Christopher Nehring

Desinformation

Titelbild:
Globus: Icon made by Freepik from www.flaticon.com
Politiker: Icon made by deemakdaksina from www.flaticon.com
Buch: Icon made by kumakamu from www.flaticon.com
Lautsprecher: Icon made by vectorsmarket15 from www.flaticon.com
Ohr: Icon made by th studio from www.flaticon.com
Fernseher: Icon made by Freepik from www.flaticon.com
Demonstration: Icon made by noomtah from www.flaticon.com

Christopher Nehring, Dr. phil., ist Experte für Desinformation, KI und Geheimdienste; Autor zahlreicher Bücher, Aufsätze und Presseartikel. Er ist Gastdozent des Medienprogramms Südosteuropa der Konrad-Adenauer-Stiftung an der Journalistischen Fakultät der Universität Potsdam mit dem Spezialgebiet Desinformation. Für den Tagesspiegel, die Deutsche Welle, Spiegel, NZZ und Welt schreibt er regelmäßig über Desinformation, KI und Geheimdienste.

Landeszentrale für politische Bildung Thüringen
Regierungsstraße 73, 99084 Erfurt
www.lztthueringen.de
2024

ISBN: 978-3-910740-27-3

Inhalt

Definition und Terminologie: Was ist eigentlich Desinformation?

Desinformation ist ein komplexes und vielschichtiges Phänomen. Und ein Phänomen mit vielen Namen, die leider oftmals falsch oder synonym benutzt werden. Da im Kontext von Desinformation viele verschiedene und miteinander verwandte Begriffe auftreten, sollen die wichtigsten hier kurz vorgestellt und erklärt werden:

Desinformation sind falsche, ungenaue, aus dem Kontext gerissene und irreführende Informationen, die verdeckt und absichtlich erstellt, veröffentlicht und verbreitet werden, um politischen, finanziellen oder anderen Einfluss auszuüben. Desinformation will also manipulieren und richtet Schaden an. Im Unterschied zur Propaganda verschleiert Desinformation häufig ihre Ursprünge und Urheber durch ausgeklügelte Schemata. Auch zielt sie weniger auf Überzeugung und mehr darauf Spaltungen, Misstrauen und Konflikt zu erzeugen.

Fehlinformation (»Misinformation«) sind falsche oder irreführende Informationen, die aber im Gegensatz zu Desinformation nicht in manipulativer Absicht verbreitet werden. Sie werden zumeist versehentlich oder aus Unwissenheit weitergegeben und verbreitet.

Propaganda ist die strategische Manipulation eines großen Publikums durch Regierungen oder mächtige Akteure. Propaganda ist oft offener und offizieller als Desinformation und zielt mehr darauf ab, Unterstützung für eine Sache, Überzeugung, Partei, Regierung oder Land zu wecken und andere davon zu überzeugen. Vor dem Missbrauch durch die totalitären Re-

gime de 20. Jahrhunderts war Propaganda ein neutraler, nicht negativ belegter Begriff, der das Werben für und Überzeugen von der eigenen Sache, Meinung etc. beschrieb. Propaganda kann auf verdeckte Formen von Desinformation zugreifen; grundsätzlich versucht Propaganda jedoch mehr zu überzeugen und Sympathien zu wecken, wohingegen Desinformation diskreditieren, schaden und spalten soll.

Falschinformation kann als Synonym für Desinformation oder Fehlinformation verwendet werden, abhängig vom Kontext. Im Allgemeinen bezieht es sich auf jegliche Art von falschen oder irreführenden Informationen, unabhängig von der Absicht hinter ihrer Verbreitung.

Informationsmanipulation ist ein breiterer Begriff, der sich auf jede Art der Verzerrung, Verfälschung oder gezielten Veränderung von Informationen bezieht, um ein bestimmtes Ziel zu erreichen, sei es politisch, finanziell oder sozial.

Fake News bezog sich ursprünglich auf gefälschte Nachrichteninhalte, die wie echte Nachrichten erscheinen und damit absichtlich täuschen sollen. In der neueren politischen und sozialen Rhetorik wird der Begriff jedoch einerseits häufig unspezifisch für alle Arten von Informationsmanipulation verwendet; andererseits wurde der Begriff von vielen, vor allem populistischen, Politikern weltweit instrumentalisiert, um jegliche Kritik abzulehnen oder missliebige Informationen zu diskreditieren. Wegen seiner definitorischen Unschärfe und da in einem traditionellen Verständnis falsche oder manipulierte Nachrichten überhaupt keine (ernsthaften) Nachrichten sein können, ist der Begriff problematisch und sollte vermieden werden.

Warum ist es wichtig, diese Begriffe und die unterschiedlichen Nuancen und Konzepte zu kennen? Im Bereich der Informationsmanipulation sind Definitionen keine akademische Schönspielerei, sondern haben ganz praktische und sehr reale Folgen: Einerseits zeichnet sich schon lange ein Trend in

politischen Debatten und politischer Kommunikation ab, jegliche Kritik und missliebige Informationen als »fake news« oder Desinformation zu diskreditieren. Neuere Studien legen nahe, dass auch seitens des Nachrichtenpublikums eine zunehmende Tendenz besteht, missliebige Informationen, die der eigenen Meinung oder dem Weltbild widersprechen, sämtlich als Desinformation abzutun. Pauschalvorwürfe, in voller Absicht manipulative Informationen zu verbreiten, greifen damit immer weiter um sich. Verschwörungsideologen, Populisten, aber auch ausländische Regierungen machen sich ihrerseits just diesen Vorwurf der Allgegenwärtigkeit von Desinformation zunutze, um ihn gegen »das System« vorzubringen und einzusetzen. Die Allgegenwärtigkeit von Vorwürfen der Desinformation, noch einmal gesteigert seit dem Aufkommen und massenhaften Einsatz »Künstlicher Intelligenz« (KI), sorgt so dafür, dass Debatten immer weiter verzerrt werden, Konsensbildung immer schwieriger wird und die Gräben zwischen Personen und Organisationen immer tiefer werden.

Ein klares Verständnis davon, was Desinformation ist (und was nicht), ist also einerseits wichtig, um politische und öffentliche Debatten auf derselben Faktengrundlage zu führen. Auch wenn es oftmals ins Vergessen gerät: Demokratie, Rechtsstaat, aber auch Bereiche der Verwaltung und Infrastruktur, beruhen auf der Unterscheidung zwischen Wahrheit und Lüge, auf der Anerkennung und Anpassung an (wissenschaftliche) Fakten. Wo Fakten aber zur »Glaubens-, Meinungs- oder Ansichtssache« werden und grundlegende wissenschaftliche Fakten wie die Gestalt der Erde oder die Existenz von Viren in Frage gestellt werden, dort werden diese Systeme über kurz oder lang an ihre Grenzen stoßen und nicht mehr funktionieren können. Professionelle Desinformationsakteure wissen das und wollen diesen Zustand bewusst herbeiführen.

Ein genaues Verständnis und die Definition von Desinformation sind aber auch für die Bekämpfung von Desinformation wichtig. Werden Gesetze und Regeln erlassen, ist es wichtig zu wissen, was eigentlich verboten oder geregelt werden soll.

Dies gilt sowohl für Gesetze, als auch für soziale Medien und Plattformen. Grundsätzlich gilt dabei, dass der Begriff »Desinformation« häufig weder in Gesetzestexten noch in den Nutzungsbedingungen und Regeln von Social-Media-Plattformen definiert wird. Die meisten Plattformen »verbieten« Desinformation als Verstoß gegen die eigenen Nutzungsbedingungen und Richtlinien. Trotzdem reißt die Flut von Desinformation nicht ab (siehe mehr dazu bei Gegenmaßnahmen).

In Gesetzestexten taucht Desinformation ebenfalls selten auf. Das hat damit zu tun, dass Desinformation trotz ihrer schädlichen Wirkung und Absicht zumeist in einer rechtlichen Grauzone agiert, immer an der Grenze zur Illegalität, aber häufig gerade noch so von der Meinungsfreiheit gedeckt. In vielen autoritären Staaten wie der Türkei oder Russland hingegen sind Desinformation oder Fake News ausdrücklich per Gesetz verboten; tatsächlich werden diese Gesetze zur Unterdrückung politischer Opposition und Andersdenkender eingesetzt.

