

Die Verbreitung von Fake News als politisches Instrument ist längst Thema im politischen Diskurs. Dabei gilt es auch, auf technologische Neuerungen zu reagieren, die das Potenzial von Desinformationskampagnen fortlaufend erweitern und somit unsere innere Sicherheit bedrohen. Nael Semaan sprach mit Dr. Hans-Jakob Schindler, dem Senior Director des Counter Extremism Project, über die „neue Superwaffe der Fake News“ – sogenannte Deepfakes.

*Ai: Herr Schindler, Deepfakes verbreiten sich inzwischen all-
täglich und sehr rasant im Netz. Dabei ist nur noch schwierig
herauszufinden, welches Foto oder Video wirklich echt ist und
welches nicht. Deepfakes sind sozusagen die neue Superwaffe der
Fake News – jetzt kann man nicht nur falsche Informationen
verbreiten, sondern sie auch noch glaubwürdig aussehen lassen.
Aber was genau sind Deepfakes und wie fügen sie sich ein in eine
der Desinformation ausgesetzten Politik?*

Hans-Jakob Schindler: Durch die Verbreitung der sozialen Medien sind in den letzten Jahren Fake News und Deepfakes Teil des alltäglichen politischen Diskurses

geworden. Es ist jedoch wichtig, beide Phänomene klar zu definieren. Fake News sind verbreitete und weiterverbreitende Falschinformationen. Diese kommen in jeglicher Art vor, wie z. B. in Text-, Ton-, Bild- oder Videoaufnahmen. Deshalb sind Fake News ein grundsätzliches gesellschaftliches Problem, dem es auf breiter Front entgegenzuwirken gilt. Deepfakes sind eine Unterkategorie von Fake News. Es handelt sich hierbei um elektronisch modifizierte Videoaufnahmen und Fotos, welche Personen und Ereignisse verändern oder simulieren und die Überzeugungskraft audiovisueller Medien nutzen, um ihre Wirkung zu erzielen.

Grundsätzlich ist die nachträgliche Veränderung audiovisueller Medien kein neues Phänomen. In der Filmindustrie ist die elektronische Veränderung von Videos und Aufnahmen mittlerweile ein akzeptiertes künstlerisches Mittel. So werden mit Spezialeffekten beispielsweise Schauspieler verjüngt oder in alte Filmaufnahmen hineinprojiziert.¹ Der Film „Forrest Gump“ war hier bereits im Jahr 1994 ein Vorreiter dieser Technologie. Das Aufkommen von Deepfakes in Form von Foto-Manipulationen im politischen Diskurs ist ebenfalls nicht unbedingt neu. Zum Beispiel wurden schon Anfang des 20. Jahrhunderts während der stalinistischen Diktatur in der Sowjetunion regelmäßig in Ungnade gefallene Regierungsmitglieder aus offiziellen Fotos retuschiert, um sie auf Befehl Stalins aus der offiziellen Geschichte und dem Gedächtnis des Landes zu entfernen. In der Vergangenheit benötigten solche Operationen ein hohes Maß an technischem und handwerklichem Wissen und Können.

Aktuell gewinnt dieses Phänomen an Bedeutung, da immer stärker die sozialen Medien als Manipulationsinstrument missbraucht werden und neben reinen Falschinformationen auch gezielte politische Manipulation betrieben wird. Zusätzlich hat die technische Entwicklung dafür gesorgt, dass die technologischen Hürden mittlerweile sehr viel

niedriger sind und weder die Möglichkeiten eines Filmstudios noch außergewöhnlich hohe Rechenleistungen erforderlich sind, um Deepfakes zu produzieren. Eine eher spielerische Variante dieser Technologie ist die *Face-Swap*-Funktion, vor allem bekannt durch die Social Media-Applikation Snapchat.²

Ai: Bedeutet das, dass man heutzutage kein Tech-Experte mehr sein muss, um Bilder und Videos zu manipulieren? Deepfakes kann also jeder?

