2022.

22 In der Psychologie bezeichnet Mimikry die Nachahmung von Menschen durch andere Menschen. Diese kann z. B. Gesichtsausdrücke (Mimik) und Körpersprache betreffen; vgl. Jessica Lakin / Tanya Chartrand, 2003: Using

Nonconscious Behavioral Mimicry to Create Affiliation and Rapport. In: Psychological Science 4/14 2003. https://doi.org/10.1111/1467-9280.14481; zum Einsatz von Deepfake-Technologie für Mimikry im Metaverse siehe: Rand Waltzman, 2022.

23 Ebd.

24 Jeremy Bailenson, 2018, S. 44-76.

25 Die großen Tech-Firmen, z. B. Microsoft, sind sich dieses Risikos bewusst, verweisen jedoch bislang einzig auf die gemeinsame Entwicklung von Sicherheitsstandards ohne konkrete Maßnahmen vorzuschlagen; vgl: Microsoft, 2022. The metaverse is coming. Here are the cornerstones of securing it. https://blogs.microsoft.com/blog/2022/03/28/the-metaverse-is-coming-here-are-the-cornerstones-for-securing-it/ (zuletzt abgerufen: 15.3.2022).

26 Vgl.: Astrid Hiorts, 2022. 5 Times Virtual Influencers Entered the „Real World". In: Virtualshumans.org, 25.1.2022. https://www.virtualhumans.org/article/5-times-virtual-influencers-entered-the-real-world (zuletzt abgerufen: 15.3.2022).

27 Vgl.: Christopher Travers, 2022. Instagram Has Verified 35 Virtual Influencers. In: Virtualhumans.org, 24.3.2022. https://www.virtualhumans.org/article/instagram-has-verified-35-virtual-influencers (zuletzt abgerufen: 15.3.2022).

28 Vgl.: Victor Tangermann, 2019. Thousands of Chinese Fans Paid to See a Virtual Hologram Singer. In: Futurism.com, 4.3.2019. https://futurism.com/virtual-idol-hologram-luo-tianyi-lang-lang-live (zuletzt abgerufen: 15.3.2022).

29 Vgl.: Andrew Webster, 2020. Ikea turned a virtual influencer into a physical installation. In: Theverge.com, 31.8.2020. https://www.theverge.com/2020/8/31/21408626/ikea-tokyo-imma-virtual-influencer (zuletzt abgerufen: 15.3.2022).

30 Experten-Interview, November 2022 (Der Gesprächspartner bestand auf Anonymität).

31 Vgl.: Jillian Deutsch / Naomi Nix / Sarah Kopit, 2021: Misinformation Has Already Made Its Way to the Metaverse. In: Bloomberg.com, 15.12.2021. https://www.bloomberg.com/news/articles/2021-12-15/misinformation-has-already-made-its-way-to-facebook-s-metaverse?leadSource=uverify%20wall (zuletzt abgerufen: 15.3.2022).

32 Vgl. wiederum für Deepfake-Technologien: Hany Farid / Hans-Jakob Schindler, 2020.

33 Bislang hinkt Deepfake-Erkennungssoftware der Entwicklung von Deepfake-Erstellungssoftware hinterher. Andere Initiativen, z. B. das von Microsoft, BBC, CCN und anderen Partnern betriebene „Project Origin", versuchen, durch die Etablierung „digitaler Wasserzeichen" in Original-Medienbeiträgen sicherzustellen, dass Manipulationen und Veränderungen erkannt und sichtbar gemacht werden können.

Impressum

Der Autor

Dr. Christopher Nehring – Gast-Dozent des KAS-Medienprogramms Südosteuropa an der Universität Sofia zum Themengebiet „Medien, Desinformation und Geheimdienste“.

Konrad-Adenauer-Stiftung e. V.

Ferdinand Alexander Gehringer
Innere- und Cybersicherheit
Analyse und Beratung
T +49 30 / 26 996-3460
ferdinand.gehringer@kas.de

Postanschrift: Konrad-Adenauer-Stiftung, 10907 Berlin

Herausgeberin: Konrad-Adenauer-Stiftung e. V. 2021, Berlin
Gestaltung & Satz: Franziska Faehnrich, yellow too, Pasiek Horntrich GbR
Die Printausgabe wurde bei copy print Kopie & Druck GmbH, Berlin gedruckt.
Printed in Germany.
Hergestellt mit finanzieller Unterstützung der Bundesrepublik Deutschland.

ISBN 978-3-98574-141-0