Publikum, Urheber, Medien und Formen von Desinformation

Desinformation hat viele Gesichter, viele Formen und Typen: Eine grundsätzliche Unterscheidung gibt es zum Beispiel beim Ziel hinter Desinformation. Manche Desinformation möchte seine Zielgruppen von einer Meinung, Politik oder einem Produkt *überzeugen*; dies ist jedoch vergleichsweise selten, da andere Kommunikationsformen (z. B. positive Kampagnen) oftmals überzeugender sind als die zumeist negativen Inhalte von Desinformation. Viel häufiger aber will Desinformation ablenken, z. B. durch emotionalisierende Inhalte Debatten umkehren, vom Thema abbringen oder in eine bestimmte Richtung lenken. Auch die konstante Überflutung mit bewusst falscher Desinformation im Online-Raum ist keineswegs zufällig, sondern Absicht. Hier sollen nicht die einzelnen Nachrichten, Videos, Botschaften oder »Narrative« an sich ihr Publikum überzeugen, sondern im Gegenteil durch eine konstante Überflutung mit widersprüchlichen Inhalten gezielt Verwirrung herbeiführen und ein Klima erzeugen, in dem niemandem geglaubt wird und alles möglich erscheint. Durch ihre negativen Inhalte zielt Desinformation auch zumeist darauf, Konflikte, z. B. zwischen Staaten, Volksgruppen, gesellschaftlichen Schichten, Parteien oder anderen Gruppen, zu schaffen, zu vertiefen und anzuheizen. Während legitime politische Akteure ihren Zuspruch und Erfolg an der Lösung von Konflikten messen und hieraus ihre Unterstützung beziehen, versuchen andere durch das Schaffen von Problemen den Zuspruch und die Unterstützung für bestehende Parteien, Regierungen oder Personen zu verringern. Ähnliches gibt es auch im Bereich der Wirtschaft, wenn Unternehmen nicht durch die positiven

Eigenschaften ihrer Produkte um Kunden konkurrieren, sondern ihre Mitbewerber schlechtmachen und in Konflikte verwickeln.

Konkrete Maßnahmen, Kampagnen und Operationen können dabei viele Gestalten annehmen: Sogenannte »Aktive Maßnahmen«, wie sie in der Sprache des sowjetischen Geheimdienstes KGB hießen, sind Maßnahmen zur Einflussnahme und Störung. Sie umfassen die gezielte Verbreitung von Desinformation. Dazu gehören falsche Telefonanrufe, gekaufte Proteste und Demonstrationen, Leaks oder die Einbindung von Stellvertreterorganisationen. Andere Maßnahmen sind das sogenannte »Astroturfing«, bei denen künstlich geschaffene Bürgerbewegungen oder Online-Communitys ins Leben gerufen werden, um legitime öffentliche Unterstützung vorzutäuschen und Meinungen größer und legitimer erscheinen zu lassen, als sie tatsächlich sind.

Online-Kampagnen nutzen Webportale, Online-Medien und soziale Netzwerke, um Desinformation zu verbreiten, während politische Parteien, Clubs, Organisationen sowie Denkfabriken und Forschungsinstitute als Stellvertreterorganisationen benutzt werden, um zu täuschen und Einfluss zu nehmen. Traditionelle Medienkampagnen spielen ebenfalls eine Rolle in Desinformationsstrategien, nehmen in ihrer Bedeutung jedoch ab. Andere Formen können mithilfe von Künstlicher Intelligenz erzeugte Deepfakes oder kostengünstige Fälschungen sein, bei denen audiovisuelle Inhalte mit anderen Technologien manipuliert werden. Weitere Fälschungen, ob digital oder analog, sind ebenso beliebte Mittel. Diffamierungskampagnen richten sich gegen Einzelpersonen wie Politiker, Experten und Journalisten. Mehr ein Mittel als eine Form sind sogenannte digitale Amplifikationsnetzwerke (»Bots« und »Trolle«), die durch koordiniertes Online-Verhalten versuchen, die Sichtbarkeit von Desinformation zu erhöhen. Datenmanipulation ist ebenfalls eine beliebte Spielart von Desinformation und erfolgt durch das Erstellen, Verzerren oder selektive Präsentieren von Daten, um das Publikum irrezuführen. Historischer

Revisionismus und die Instrumentalisierung von Geschichte und historischen Narrativen ist eine oft gebrauchte Form von Desinformation. Dazu gehört, durch die verzerrte Darstellung historischer Ereignisse politische oder gesellschaftliche Erzählungen zu unterstützen und so Politik und Gesellschaft zu beeinflussen. Desinformation beinhaltet auch oft Verschwörungstheorien, die unbegründete und oft reißerische, jedoch nicht faktenbasierte Erklärungen für Ereignisse verbreiten, bei denen eine geheime Verschwörung im Mittelpunkt steht. Meme-Kriegsführung verbreitet online Memes, um die öffentliche Wahrnehmung zu formen. Staatliche Desinformation und ausländische Einflussnahme sind weitere Formen, die von Regierungen genutzt werden, um falsche Informationen zu politischen Zwecken zu verbreiten, sowohl im Inland als auch im Ausland. Wahlbeeinflussung, vor allem im Ausland bzw. durch ausländische Akteure, durch die Verbreitung falscher Informationen, gefälschte Telefonanrufe und Drohungen zielt darauf ab, politische Interessen durch die Verbreitung von Desinformation durchzusetzen.

Grundsätzlich kann man zwischen staatlichen und nichtstaatlichen Urhebern unterscheiden. Staatliche Akteure verbreiten Desinformation zumeist im Regierungsauftrag, entweder, um das eigene Volk und Gesellschaft zu manipulieren, oder um Einfluss auf politische und gesellschaftliche Prozesse in anderen Ländern zu nehmen. Die ausführenden Stellen sind dann besonders oft Geheimdienste, aber auch staatliche Medien, Außenministerien, spezielle Informations- und Propagandabehörden oder auch Hackergruppen, die im Staatsauftrag handeln. Doch auch diese staatlichen Stellen greifen bei der Ausführung ihrer Aufträge zur Verbreitung von Desinformation auf viele Helfer und Stellvertreter zurück. Diese Beziehungen werden oft geheim gehalten und verschleiert, sodass sie selten in Echtzeit zu erkennen sind.

Nicht staatliche Urheber von Desinformation gibt es viele: Zum Beispiel politische Parteien, die im Wahlkampf Desinformation verbreiten; oder Firmen und Wirtschaftsverbände, die

wie die Tabak- oder die Öl-Industrie in der Vergangenheit belegtermaßen gezielt mit Desinformation arbeiteten, um ihr finanzielles Interesse zu wahren und von schädlichen Folgen ihrer Produkte abzulenken. Wie auch bei Parteien oder im Staatsauftrag, geben viele Urheber hinter Desinformationskampagnen die tatsächliche Arbeit und Gestaltung von Desinformation an PR-Firmen ab. Oftmals dienen auch Stiftungen, Think Tanks, Forschungszentren oder andere Organisationen als ausführende Stellen bei der Verbreitung von Desinformation. Dahinter stehen dann wiederum staatliche Stellen oder eben Parteien, Firmen oder Einzelpersonen wie Oligarchen, Tycoons und Magnaten. Viele Beispiele weltweit haben gezeigt, dass PR-Firmen, TV-Sender und Online-Medien, die Desinformation verbreiten, ohnehin zum festen Bestandteil von Firmengeflechten von Oligarchen gehören. Stellvertreter, die für die wahren Urheber Desinformation entweder als »nützliche Idioten« aus Überzeugung oder gegen Geld oder sonstige Leistungen verbreiten, sind ein fester Bestandteil der Welt manipulativer Desinformation.

In dieser Welt spielen Medienschaffende aller Art eine wichtige Rolle. Einerseits können zum Beispiel angesehene Journalisten von Qualitätsmedien gekauft oder als »Einflussagenten« angeworben werden, um immer wieder gezielt Falschinformationen zu verbreiten. Diese relativ aufwendige Methode hat heute keinen hohen Stellenwert mehr. In der Welt der digitalen und sozialen Medien kommt einzelnen, traditionellen Journalisten nicht mehr derselbe Stellenwert zu wie früher. Stattdessen lassen sich Social-Media-Influencer immer öfter als Verbreiter von Desinformation erkennen. Publik wurden zum Beispiel Angebote von PR-Firmen mit Verbindungen nach Russland, die Influencern in Deutschland, Frankreich, Brasilien oder Indien Geld boten, um Falschinformationen über Corona-Impfstoffe zu verbreiten; in Afrika wurden Zahlungen russischer Botschaften an Influencer in verschiedenen Ländern öffentlich, durch die antiamerikanische oder antifranzösische Beiträge gekauft wurden. Darüber hinaus gehört es zum festen Instrumentarium professioneller Desinformation,

dass Webportale unterhalten werden, die wie seriöse Nachrichtenseiten wirken, tatsächlich aber von ein bis zwei Angestellten automatisiert betrieben werden und deren Seiten nur als Ausgangspunkt dienen, um Artikel, Videos, Aufnahmen oder Posts über Social Media zu verbreiten. Um eine möglichst große Reichweite zu erzeugen, gehören auch Netzwerke von sogenannten »Trollen« und »Bots« ins Repertoire. Diese bezeichnen bezahlte Angestellte (Trolle), die zahlreiche Social-Media-Profile auf verschiedenen Plattformen unterhalten, um Beiträge zu verbreiten und ihre Reichweite zu erhöhen; in immer mehr Fällen wird dies auch von Programmen (Bots) und Künstlicher Intelligenz automatisiert ausgeführt.