Hans-Jakob Schindler: Prof. Dr. Hany Farid, der Senior Advisor des Counter Extremism Projects (CEP), arbeitet aktuell im Auftrag von CEP und der Konrad-Adenauer-Stiftung an einer Studie zu diesem Thema.³ Er spricht in diesem Zusammenhang von der „Demokratisierung“



Mit Apps zur Manipulation: Die technologischen Hürden für die Produktion von Deepfakes werden immer niedriger.
Quelle: © Steve Marcus, Reuters.

der Deepfake-Technologie. Dies bedeutet, dass die Produktion von Deepfakes von einer weitaus größeren Anzahl von Akteuren betrieben werden kann und sich so ihre Anzahl und politische Schlagkraft erhöhen wird.

Grundsätzlich werden aktuell drei Methoden zur Herstellung von Deepfakes angewandt: *Face Swap*, *Lip Sync* und *Puppet Master*. Bei der *Face Swap*-Methode werden die gesamten Gesichtszüge einer Person auf den Kopf einer anderen Person übertragen. So kann beispielsweise ein Schauspieler Aktionen durchführen, während das Gesicht der Zielperson eingefügt wird, und den Eindruck erwecken, die Zielperson habe diese Aktionen durchgeführt.

Bei der technisch aufwändigeren *Lip-Sync*-Methode werden ausschließlich die Lippenbewegungen in der Aufnahme der Zielperson simuliert, damit sich die Mundbewegungen an einen neuen Sprachtext anpassen. Dieser neue Text ist dann entweder synchron gesprochen oder durch eine synthetisierte Stimme der Zielperson ersetzt. Dies erlaubt, dass eine Aufnahme so manipuliert wird, dass die Zielperson jeden beliebigen Text in dem Video sagt, der für die Manipulation notwendig ist. Hier ist jedoch unter Umständen noch zu erkennen, dass die Lippenbewegungen nicht immer mit den restlichen Gesichtsbewegungen der Zielperson übereinstimmen.

Die *Puppet Master*-Methode ist technisch am aufwändigsten und noch nicht vollkommen zu Ende entwickelt und perfektioniert. Hier wird das Gesicht der Zielperson in dem Video beibehalten, elektronisch können jedoch die Gesichtsbewegungen der Zielperson komplett manipuliert werden. Damit sind nun nicht nur die Stimme, sondern auch die Gesichtsbewegungen komplett synthetisiert. Somit ist für den bloßen Betrachter nicht mehr zu erkennen, dass eine Manipulation vorliegt. Mit dieser Methode ist es nun möglich, eine Zielperson authentisch sprechen zu lassen, da die Bewegungen der Gesichtsmuskeln vollkommen mit denen der Mundbewegungen harmonisieren. Ein Schwachpunkt dieser Methode ist, dass die Gesichtsbewegung der manipulierten Darstellung nicht immer dem natürlichen Bewegungsmuster der Zielperson entspricht – ein wichtiger Punkt für die forensische Erkennung und den Nachweis der Manipulation.

Ai: Was wären denn aktuelle Beispiele für den Einsatz von Deepfakes?

Hans-Jakob Schindler: Aktuell werden illegale Deepfakes hauptsächlich in Betrugs- und Erpressungsfällen eingesetzt.

Mir wurde vor Kurzem von einem Fall berichtet, bei dem ein Unternehmer einen Anruf erhielt und er davon ausging, dass er mit seinem Vorgesetzten gesprochen habe. Die Stimme am Telefon war jedoch synthetisiert. Der Unternehmer gab wichtige Kontodaten an die Stimme am Telefon weiter, was zu einem finanziellen Schaden seiner Firma führte.⁴ Auch im Bereich *non-consensual pornography* werden Deepfakes eingesetzt.⁵ Hier geht es um Erpressungsfälle, bei denen elektronisch manipulierte Aufnahmen eingesetzt werden, welche die Opfer angeblich in peinlichen Situationen zeigen, um für die Nichtweiterverbreitung Schweigegelder zu erpressen.

Eine Unterkategorie der Deepfakes ist die Herstellung künstlicher Identitäten. Hier werden Bilder existierender Personen elektronisch so kombiniert, dass Bilder einer neuen Person entstehen, welche mit keiner anderen lebenden Person übereinstimmen. Für eine

solche neue, einmalige elektronische Identität können dann Lebensläufe geschrieben und biografische Dokumente online bestellt werden. Dies ist eine neue Variante des Identitätsbetrugs. Die künstlichen Identitäten werden dann zur Umfeldaufklärung von Zielpersonen von Spionage oder zur Vorbereitung von *Spear-Phishing*-Operationen eingesetzt.⁶

Zunehmend ist jedoch auch der Einsatz von Deepfake-Videos im politischen Bereich beobachtbar. Im letzten Jahr kursierte ein Video der Sprecherin des amerikanischen Repräsentantenhauses, Nancy Pelosi, auf dem sie angeblich betrunken einen Vortrag gehalten haben soll.⁷ Obwohl dieses Video relativ schnell als falsch erkannt wurde, verdeutlichte dieser Vorfall, wie viel potenzielle politische Sprengkraft die Kombination dieser Technologie mit den Verbreitungsmöglichkeiten der sozialen Medien entfalten kann.

Ai: Welche konkrete Gefahr geht von Deepfakes für unsere Gesellschaft aus? Welche Akteure haben die Absichten und auch die Fähigkeiten, Deepfakes als Waffe einzusetzen?

Hans-Jakob Schindler: Filmaufnahmen haben eine extrem hohe Glaubwürdigkeit, da sie eigentlich eine korrekte Darstellung der Realität sind. Daher ist eine geschickte Manipulation solcher Aufnahmen für kriminelle oder politisch manipulative Zwecke im höchsten Maße problematisch. Sollte sich, wie zu erwarten ist, der aktuelle technische Trend der



Effektive Propagandamaschinerie: Es ist davon auszugehen, dass Terrororganisationen in Zukunft neue Technologien einsetzen, um ihre Manipulationen von Individuen bei der Radikalisierung und Rekrutierung im Internet zu unterstützen. [Quelle: © Dado Ruvic, Reuters.](#)

Vereinfachung und Verbreitung dieser Technologie fortsetzen, wird dies den gesellschaftlichen Grundkonsens darüber, was real und faktisch wahr ist und was nicht, weiter unterminieren. Eine der gravierendsten Auswirkungen ist die *liar's dividend*.⁸ Da es nun möglich ist, Videos nahezu perfekt zu manipulieren, kann immer behauptet werden, dass es sich bei Aufnahmen von peinlichen oder illegalen Handlungen um angebliche Deepfakes handelt. Dies hat Auswirkungen sowohl auf den politischen Diskurs als auch unter Umständen auf juristische Fälle. Daher ist die Entwicklung von Technologien, welche das Erkennen von Deepfakes ermöglichen, eine wichtige gesellschaftliche Aufgabe.

Im politischen Bereich wurden in den letzten Jahren immer wieder Fälle bekannt, in denen autoritäre Regime versuchten, politische Prozesse und Wahlen in demokratischen Staaten zu manipulieren und den gesellschaftlichen Grundkonsens zu erodieren. Die amerikanischen Präsidentschaftswahlen von 2016 sind nur das bekannteste Beispiel in diesem Zusammenhang. Die fortschreitende Verbreitung und Vereinfachung dieser Technologie erlaubt solchen Akteuren den Verzicht auf staatliche Strukturen bei der Umsetzung ihrer Strategien. Wenn nun angebliche Privatpersonen im staatlichen Auftrag Deepfakes produzieren können, wird es umso schwieriger werden, hier eindeutige politische Verantwortlichkeiten zu identifizieren. Dies stellt eine wachsende Gefahr dar, insbesondere da die großen Technologiekonzerne weiterhin so gut wie keine Verantwortung übernehmen, was die Verbreitung solcher Manipulationen angeht. Es sei hier nur an die Anhörung von Mark Zuckerberg im amerikanischen Kongress Ende Oktober 2019 erinnert, bei der er als Vorstandsvorsitzender von Facebook jegliche Verantwortung seiner globalen Plattform für die Verbreitung von politischen Falschinformationen von sich wies.⁹