Desinformation braucht Medien, um ihre Botschaften zu verbreiten. Breit angelegte Desinformationskampagnen suchen Leitmedien, um eine möglichst große Reichweite und Massen von Lesern oder Zuschauern zu erreichen. Spezialisierte Kampagnen, die auf die Verbreitung einer einzelnen Information und die Einflussnahme auf einzelne Prozesse zielen, versuchen hingegen eher, ihre Botschaften in einem bestimmten Medium zu veröffentlichen. Oft geht es also um Masse und selten um Klasse.

Zu den traditionellen Medien (»Klasse«), die für solche Zwecke eingesetzt werden, gehören Print- und Online-Artikel in etablierten Nachrichtenportalen, Fernsehsendungen sowie Radioprogramme, die aufgrund ihrer Reichweite und ihrer Autorität in der Bevölkerung ein hohes Maß an Glaubwürdigkeit genießen. Der »Vorteil« für Urheber und Verbreiter von Desinformation dabei ist, dass ihre Botschaft ein »Gütesiegel« und »Qualitätsbooster« erhält. Der Nachteil für sie ist jedoch, dass erstens die Bedeutung und Reichweite traditioneller Nachrichtenmedien abnimmt und zweitens, es durch redaktionelle Standards und Überprüfungen viel schwerer ist, Desinformation dort unterzubringen. Das bedeutet viel Aufwand für geringe Erfolgsaussichten.

Für Desinformation lukrativer sind deshalb Webportale, also einfache Seiten, die angebliche Nachrichten ohne

Redaktion und traditionelle Standards veröffentlichen. Sie können relativ einfach eröffnet und auch wieder geschlossen werden. Sie eignen sich gut, um Nachrichten umzuschreiben oder als vermeintlich seriöse Quelle für Informationen zu erscheinen, die dann in anderen Online-Kanälen wie den Sozialen Medien vervielfältigt werden. Das heute jedoch zumindest der Anzahl nach wichtigste Medium für die Verbreitung von Desinformation sind die Sozialen Medien, auf denen Influencer und Gruppen mit großer Reichweite gezielt Desinformation streuen können. Die persönlichen und scheinbar authentischen Beiträge von Influencern und die dynamischen Diskussionen in Gruppen, Foren und Chats bieten eine direkte und oftmals unregulierte Route, um Debatten und die öffentliche Wahrnehmung zu beeinflussen. Soziale Medien haben viele Vorteile für die Verbreitung von Desinformation: Sie ermöglichen Anonymität, eine unbegrenzte Reichweite, geringe Kontrolle und bieten leichte Einfallstore, um Debatten zu manipulieren. So werden kontroverse, viel diskutierte und oft geteilte Beiträge von den Algorithmen der Plattformen automatisch anderen Nutzern vorgeschlagen. Setzt man »Bots« und »Trolle« ein, um eigene Beiträge zu vervielfältigen und kontrovers zu diskutieren, macht der Algorithmus dann den Rest.

Ein anderes, recht spezielles digitales Medium sind Datenlecks oder geklaute digitale Informationen (»Leaks«). Ein beliebtes Vorgehen ist es dabei, sensible Informationen durch einen Hackerangriff zu erbeuten, und anschließend in manipulierter Form auf einer Plattform, in einem Forum oder Chat, eigens kreierten Webseiten oder eben über Soziale Medien zu veröffentlichen.

Obgleich digitale Medien heute die wichtigsten und reichweitenstärksten Medien sind, benutzt Desinformation auch immer noch traditionelle »Offline«-Medien und Methoden. »Mundpropaganda« und Gerüchte, zum Beispiel im Kontext von Kriegen, waren und sind ein recht altes aber wirkungsvolles Mittel. Auch haben Bücher und andere Print-Publikationen zwar nicht mehr den Stellenwert vergangener Zeiten,

nichtsdestoweniger gibt es auch heute noch Autoren, Publizisten, Journalisten und Wissenschaftler, die für Auftragsarbeiten in Propaganda und Desinformation bezahlt wurden.

Das letzte wichtige Trägermedium von Desinformation ist der Mensch. Menschen agieren in der Welt der Desinformation als (zumeist bezahlte) Fürsprecher, Stellvertreter oder »Einflussagenten«. Das können zum Beispiel Journalisten im Staats- oder Oligarchenauftrag sein, Politiker oder auch Wissenschaftler und Experten. Sie nutzen ihre scheinbare Autorität und Expertise, um falsche Narrative und Informationen zu verbreiten und die öffentliche Meinung zu manipulieren.

Den Akteuren und Medien von Desinformation stehen auf der Empfängerseite eine Bandbreite von Zielgruppen und Publikum gegenüber. Darunter finden sich gleichfalls viele Zielgruppen, die sich auch auf der »Täter«- oder Urheberseite von Desinformation befinden. Medien, Journalisten, Publizisten oder Social-Media-Influencer und -Journalisten sind besonders beliebte Zielgruppen von Desinformation. Hier geht es nicht so sehr darum, Einzelpersonen von bestimmten Positionen, Sachverhalten oder Informationen zu überzeugen, sondern sie dazu zu bringen, die Botschaften von Desinformation weiter zu verbreiten, zu multiplizieren und die Reichweite zu vergrößern. Politiker und gesellschaftlich einflussreiche Personen hingegen sind Ziele von Desinformation, um Entscheidungen zu beeinflussen und Stimmungen, Debatten und die gesellschaftliche Wahrnehmung zu formen. Ähnliches gilt für Behörden, staatliche und öffentliche Einrichtungen, die durch Desinformation in ihrer Arbeit beeinträchtigt, verwirrt, gelähmt oder beeinflusst werden sollen. Die breite Öffentlichkeit und Gesellschaft, die Bürger und Wähler sollen gleichfalls in ihren (Wahl-)Entscheidungen, Meinungen und Stimmungen beeinflusst, verwirrt, abgelenkt und zu bestimmten Handlungen manipuliert werden.

Desinformation zielt dabei nicht nur auf den politischen und gesellschaftlichen Bereich, sondern auch die Wirtschaft. Unternehmen und Betriebe können zur Zielscheibe von

Desinformation werden, um ihre Geschäfte zu stören, ihren Ruf zu schädigen, Produktion und Aufträge zu sabotieren oder um konkurrierenden Unternehmen gezielt Vorteile zu verschaffen. Umgekehrt gilt dies jedoch auch für Kunden, die in ihren Entscheidungen und in ihrem wirtschaftlichen Verhalten gezielt durch Falschinformationen beeinflusst oder verwirrt werden sollen.

Eine letzte »Zielgruppe« der digitalen Desinformation sind schließlich auch Algorithmen. Da in der Welt der Sozialen Medien, Messengerdienste etc. Algorithmen die wichtige Funktion übernehmen, den menschlichen Endnutzern Information gezielt und kuratiert vorzuschlagen, sind auch sie Ziel von Desinformation. Diese wird von ihren Urhebern so maßgeschneidert, dass die Algorithmen der Suchmaschinen und Nachrichten-»Feeds« sie besser platzieren und öfter anzeigen. Dies spielt für die Reichweite und Verbreitung von Desinformation eine wichtige Rolle.

Wer betreibt Desinformation?

Russland

In vielerlei Hinsicht gilt Russland als das Mutterland der Desinformation. Zwar ist die These, der russische Staat habe das Konzept und den Begriff von Desinformation erfunden und als erster umgesetzt, weder belegbar noch stichhaltig. Doch diese Frage ist auch eher nebensächlich, solange Desinformation in all ihren Facetten ein grundlegendes Instrument russischer Politik im In- und Ausland ist. Dies ist eines der wichtigsten Merkmale, das Russland von anderen Staaten unterscheidet und ein Grund dafür, warum der russische Staat beim Thema »Desinformation« so oft im Rampenlicht steht: Desinformation war und ist für den russischen Staat nachweisbar seit der späten Zarenzeit ein festes Instrument zur Erreichung und Umsetzung politischer Ziele. Wo andere Staaten punktuell, zum Beispiel in militärischen Konflikten, Desinformation zur Flankierung ihrer Politik einsetzen, hat der russische Staat einen festen Apparat und Systeme geschaffen, die gezielte Desinformation zu einem »normalen Politikinstrument« gemacht haben. Als eine der Weltmächte setzt Russland dieses Instrument seit Jahrzehnten global ein. Als normales Politikinstrument genießt Desinformation deshalb einen recht großen Stellenwert in der russischen Politik. Sie ist eingebunden in ein ganzheitliches System zur weltweiten Einflussnahme, aber auch der Manipulation und Indoktrinierung der russischen Bevölkerung. Desinformation ist dabei immer ein Mittel unter vielen zur Einflussnahme und Umsetzung russischer Politik. Anders als in anderen Staaten wird Desinformation von russischen Polit-Strategien also immer mitgedacht, wenn es darum geht,

Politik zu machen. Der hohe Stellenwert zeigt sich einerseits an den zahlreichen Stellen und Einheiten, die damit befasst sind, aber auch an den gigantischen Summen, die dafür ausgegeben werden. Wie aus geleakten Dokumenten bekannt wurde, veranschlagte die russische Präsidialadministration rund 500 Millionen Euro für »Informationsmaßnahmen« im Zuge der Präsidentschaftswahl 2024. Der Propagandasender »RT« eines der wichtigsten Instrumente der globalen Verbreitung russischer Desinformation, hat für 2024 ein kolportiertes Jahresbudget von fast 1 Milliarde US-$.

Doch es gibt auch andere Gründe, warum wir über russische Desinformation mehr wissen und auch mehr hören als z. B. über chinesische: Zunächst einmal die geografische Nähe Deutschlands und Europas zu Russland. Länder im direkten Umkreis sowie Länder mit großer außenpolitischer Bedeutung für Russland, wurden und werden öfter zum Ziel russischer Desinformation als andere. Andererseits – auch dies ist für die öffentliche Wahrnehmung russischer Desinformation von großer Bedeutung – ist über russische Desinformation viel mehr bekannt als über solche Maßnahmen anderer Staaten. Das gesicherte Wissen darüber ist recht groß. Dies ist auf die Brüche in der russischen Geschichte zurückzuführen: Vom Zarenregime über die Sowjetunion unter Stalin und einer kurzen (mehr oder weniger) demokratischen Phase hin zum System Putin. Diese Brüche bedeuteten immer, dass Wissen aus Unterlagen, Archiven, Behörden oder von ehemaligen Mitarbeitern und Überläufern öffentlich wurde. So wurden auch jedes Mal große Kontinuitäten sichtbar, die zeigen, dass sich der strategische Einsatz von Desinformation in den verschiedenen Systemen meist nur im Ausmaß der Aggressivität und den zur Verfügung stehenden Ressourcen unterschieden hat.

Das System russischer Desinformation

Russische Desinformation ist nicht nur ein sehr komplexes Phänomen, sondern auch ein überaus komplexes System von unterschiedlichen Akteuren, Taktiken, Strategien, Medien und

Inhalten. Dieses System ist von außen oft nicht leicht zu durchschauen, da viele Querverbindungen und Wechselwirkungen bestehen. Andererseits werden Verbindungen, Urheberschaft und Ziel bei koordinierter politischer Desinformation ja zumeist gezielt verschleiert.

Ein Grundschema russischer Desinformation, das schon zu Sowjetzeiten in ähnlicher Weise bestand, ist, dass es drei grobe Säulen gibt. Dies wurde früher mit »schwarzer«, »grauer« und »weißer Propaganda- bzw. Einflussarbeit« beschrieben. »Weiß« meinte dabei, dass staatliche Institutionen ganz offen Propaganda betreiben, bei der sie als Absender und Urheber offen in Erscheinung treten. Dies gilt heute zum Beispiel für die gezielte Verbreitung von Falschmeldungen durch Social-Media-Profile russischer Botschaften im Ausland, oder aber durch offizielle Stellungnahmen des Außenministeriums oder der Präsidialverwaltung. Präsidialadministration (wo ohnehin alle Fäden zusammenlaufen), Außenministerium, Innenministerium, Geheimdienste, Nationaler Sicherheitsrat und Behörden für die Internet- und Telekommunikationsaufsicht sind im heutigen System russischer Desinformation die wichtigsten Akteure. Aber auch Staatsmedien wie der »Erste Kanal« oder »RT« spielen eine hervorgehobene Rolle, vor allem, wenn es um die Durch- und Ausführung von Desinformation geht.

»Schwarze Propaganda« beschrieb hingegen verdeckte Einfluss-, Desinformations- und Propagandaaktionen. Diese werden auch heute noch hauptsächlich von den Geheimdiensten (früher KGB, heute FSB, SWR und GRU) geplant, organisiert und selbst, öfter jedoch durch Tarnorganisationen wie Medien, die speziell zu diesem Zweck im Ausland gegründet wurden, geheimdienstlich kontrollierten Organisationen oder Tarnfirmen wie PR- oder Cybersecurity-Unternehmen ausgeführt. So gibt es eine Vielzahl bekannter Fake-News-Webseiten, wie zum Beispiel »Newsfront«, »Southfront« oder »InfoRos«, die direkt von Geheimdiensten betrieben werden sollen.

»Graue Propaganda und Desinformation« meinte in diesem Kontext eine Mischform, also halbverdeckte Organisationen,

die vordergründig keine staatlichen Akteure sind, auf den zweiten Blick jedoch Verbindungen durch staatliche Kontrollorgane, direkte Finanzierung oder staatliches Führungspersonal aufweisen. Das trifft auf viele der bekannten russischen Desinformationsfabriken wie die »Internet Research Agency«, Teile der ehemaligen »Gruppe Wagner« oder auch verschiedene Medien und Webseiten zu, die offiziell als Privatfirmen registriert sind, aber über verdeckte Firmenkonstruktionen als Tochterkanäle von Staatsmedien, Geheimdiensten oder Funktionären erkennbar sind. Die Cybersecurityfirma »Vulkan«, die Programme für Cyberangriffe und Informationskontrolle produzierte, fiel so durch Verbindungen zum Geheimdienst FSB auf. Andere Cybersecurity- oder PR-Firmen wie »Structura National Technologies« und »Social Design Agency«, wurden von Meta und der EU sanktioniert, da sie hinter dem Netz aus gefälschten Nachrichtenseiten und gefakten Social-Media-Accounts stehen sollen, das seit 2022 Desinformation über die Ukraine verbreitet. Andere Beispiele sind die Medienunternehmen, die von russischen Oligarchen wie Viktor Malofeew oder dem getöteten Jewgeni Prigozhin betrieben werden. Dazu gehören Prigozhins »Patriot Media Group« oder die Webseiten »Geopolitik.ru« oder »Katheon«, die Malofeew zugeordnet werden. Das System dahinter ist recht einfach: Diese Firmen und Medien treten vordergründig als private Medienunternehmen ihrer Besitzer auf. Der russische Staat tritt nicht in Erscheinung. Im Gegenzug erhalten die Oligarchen massiv Staatsaufträge, die diese Aktivitäten finanzieren. Geheimdienstoffiziere beraten die Medienfirmen. Neben solchen verdeckten Medien- und PR-Firmen gibt es auch eine unübersichtliche Reihe von »gemeinnützigen Organisationen«, Think Tanks, Stiftungen und anderen Organisationen, die sich vordergründig mit Forschung, Veranstaltungen oder internationaler Kooperation beschäftigen, jedoch Vehikel des russischen Staates sind.

Diese drei Säulen bilden die Basis für das Ökosystem russischer Desinformation. Die unterschiedlichen Formen zwischen

offen und getarnt stehen dabei nie für sich allein, sondern werden gleichzeitig, nebeneinander und mit Wechselwirkung durchgeführt. So ist es zum Beispiel eine regelmäßige Erscheinung, dass offizielle staatliche Stellen bestimmte (Falsch-)Meldungen veröffentlichen, die dann von dem Geflecht an staatlichen und verdeckt kontrollierten Medien aufgegriffen werden, bevor sie Bot- und Troll-Armeen aus geheimdienstlich kontrollierten Tarnfirmen massiv online verbreiten. Dieses schwer zu durchdringende Geflecht von Wechselwirkungen zwischen den einzelnen Akteuren wird zumeist nicht anhand einer Einzelmeldung oder Information, sondern nur durch ausführliche Untersuchungen in der Gesamtschau sichtbar.