Ai: Sie beschäftigen sich seit über 20 Jahren mit internationaler Sicherheitspolitik. Dabei lag ein Schwerpunkt Ihrer Arbeit immer auf der Bekämpfung von Terrorismus. Große dschihadistische Organisationen wie der sogenannte Islamische Staat sind bekannt für ihre effektiven Medien- und Propagandastrategien. Wie relevant und umsetzbar ist der Einsatz von Deepfakes für Terrororganisationen?

Hans-Jakob Schindler: Im Moment sind noch keine Fälle bekannt, in denen Terrororganisationen Deepfakes produziert haben. Dies heißt jedoch nicht, dass die effektive Propagandamachinerie von Organisationen wie dem Islamischen Staat (IS) in Zukunft keine solche Technologie einsetzen wird, um ihre Manipulationen von Individuen bei der Radikalisierung und Rekrutierung zu unterstützen.

Konkret kann das Phänomen von Deepfakes bei der juristischen Aufarbeitung von IS-Rückkehrern aus dem Irak und Syrien eine Rolle spielen. Bei einigen Gerichtsverfahren in Europa werden aktuell schwere IS-Verbrechen aufgearbeitet.¹⁰ Dabei werden auch Bild- und Videoaufnahmen als Beweismittel eingesetzt. Die Authentizität dieser IS-Aufnahmen steht zwar außer Frage, bei weniger schweren Fällen könnte jedoch die *liar's dividend* die Beweisführung wesentlich komplizieren. Wenn angeklagte IS-Mitglieder nun unter Umständen glaubhaft behaupten können, dass Film-, Ton- und Bildaufnahmen, auf denen sie bei der Verübung von Verbrechen zu sehen und hören sind, elektronisch manipuliert wurden, wird dies die Anklage vor neue technische Herausforderungen stellen.

Ai: Mit ein wenig Zeit ist es doch oft möglich, die Manipulation eines Bildes oder Videos nachzuweisen. Sollte eine Gegendarstellung und Aufklärung der Fehlinformationen nicht ausreichend sein, um die Wirkung von Deepfakes zu bekämpfen?

Hans-Jakob Schindler: Das zweifelsfreie elektronische Erkennen von Deepfake-Videos ist mittler-

weile möglich, jedoch nur unter erheblichem technischem Aufwand. An der Universität Berkeley wird zurzeit an der Weiterentwicklung solcher Methoden gearbeitet.¹¹ Im Grundsatz beruhen diese Erkennungsmethoden auf der Erstellung von typischen Bewegungsmustern von Personen. Jede Person hat eine Reihe von individuellen Kopf-, Mund- und Muskelbewegungen, welche mit den gesprochenen Worten übereinstimmen und ein Sprach- und Bewegungsmuster ergeben, das einmalig für dieses Individuum ist. Aus der Kombination dieser verschiedenen Faktoren kann ein relativ genaues Muster berechnet werden. Dieses Sprach- und Bewegungsmuster wird dann mit den auf dem Video erkennbaren Mustern verglichen. Da sich bei Manipulationen diese Muster notwendigerweise ändern, kann somit mit hoher mathematischer Wahrscheinlichkeit die Manipulation nachgewiesen werden.

Diese Methode funktioniert jedoch nur, wenn für die in dem verdächtigen Video gezeigte Person ausreichend verlässliche Originalaufnahmen bestehen, aus denen diese Muster errechnet werden können. Daher ist sie aktuell nur für Personen des öffentlichen Lebens anwendbar. Da jedoch für die Produktion von qualitativ hochwertigen Deepfake-Videos ebenfalls eine große Anzahl solcher Originalaufnahmen notwendig ist, stellt diese Methode eine effektive Nachweistechnologie dar.

Solche forensischen Methoden sind insbesondere im juristischen Bereich einsetzbar. Dort besteht im Rahmen der Beweisaufnahme ausreichend Zeit, um den forensischen Nachweis effektiv zu erbringen. Für die effektive Bekämpfung von Deepfake-Videos, die für politische Manipulationen eingesetzt werden, sind solche Methoden ebenfalls hilfreich, jedoch nicht ausreichend. Sozialwissenschaftliche Forschungen haben gezeigt, dass das Aufdecken von Fake News nicht ausreichend ist, um ihre Wirkung erheblich zu mindern.¹² Die Richtigstellung falscher Informationen kommt bei den Konsumenten der Fake News nicht so wirksam an wie die ursprüngliche Falschmeldung. Der gleiche Effekt kann für Deepfake-Videos angenommen werden. Daher kann der forensische Nachweis solcher Manipulationen nur ein Teil eines größeren Maßnahmenkataloges sein.

Ai: Wie sonst kann die Bedrohung durch Deepfakes effektiv bekämpft werden?

Hans-Jakob Schindler: Die effektive Bekämpfung politischer Manipulation durch Deepfake-Videos

muss breit aufgestellt werden. Zunächst ist es wichtig, das gesellschaftliche und politische Bewusstsein darüber zu schaffen, welche Möglichkeiten und Gefahren sich durch diese Technologie ergeben. Es muss deutlich werden, dass nicht jedes Video, das in den sozialen Medien verbreitet wird, glaubhaft ist. Weiterhin sind hier Fragen des Systemvertrauens wichtig. Sinkt das Vertrauen in die Effektivität und Glaubwürdigkeit des politischen Systems, werden Manipulationsversuche einfacher und wird der Schaden durch den Einsatz von manipulativen Deepfake-Videos größer.

Zusätzlich zur Bewusstseinsweiterung bestehen technische Möglichkeiten, den Effekt von Deepfake-Videos einzuschränken. Wenn sich die Industrie darauf einigen könnte, dass bei der elektronischen Aufnahme von originalen Videos automatisch eine elektronische Signatur im Datensatz der Aufnahme verankert wird, könnten somit Originalvideos zertifiziert werden. Diese Technologie, die sogenannten *Hashes*, existiert schon recht lange und wird erfolgreich zum Beispiel bei der Datenübertragung eingesetzt.¹³ Bei jeglicher Veränderung der Ursprungsdatei verändert sich der Hash ebenfalls, was ein erster Hinweis auf eine mögliche Manipulation sein könnte.

Schließlich wird es auch notwendig sein, die Verbreitungsmechanismen von Deepfake-Videos näher zu betrachten. Hiermit sind vor allem die großen Plattformen und Konzerne der sozialen Medien angesprochen. Die Kontrolle über globale Verbreitungsmechanismen mit Hunderten Millionen Nutzern, im Falle von Facebook sogar Milliarden, kann nicht mit einer völligen Verweigerung der Corporate Social Responsibility verbunden werden. Die Sprengkraft gezielter politischer Manipulationen wird entscheidend durch den Verbreitungsgrad erhöht. Das Counter Extremism Project argumentiert hier schon seit einigen Jahren, dass es unumgänglich ist, regulatorische und gesetzgeberische Maßnahmen zu ergreifen. Mit dem Netzwerkdurchsetzungsgesetz (NetzDG) hat die Bundesrepublik einen richtungsweisenden ersten Schritt unternommen, die Plattformbetreiber stärker in die Pflicht zu nehmen.¹⁴ Deepfake-Videos, welche zu kriminellen oder politisch manipulativen Zwecken eingesetzt werden, können als Eingriff in das Recht auf das eigene Bild definiert werden. Sie stellen daher illegale Inhalte im Sinne des Paragraphen 1 Absatz 3 des NetzDG dar und sind potenziell schon jetzt durch das Gesetz abgedeckt.¹⁵ Das Counter Extremism Project wird die Nachbesserung des Gesetzes, die im Jahr 2020 erfolgen soll, aktiv durch sein neues Büro in Berlin unterstützen und begleiten.