Das russische Mediensystem spielt eine wichtige Rolle bei der Verbreitung von Desinformation und ist geprägt durch eine komplexe Verflechtung staatlicher Kontrolle, Infiltration, Selbstzensur und Einflussnahme durch Oligarchen. Die Verfassung Russlands garantiert zwar die Meinungsfreiheit, doch in der Praxis sind die Medien mit staatlicher Zensur und Selbstzensur konfrontiert. Dieses System besteht aus verschiedenen Arten von Medien: *Staatsmedien*, wie z. B. der »Erste Kanal« im Inland, oder der Auslandssender »RT«. Letzterer ist Teil des aus der ehemaligen Nachrichtenagentur »RIA Novosti« hervorgegangenen staatlichen Medienunternehmens »Russland Heute« (Rossija Sewodnja), zum dem auch die TV-Agentur »Ruptly«, der Radiosender »Sputnik/SNA News« und weitere gehören. Diese Tochterunternehmen gründeten in der Vergangenheit wiederum weitere Tochterunternehmen wie »Maffick Media« oder »Redfish«, die spezielle Inhalte für Social-Media-Kanäle produzierten und dabei versuchten, ihre Verbindung zum russischen Staat zu verschleiern.

Große (und nach dem Überfall auf die Ukraine nicht verbotene) russische Privatmedien haben hingegen oft mehr oder weniger verdeckte Verbindungen zu staatlichen Organen, Geheimdiensten, befinden sich im Besitz kremltreuer Oligarchen oder werden durch Gesetzgebung und Zensurbehörden eingeschränkt und für staatliche Ziele instrumentalisiert. Große

Medienhäuser, wie zum Beispiel Gazprom-Media, besitzen bedeutende Anteile an Fernseh- und Radiostationen sowie an Printmedien. Diese Verbindungen beeinflussen die Berichterstattung, wobei eine pro-Putin und nationalistische Leitlinie gilt. Die Vergabe von Werbeaufträgen durch staatliche Stellen ist ein weiteres Mittel zur Einflussnahme auf den Inhalt der Medienberichterstattung. Privatmedien befinden sich also zumeist entweder im verschleierten Staatsbesitz oder gehören zu den Firmenimperien von Oligarchen wie Jewgeni Prigozhin oder Viktor Malofeew. Diese unterhalten und betreiben PR-Agenturen zur Verbreitung von Desinformation auf Social-Media-Kanälen oder zahlreiche Fake-News-Webseiten für das Ausland oder sogar TV-Sender. Diese gehören vordergründig zu den Firmengeflechten der Oligarchen und werden durch diese finanziert; im Gegenzug jedoch erhalten sie massenhaft lukrative Staatsaufträge für ihre anderen Firmen, wodurch sie ihr Imperium finanzieren.

Die staatliche Kontrolle und Instrumentalisierung für Desinformation erstreckt sich auch auf das Internet, Soziale Medien und Messengerdienste. Die russische Gesetzgebung erlaubt es, Websites ohne gerichtliche Anordnung zu blockieren. Zudem müssen Blogger und soziale Netzwerke, die eine hohe Besucherzahl aufweisen, sich registrieren lassen. Zu diesen Netzwerken, die im gesamten ehemaligen sowjetischen Orbit wichtige Informationsquellen sind, zählen zum Beispiel »Vkontakte«, »Odnoklasniki« oder der Messengerdienst Telegram. Telegram-»Kanäle«, also öffentliche Chat-Gruppen, entwickelten sich in den vergangenen Jahren zu den wichtigsten Desinformations-Kanälen überhaupt (siehe auch Kap. Neue Rechte). In Bezug auf Russland traten hier in der jüngsten Vergangenheit vor allem sogenannte Militärblogger in Erscheinung. Diese Social-Media-Journalisten verbreiten massenhaft Nachrichten und Aufnahmen zum russischen Krieg gegen die Ukraine. Dabei veröffentlichen einige von ihnen immer wieder (Falsch-)Informationen, die sie direkt aus den Ministerien, Geheimdiensten oder der Präsidialverwaltung bekommen.

Gleichzeitig sind diese Kanäle eine besonders häufige Quelle für gezielte Falschinformationen, manipulierte Bild- und Videoaufzeichnungen und übertragen sanktionierte und im Ausland verbotene russische Staatsmedien.

»Operation Doppelgänger«

Die Desinformationsoperation »Doppelgänger« ist eine umfangreiche und raffinierte Online-Desinformationskampagne, die von russischen Akteuren gesteuert wird. Sie wurde erstmals im Sommer 2022 von verschiedenen Organisationen entdeckt. Sie besteht in der gezielten Verbreitung von Falschinformationen, gefälschten Kampagnen und manipulierten Narrativen rund um den russischen Krieg gegen die Ukraine. Ihre Zielgruppen sind Social-Media-Nutzer in der Ukraine, den USA, Deutschland, Frankreich und vielen mehr. Die Kampagne nutzt gefälschte Nachrichtenseiten bekannter westlicher Qualitätsmedien (in Deutschland z. B. »Spiegel«, »Welt« oder »Süddeutsche«), deren Layout, Design und Stil kopiert wird, um völlig falsche Artikel zu produzieren. Diese sind inhaltlich immer mit dem Krieg gegen die Ukraine bzw. der westlichen Unterstützung für die Ukraine verbunden. Diese gefälschten Artikel werden dann über gefälschte Social-Media-Accounts (Bots und Trolle) massiv verbreitet. Dabei kommen elaborierte Verschleierungstaktiken zum Einsatz, z. B. die Manipulation von Social-Media-Vorschaubildern und mehrstufige Website-Umleitungen. Es gab auch Hinweise auf den Einsatz von generativer KI zur Erstellung von Beiträgen. Die Hauptziele der Kampagne sind eine Einwirkung auf die öffentliche Meinung, die Verstärkung politischer Polarisierung und Erosion des öffentlichen Vertrauens.

Zu Beginn des Jahres 2024 entdeckten Behörden und Nichtregierungsorganisationen weitere Aktivitäten, die derselben Operation zugeordnet werden. Im Januar 2024 machte zum Beispiel das deutsche Auswärtige Amt öffentlich, innerhalb nur eines Monats ein Netzwerk von über 50.000 gefälschten Social-Media-Profilen auf dem Kurznachrichtendienst »X« (früher Twitter) entdeckt zu haben. Diese verbreiteten gefälschten Nachrichten im Stil von »Doppelgänger«. Diese zielten darauf, die gesellschaftlichen Spannungen in Deutschland und die Unzufriedenheit der Bevölkerung mit der Regierung zu verstärken und

dahingehend zu lenken, dass der wahre Ursprung in der deutschen Unterstützung für die Ukraine zu suchen sei.

Der Facebook-Mutterkonzern »Meta« nannte die Operation bereits 2023 die wohl »größte und hartnäckigste Einflussoperation«, die sie je in ihrem Netzwerk aufgedeckt haben. Sowohl Meta als auch die USA und die Europäische Union sanktionierten zwei russische IT-Unternehmen, die Meta als Ursprung zahlreicher »Doppelgänger«-Accounts identifizieren konnte.

Der Angriff auf die US-Präsidentschaftswahlen 2016

Die US-Präsidentschaftswahlen zwischen Hillary Clinton und Donald Trump 2016 sind eines der bekanntesten Beispiele für eine elaborierte Desinformationskampagne zur gezielten Beeinflussung einer Wahl. Computer-Hacker, die mit dem russischen Militärgeheimdienst GRU in Verbindung standen, infiltrierten die Computersysteme der Demokratischen Partei der USA. Dort beschafften sie sich eine große Menge an sensiblen internen Daten der Partei – insgesamt über 150.000 persönliche E-Mails und Dokumente. Der Angriff blieb jedoch zunächst unbemerkt. Die gestohlenen Daten wurden zunächst intern analysiert, an manchen Stellen mit manipulierten Informationen ergänzt und anschließend veröffentlicht. Dabei ging der russische Geheimdienst strategisch vor, kreierte zunächst selbst zwei Webseiten (»Guccifer 2.0« und »DCLeaks«), auf denen die Dokumente veröffentlicht wurden. Dort erhielten sie jedoch nur eine geringe Aufmerksamkeit. Einige Zeit später wurden die Dokumente dann an die auf die Veröffentlichung geheimer Daten spezialisierte Web-Plattform »WikiLeaks« weitergegeben, die sie dann schubweise veröffentlichte. Das führte unter anderem auch zu einem parteiinternen und öffentlichen Skandal und zum Rücktritt führender Parteimitglieder in Washington. Die gestohlenen Daten legten interne Meinungsverschiedenheiten und strategische Pläne der Demokratischen Partei offen, was zu einem Vertrauensverlust unter den Wählern führte und den Wahlkampf massiv störte. Das zeigt auch, dass Cybersicherheit und politische Integrität zunehmend miteinander

verknüpft sind. Staatlich unterstützte Cyberoperationen stellen ein neues Feld in geopolitischen Auseinandersetzungen und politischer Einflussnahme dar. Diese Operation ist demnach ein Beispiel dafür, wie digitale Einflussnahme genutzt werden kann, um demokratische Institutionen zu unterminieren und politische Ergebnisse zu manipulieren. Bis heute werden mindestens 12 GRU-Offiziere von den US-Behörden in Verbindung mit dieser Operation gesucht. Einige davon auch in anderen Ländern, zum Beispiel in Deutschland, wo dieselbe Gruppe für großangelegte Hackerangriffe, z. B. auf den Bundestag, verantwortlich gemacht wird.

China

Lange Zeit galt China als die große Unbekannte in der Welt staatlich organisierter Desinformation. Dies hat sich in den vergangenen Jahren verändert. Traditionell verfolgte Peking einen klassischen Propagandaansatz kommunistischer Regime, d. h. es war vor allem um eine positive Außendarstellung sowie ein absolutes Informationsmonopol im Inland bemüht. Die Basis dafür war die kommunistische Ideologie chinesischer Prägung. Dazu gehörte, dass Kritik, Fehler, Skandale oder unerwünschte Entwicklungen ausgeklammert, umgekehrt oder medial und propagandistisch überdeckt wurden. Im chinesischen Internet gehörte dazu auch eine besonders restriktive Zensur, Blockierung politisch unerwünschter Inhalte und Überwachung der für die chinesische Kommunistische Partei und ihr Regime besonders sensiblen Themen; Minderheiten, Dissidenten und politische Proteste, Taiwan, Tibet oder Hongkong erhielten dabei seit jeher viel Aufmerksamkeit. Bis vor einigen Jahren war es jedoch eher die Leitlinie Pekings, positive Nachrichten über China zu verbreiten und Probleme totzuschweigen oder zu verneinen als Gegner offen anzugreifen und mit gezielten Falschinformationen zu arbeiten. Dies hat sich geändert. China ist sichtbar zu einer deutlich aggressiveren Informations- und Desinformationspolitik

im Ausland und dem globalen Informationsraum übergegangen.

Für Informationsoperationen, Cyberkriegsführung, Propaganda und Desinformationskampagnen sind in China zahlreiche Einheiten des Militärs, der Geheimdienste und Abteilungen innerhalb der Kommunistischen Partei Chinas (KPCh), aber vor allem auch Botschaften zuständig. Diese Einheiten spielen eine zentrale Rolle in der Umsetzung der strategischen Ziele des Landes im Bereich der Informationskriegsführung und der globalen Einflussnahme:

Militär (»Volksbefreiungsarmee« – VBA)
- Einheit für Strategische Unterstützung (Strategic Support Force, SSF): Eine Einheit innerhalb der VBA, die für Cyberoperationen, Weltraumoperationen und elektronische Kriegsführung zuständig ist. Die SSF spielt eine Schlüsselrolle in Chinas Bestrebungen, in den Bereichen Cyberkriegsführung und Informationsdominanz führend zu sein.
- Einheit 61398 (auch bekannt als »APT1«): Eine berüchtigte Cyberkriegseinheit, die mit einer Vielzahl von Cyberangriffen und Spionageaktivitäten gegen ausländische Regierungen und Unternehmen in Verbindung gebracht wird.

Geheimdienste
- Ministerium für Staatssicherheit (MSS): Chinas wichtigster Geheimdienst, der für alle Arten von Spionage, Einflussoperationen und Desinformation verantwortlich ist. Das MSS führt umfangreiche Überwachungs- und Informationsgewinnungsoperationen durch, um Chinas nationale Sicherheit zu schützen und seine geopolitischen Interessen zu fördern.
- VBA-Aufklärungsabteilung: Diese Abteilung ist für die elektronische Kriegsführung und Signalaufklärung (SIGINT) zuständig, einschließlich der Überwachung und des Abfangens internationaler Kommunikation.

Kommunistische Partei Chinas

- Zentrale Propagandaabteilung: Verantwortlich für die Steuerung der öffentlichen Meinung und die Verbreitung der Parteilinie sowohl innerhalb Chinas als auch international. Sie spielt eine zentrale Rolle in der Medienkontrolle und der Durchführung von Propagandakampagnen. Dieser Abteilung unterstellt sind auch die »Konfuzius-Institute«, die China weltweit unterhält und zu deren Aufgaben neben Vermittlung chinesischer Kultur und Sprache auch Propagandaaktivitäten gehören.
- Vereinigte Arbeitsfront: Eine spezialisierte Abteilung, für den Einfluss auf Nicht-KP-Mitglieder, Minderheiten und die chinesische Diaspora im Ausland.
- Abteilung für Internationale Verbindungen: Diese Abteilung arbeitet daran, Beziehungen zu ausländischen politischen Parteien, Organisationen und Eliten aufzubauen, um Chinas geopolitische Interessen zu fördern und positive Beziehungen zu Schlüsselakteuren weltweit zu etablieren.

Außenministerium

- Botschaften: Chinesische Botschaften im Ausland traten in den letzten Jahren oftmals mit aggressiven Äußerungen auf, wenn es um sensible Themen (z. B. Minderheiten, Dissidenten, Taiwan) ging. Darüber hinaus sind die Botschaften Ausgangspunkt und Anlaufstellen für vielfältige Informations- und Propagandaaktivitäten. Die Botschaften unterhalten gleichzeitig sehr aktive Social-Media-Kanäle, deren Nachrichten oft durch Netzwerke von »Bots« und »Trollen« verstärkt werden.

Diese Einheiten und Abteilungen arbeiten oft verdeckt und ihre Operationen sind in hohem Maße geheim. Ihre Aktivitäten sind Bestandteil von Chinas umfassender Strategie zur Informationskriegsführung, die darauf abzielt, Chinas Präsenz im globalen Informationsraum zu beeinflussen und zu kontrollieren, um die nationalen Interessen und die geopolitische

Stellung Chinas zu stärken. Seine Strategie für den Informationskrieg fasste Peking zum Beispiel 2008 im Weißbuch zur Verteidigung Chinas zusammen. Dabei geht es vor allem um »Informationsdominanz«, die auch psychologische Operationen, elektronische Kriegsführung und militärische Täuschung beinhaltet. Neben offensiven Fähigkeiten setzt China defensive Maßnahmen ein, wie das Programm »Goldener Schild« (auch als »Große Firewall von China« bezeichnet), das Zensur- und Überwachungsmechanismen umfasst, um die Informationskontrolle der Kommunistischen Partei im chinesischen Internet zu sichern.

Desinformation und die Beeinflussung der öffentlichen Meinung sind also Teil eines umfassenden Ansatzes von Sicherheits-, Außen- und Geopolitik. Die Stoßrichtung hat sich dabei in den letzten Jahren schnell und heftig verändert. Wo früher vor allem Eigenwerbung und positive Darstellung das Ziel war, gehören nun teils aggressive Einfluss- und Desinformationskampagnen im Ausland zu regelmäßigen Erscheinungen. In den breiteren Kontext chinesischer Einflusskampagnen gehören dabei neben Desinformation auch andere Aktivitäten. Die »Konfuzius-Institute«, die China weltweit unterhält, traten in den vergangenen Jahren immer öfter mit propagandistischen Veranstaltungen und Publikationen in Erscheinung. Ein anderes Instrument sind massive Investitionen in ausländische Informations- und Medienbranchen. So zum Beispiel kaufte der chinesische Staat über Mittelsmänner und Tarnfirmen im vergangenen Jahrzehnt massiv ausländische Medienunternehmen wie TV-Sender, Online-Nachrichten, Radiostationen etc. in Südosteuropa, auch Afrika und südostasiatische Staaten standen dabei im Fokus. Ebenso schlossen die chinesischen Staatsmedien »Kooperationsverträge« mit Medien in wirtschaftlich schwachen Ländern ab. In der Folge wurden zum Beispiel Meldungen und Nachrichten der chinesischen KP oder der Staatsmedien in viele Länder wörtlich exportiert und die China-Berichterstattung gezielt beeinflusst. Dies spiegelt auch andere strategische Wirtschafts- und Investitionsaktivitäten

der Volksrepublik wider, bei denen zum Beispiel durch Investitionen in Infrastrukturprojekte wie Flughäfen, Eisenbahnlinien, Straßen, Tunneln und Brücken gezielt Abhängigkeiten und Druckmittel geschaffen wurden.