Ai: Wir bei der KAS beschäftigen uns ja sehr facettenreich mit dem Thema Deepfakes – beispielsweise in unserem Format Analysen & Argumente, in dem der Wirtschaftsjournalist Norbert Lossau den Handlungsbedarf und mögliche Lösungsansätze zum Umgang mit Deepfakes diskutiert. Spezifisch zum Sicherheitsaspekt von Deepfakes veröffentlichen wir Mitte des Jahres auch gemeinsam mit dem CEP eine Studie. In diesem Rahmen möchte ich Sie nach einem Ausblick auf die Situation in Deutschland fragen: Glauben Sie, dass die kommende Bundestagswahl Ziel für einen Angriff durch Deepfakes werden kann?

Hans-Jakob Schindler: Es steht außer Zweifel, dass in den letzten Jahren von externen Akteuren ver-

sucht wurde, den politischen Prozess innerhalb Deutschlands zu beeinflussen.¹⁶ Aktuell gibt es Hinweise, dass auch bei den Wahlen zum britischen Unterhaus Deepfake-Videos zur politischen Desinformation eingesetzt wurden.¹⁷ Es gibt keinen Grund anzunehmen, dass solche Akteure nicht weiterhin versuchen werden, alle ihnen zur Verfügung stehenden technischen Mittel zu nutzen, um ihre Ziele zu erreichen. Deepfakes sind eine potenziell extrem wirksame neue technische Waffe in diesem Zusammenhang. Daher wird es wichtig sein, dass durch öffentliche Aufklärung sowie technische und legislative Maßnahmen der politische Prozess in Deutschland seine Abwehrfähigkeit erhöht. Manipulation wird in jedem System in einem gewissen Umfang möglich sein.

Die Frage ist jedoch, ob die Wirksamkeit solcher Versuche und damit der Schaden am politischen und gesellschaftlichen Diskurs eingedämmt werden kann.

In Bezug auf Deepfakes besteht hier noch ausreichend Zeit, den manipulativen Möglichkeiten dieser technologischen Entwicklung entgegenzutreten. Die gesellschaftliche Debatte hierzu sollte jedoch jetzt beginnen, da es hierbei, wie oben dargestellt, um ein Paket von Maßnahmen gehen wird. Entscheidungen, wie und in welchem Umfang neue Strukturen geschaffen, technische Innovationen umgesetzt oder regulatorische Eingriffe notwendig sind, werden mit Sicherheit mehr Zeit in Anspruch nehmen als die weitere technische Ausreifung der Deepfake-Technologie. CEP und die Konrad-Adenauer-Stiftung werden Mitte 2020 die Ergebnisse ihrer gemeinsamen Studie der Öffentlichkeit vorstellen. Diese wird auch erste konkrete Handlungsempfehlungen an die politischen Entscheider in Berlin enthalten.

*Das Gespräch führte Nael Semaan,
Referentin für Terrorismusbekämpfung
der Konrad-Adenauer-Stiftung.*

- 1 Osteried, Peter 2019: Wie Hollywood die Totenruhe stört, golem.de, 13.11.2019, in: <https://glm.io/144938?t> [10.02.2020].
- 2 Goss, Tricia 2019: How to Do a Face Swap, lifewire, 11.11.2019, in: <https://bit.ly/38ga0x3> [10.02.2020].
- 3 Counter Extremism Project, in: <https://counterextremism.com> [12.02.2020].
- 4 Stupp, Catherine 2019: Fraudsters Used AI to Mimic CEO's Voice in Unusual Cybercrime Case, The Wall Street Journal, 30.08.2019, in: <https://on.wsj.com/31LyThL> [10.02.2020].
- 5 Als „non-consensual pornography“ wird die Verbreitung von privaten Bild- und Filmaufnahmen gegen den Willen des Betroffenen bezeichnet. Siehe: Scott, Alexandra 2017: What is Nonconsensual Pornography?, National Council of Juvenile and Family Court Judges, 12.02.2017, in: <https://bit.ly/2tUh43A> [10.02.2020].
- 6 Satter, Raphael 2019: Experts: Spy used AI-generated face to connect with targets, AP News, 13.06.2019, in: <https://bit.ly/37fnaJm> [10.02.2020]; Swinhoe, Dan 2019: What is spear fishing? Why targeted email attacks are so difficult to stop, CSO, 21.01.2019, in: <https://bit.ly/31UfaMY> [10.02.2020].
- 7 Winkler, Peter 2019: Ein Video zeigt eine betrunkenene Nancy Pelosi – und führt uns vor Augen, was mit Deepfakes heute alles möglich ist, Neue Zürcher Zeitung, 25.05.2019, in: <https://nzz.ch/ld.1484614> [10.02.2020].
- 8 Harwell, Drew 2019: Top AI researchers race to detect ‚deepfake‘ videos: ‚We are outgunned‘, The Washington Post, 12.06.2019, in: <https://wapo.st/2UKvb6A> [10.02.2020].
- 9 Rodriguez, Salvador 2019: Watch video of AOC grilling Zuckerberg on Facebook allowing lies in political ads, CNBC, 24.10.2019, in: <https://cnb.cx/2OLgM64> [10.02.2020].
- 10 United Nations Meetings Coverage and Press Releases 2019: Victims' Testimony Steering United Nations Team Investigating ISIL / Da'esh Atrocity Crimes in Iraq, Special Adviser Tells Security Council, 26.11.2019, in: <https://bit.ly/31UfGdS> [10.02.2020].
- 11 Manke, Kara 2019: Researchers From the I School and Engineering Use Facial Quirks to Unmask ‚Deepfakes‘, Berkeley School of Information, 18.06.2019, in: <https://bit.ly/38gRggS> [11.02.2020].
- 12 Chan, Man-pui Sally / Jones, Christopher R. / Jamieson, Kathleen Hall / Albarracin, Dolores 2017: Debunking, A Meta-Analysis of the Psychological Efficacy of Messages Countering Misinformation, in: Psychological Science 28:11, S.1531–1546.
- 13 Schmitz, Peter 2017: Was ist ein Hash?, Security Insider, 23.08.2017, in: <https://bit.ly/2HhVdGc> [10.02.2020].
- 14 Echikson, William / Knodt, Olivia 2018: Germany's NetzDG: A key test for combatting online hate, Counter Extremism Report 2018/09, Centre for European Policy Studies (CEPS), 11/2018, in: <https://bit.ly/2tUh8Ak> [10.02.2020].
- 15 Hier wäre besonders § 1 Abs. 3 NetzDG in Verbindung mit § 201a StGB anzuführen, siehe: Bundesministerium der Justiz und für Verbraucherschutz 2017: Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (Netzwerkdurchsetzungsgesetz – NetzDG), 01.09.2019, in: <https://bit.ly/2SDlMej> [10.02.2020].
- 16 Pörzgen, Gemma 2017: Informationskrieg in Deutschland? Zur Gefahr russischer Desinformation im Bundestagswahljahr, Bundeszentrale für politische Bildung (bpb), Aus Politik und Zeitgeschichte (APuZ), 19.05.2017, in: <https://bpb.de/248506> [10.02.2020].
- 17 The Soufan Center 2019: IntelBrief: The Use of Disinformation in the British Election, 13.12.2019, in: <https://bit.ly/2UJTckt> [10.02.2020].