Chinesische Desinformation und Einflussoperationen wurden in den vergangenen fünf Jahren deutlich präsenter und aggressiver. In ihren Taktiken, Methoden und auch Inhalten trat dabei gerade seit 2020 eine erstaunliche Ähnlichkeit zu russischer Desinformation auf. Dabei treffen verschiedene Entwicklungen aufeinander: Erstens verschärfte sich der geopolitische Konflikt zwischen den USA und China in den vergangen fünf Jahren. Zweitens bedeutete die Covid-Pandemie sowohl ein PR- und Imagedesaster als auch ein politisches Problem für den kommunistischen Einparteienstaat in China. Und drittens erfolgte der russische Angriff auf die Ukraine 2022 mit dem anschließenden Schulterschluss Chinas mit Russland. Gerade letzteres brachte ein erhebliches Ausmaß an Angleichung zwischen russischer und chinesischer Desinformation. In vielen Ländern (vor allem außerhalb Europas) war so zu beobachten, dass offizielle chinesische Kanäle (Staatsmedien, Botschaften und andere Behörden sowie ihre Social-Media-Kanäle, aber auch aus China gesteuerte Online-Gruppen) teils wörtlich die Botschaften des Kremls übernahmen und verbreiteten.

In der zunehmenden geopolitischen Rivalität mit den USA setzte China verstärkt auf klassische Desinformation, um seine geopolitischen Ziele zu unterstützen und die öffentliche Meinung zu beeinflussen. Einige Beispiele dafür sind:

– Verschwörungstheorien: Zu Beginn der COVID-19-Pandemie 2020 verbreiteten chinesische Staatsmedien und offizielle Social-Media-Accounts die Theorie, dass das Virus von der US-Armee nach China gebracht worden sei. Diese Behauptungen wurden ohne stichhaltige Beweise aufgestellt und zielten darauf ab, von Chinas eigenem Umgang mit dem Virusausbruch abzulenken und die globale Kritik an der anfänglichen Reaktion Chinas auf die Pandemie umzulenken. 2023 verbreiteten chinesische Accounts während

der großen Waldbrände auf Hawaii mit Künstlicher Intelligenz erstellte Bilder, die Verschwörungstheorien untermauern sollten, wonach die Feuer durch geheime Waffen des US-Pentagon entfacht worden seien.
- US-Wahlen 2020: Im Vorfeld der US-Präsidentschaftswahlen 2020 setzte China Desinformationskampagnen ein, um Misstrauen gegenüber dem Wahlprozess zu schüren und die politische Polarisierung in den USA zu verstärken. Durch den Einsatz von Social-Media-Bots und gefälschten Accounts wurden Falschinformationen und polarisierende Inhalte verbreitet, die darauf abzielten, die Glaubwürdigkeit des Wahlprozesses in Frage zu stellen und dadurch gesellschaftliche Spaltungen zu vertiefen.
- Der Handelsstreit zwischen den USA und China: Während des eskalierenden Handelsstreits zwischen den USA und China nutzte die chinesische Regierung Desinformationskampagnen, um die US-Handelspolitik zu kritisieren und die eigene Wirtschaftspolitik in einem positiven Licht darzustellen. Durch staatlich kontrollierte Medien und koordinierte Social-Media-Operationen wurden Nachrichten verbreitet, die die Stärke der chinesischen Wirtschaft betonten und gleichzeitig die Handelsmaßnahmen der USA als ungerecht und schädlich für die globale Wirtschaft darstellten. Diese Kampagnen zielten darauf ab, internationale Unterstützung für Chinas Position im Handelsstreit zu gewinnen und den Druck auf die US-Regierung zu erhöhen.

Im Zuge des russischen Angriffskrieges gegen die Ukraine, bei dem sich China an der Seite Russlands und gegen den Westen positionierte, passte Peking auch seine Medien- und Informationsstrategien an. Seit Februar 2022 verbreiten chinesische offizielle und inoffizielle Stellen russische Desinformationsnarrative über den Krieg, die Chinas komplexes Verhältnis zu Russland und seine strategischen Interessen in Bezug auf die geopolitische Ordnung widerspiegeln. Einige Beispiele dafür sind:

– Verbreitung russischer Narrative über den Kriegsgrund: Chinesische staatlich kontrollierte Medien und Social-Media-Accounts, z. B. von chinesischen Botschaften in Afrika und andernorts, haben aktiv russische Darstellungen des Konflikts übernommen und verbreitet. Diese Nachrichten stellten den Krieg als eine Reaktion auf provokative Handlungen des Westens und der ukrainischen Regierung dar. Durch die Veröffentlichung von Artikeln, Kommentaren und Videos, die die russischen Positionen unterstützen, tragen sie dazu bei, die Glaubwürdigkeit und Reichweite russischer Desinformation zu erhöhen. Ein Beispiel hierfür ist die unkritische Übernahme und Verbreitung der russischen Behauptung, die militärischen Aktionen in der Ukraine seien notwendig, um eine »Entnazifizierung« durchzuführen.
– Bio-Waffen: Offizielle und inoffizielle Stimmen Chinas haben russische Behauptungen aufgegriffen und verbreitet, wonach die USA in der Ukraine geheime biologische Waffenlabore betreiben würden. Diese unbewiesenen Behauptungen wurden von chinesischen Staatsmedien und über offizielle Social-Media-Kanäle verbreitet. Diese Aktionen zielen darauf ab, Misstrauen gegenüber den USA und der NATO zu schüren und die russische Invasion der Ukraine als präventive Maßnahme gegen eine angebliche Bedrohung darzustellen.
– Leugnung von Kriegsverbrechen und zivilen Opfern: Chinesische Medien haben auch dazu beigetragen, russische Desinformation zu verbreiten, die darauf abzielt, Berichte über Kriegsverbrechen und zivile Opfer, die russischen Streitkräften zugeschrieben werden, zu leugnen oder in Frage zu stellen. Ein Beispiel dafür war das Massaker von Butscha 2022. China unterstützt indirekt Russlands Bemühungen, seine militärischen Aktionen in der Ukraine zu rechtfertigen und internationale Kritik zu untergraben.

Taiwan, der von Festland-China abtrünnige Inselstaat, ist jedoch bei weitem die wichtigste Zielscheibe chinesischer

Desinformation. Kein anderes Land, so ergaben zahlreiche Studien, ist so von Desinformation betroffen wie Taiwan. Chinas Desinformationskampagnen gegen das Land sind Teil einer langfristigen Strategie, um die politische Landschaft und die öffentliche Meinung zu beeinflussen, Zweifel an der Legitimität der taiwanesischen Regierung zu säen und die Idee der Wiedervereinigung unter Pekings Bedingungen zu fördern. Diese Kampagnen nutzen eine Vielzahl von Methoden, einschließlich sozialer Medien, gefälschter Nachrichten und psychologischer Kriegsführung. Einige Beispiele dafür sind:

– Selbstmord von Su Chii-cherng: Im Jahr 2018 nahm sich Su Chii-cherng, der Direktor des Osaka-Büros des taiwanesischen Außenministeriums, das Leben. Grund dafür waren massive Anschuldigungen gegen ihn, taiwanesischen Bürgern in Japan nach einer Tsunamikatastrophe nicht geholfen zu haben. Diese fälschlichen Anschuldigungen verbreiteten sich rasant über soziale Medien und wurden von verdeckten chinesischen Accounts befeuert. Sein Tod wiederum wurde ebenfalls von chinesischen Desinformationskampagnen ausgenutzt, die falsche Narrative und Gerüchte verbreiteten.
– Präsidentschaftswahl in Taiwan 2024: Im Vorfeld der Präsidentschaftswahlen von 2024 intensivierte China seine Bemühungen, durch Desinformationskampagnen Einfluss auf den Wahlprozess zu nehmen. Diese Kampagnen umfassten die Verbreitung gefälschter Nachrichten über soziale Medien, die darauf abzielten, die Kandidaten, die Peking gegenüber kritisch eingestellt waren, zu diskreditieren, und die pro-chinesischen Kandidaten und Positionen zu unterstützen. Ein chinesisches Hashtag, der den China-kritischen Spitzenkandidaten Lai Ching-te von der Demokratischen Fortschrittspartei (DPP) verspottete, erreichte mehr als 8,5 Millionen Aufrufe, und die Reaktionen auf Beiträge und Videos gegen die DPP waren voll von abfälligen Kommentaren und Verschwörungstheorien. Ein besonders hartnäckiger Vorwurf, der auch durch KI-Fälschungen (»Deepfakes«)

in den sozialen Medien verbreitet wurde, war die unbegründete Behauptung, dass Lais Running Mate Hsiao Bi-khim US-Bürgerin sei und somit nicht wählbar wäre.
– COVID-19: Während der COVID-19-Pandemie nutzte China Desinformationskampagnen, um falsche Informationen über Taiwans Umgang mit dem Virus zu verbreiten. Diese Kampagnen behaupteten irreführend, dass die taiwanische Regierung die Schwere der Pandemie verberge und die öffentliche Gesundheit gefährde. Ziel dieser Falschinformationen war es, Misstrauen gegenüber der taiwanischen Regierung zu säen und Chinas eigene Bemühungen zur Bekämpfung des Virus in einem positiveren Licht darzustellen.

TikTok und Desinformation

TikTok ist die wahrscheinlich erfolgreichste Social-Media-Plattform der letzten Jahre. Sie bietet Kurzvideos an und ist vor allem bei jungen Zielgruppen äußerst populär. Anders als alle anderen globalen Social-Media-Plattformen ist TikTok keine US-amerikanische Firma, sondern wird von der chinesischen Firma »ByteDance« betrieben. Forscher und Journalisten haben immer wieder hervorgehoben, dass TikToks Erfolg darauf beruht, dass die Algorithmen, die den Nutzern ihre Inhalte vorschlagen und so großen Einfluss auf die angezeigten Informationen haben, von allen anderen Social-Media-Plattformen abweichen, wodurch Inhalte viel schneller und viel größer »viral gehen«.

Untersuchungen haben Hinweise darauf geliefert, dass TikTok Beiträge zu Themen, die von der chinesischen Regierung und der Kommunistischen Partei Chinas als sensibel eingestuft werden, herabgestuft hat. Videos zu Taiwan oder Hongkong zum Beispiel, die der offiziellen Politik Chinas widersprechen, sind schwerer zu finden und erreichen nicht dieselbe Reichweite. Zu den Themen, die angeblich von der Plattform zensiert wurden, gehören der Völkermord an den Uiguren, die Proteste in Hongkong 2019–2020, der Grenzkonflikt zwischen China und Indien, ausländische politische Führer, LGBTQ+-Personen, behinderte Menschen und schwarze Menschen. TikTok hat auch Informationen aus seinen Diensten entfernt, um den Unternehmensrichtlinien, rechtlichen Anforderungen und staatlichen Zensurgeset-

zen in China zu entsprechen. Die Reaktionen von TikTok auf Vorwürfe der Zensur waren unterschiedlich, wobei das Unternehmen behauptete, es habe versucht, Nutzer vor Mobbing zu schützen, oder es argumentierte, dass bestimmte Vorfälle auf menschliche Fehler zurückzuführen seien.

Darüber hinaus ist TikTok auch eine beliebte Plattform für chinesische (und auch alle anderen) Desinformationsnetzwerke. Im Sommer 2023 identifizierte Meta 284 Nutzerkonten auf TikTok, die mit einer chinesischen Desinformationskampagne in Australien in Verbindung standen. Laut Meta umfasste das Netzwerk fast 9.000 Facebook- und Instagram-Konten, Gruppen und Seiten, die mit einem chinesischen politischen Spam-Netzwerk verbunden waren, das Nutzer in Australien und anderen Teilen der Welt ins Visier genommen hatte. Die Untersuchung von Meta deckte die Einflussoperation auf mehr als 50 Online-Plattformen und Foren auf, einschließlich YouTube, TikTok, Reddit, Pinterest, Medium, Blogspot, Livejournal und X (ehemals Twitter) – zusätzlich zu Instagram und Facebook. Das Netzwerk veröffentlichte positive Kommentare zu China und der Provinz Xinjiang sowie negative Kommentare zu den USA, westlicher Außenpolitik und Kritikern der chinesischen Regierung. Die Videos des Netzwerks auf TikTok konzentrierten sich stark auf Berichte über Zwangsarbeit in Xinjiang und über Taiwan. Einige dieser Videos erreichten Zehntausende von Aufrufen.

In einem anderen Fall war TikTok die Plattform, über die KI-Fälschungen (»Deepfakes«) gestreut wurden; zum Beispiel wurden die chinakritische Partei DPP und ihr Spitzenkandidat Lai durch die Verbreitung falscher Reden angegriffen. Diese Videos hatten auf TikTok mehrere Hunderttausend Aufrufe.

Chinesische »Wolfskrieger«

»Wolfskriegerdiplomatie« bezeichnet einen aggressiven und konfrontativen Stil chinesischer Diplomatie, der von Diplomaten und offiziellen Vertretern in den letzten Jahren geprägt wurde. Benannt nach der populären chinesischen Filmreihe »Wolf Warrior«, zeichnet sich diese Diplomatie durch kämpferische Rhetorik, die entschiedene und aggressive Verteidigung nationaler Interessen und eine oft provokative

Reaktion auf Kritik an China aus. Ziel ist es, Chinas Stärke und Entschlossenheit auf der internationalen Bühne zu demonstrieren und gleichzeitig Kritiker einzuschüchtern und Gegner abzuschrecken. Ein Beispiel dafür ist: Zhao Lijian sorgte als stellvertretender Direktor des Informationsbüros des chinesischen Außenministeriums und Sprecher des Ministeriums durch seine Botschaften in den sozialen Medien für Aufsehen. Besonders bekannt wurde er für seine Tweets, in denen er die USA und andere westliche Länder direkt angegriffen und Verschwörungstheorien verbreitete (z. B., dass das US-Militär das Coronavirus nach China gebracht haben könnte). Seine direkte und oft angriffslustige Art symbolisiert den Wechsel Chinas zu einer offensiveren Außenpolitik.

Ein anderes Beispiel war die Reaktion auf die Kritik an der Behandlung der uigurischen Minderheit in China. Chinesische Diplomaten und staatliche Medien haben aggressiv auf internationale Kritik am Umgang Pekings mit den Uiguren in Xinjiang reagiert. Anstatt Zurückhaltung zu üben oder sich auf diplomatische Gespräche zu beschränken, haben sie eine Gegenoffensive gestartet, die Kritiker der Verbreitung von »Fake News« beschuldigt oder Gegenberichte veröffentlicht, die Chinas Politik verteidigen. Diese Reaktionen beinhalten auch Drohungen gegen Länder oder Organisationen, die Sanktionen gegen China wegen seiner Menschenrechtssituation in Betracht ziehen.

USA

Als globale Supermacht und Hegemon stehen auch die USA oft am Pranger wegen Einflussnahme auf ausländische Staaten oder Desinformation. Grundsätzlich gibt es viele Beispiele dafür, dass auch die USA über Geheimdienste wie die CIA oder das Militär in anderen Staaten falsche Informationen verbreitet haben. »Psychologische Kriegsführung«, Informationsoperationen und Einflussnahme werden also auch von offiziellen US-amerikanischen Stellen wie den Geheimdiensten oder dem Militär durchgeführt. Dabei sind jedoch einige wichtige Abgrenzungen

und Unterschiede zu autoritären Staaten wie Russland oder China und deren staatlicher Desinformation notwendig.

Zum einen unterscheidet sich der Umfang, Einsatz und die Dauer von Einflussoperationen oder staatlicher Desinformation aus den USA ganz erheblich. Anders als in Russland oder China ist Desinformation kein fester und regulärer Bestandteil von US-Außenpolitik, sondern kommt, wie die Beispiele unten verdeutlichen, punktuell und zeitlich begrenzt, im Rahmen von militärischen Engagements und Konflikten zum Einsatz (meist als Ergänzung zu militärischen Operationen).

Darüber hinaus finden solche Operation nicht gänzlich unkontrolliert und außerhalb von rechtlichen Rahmen statt und haben Ressourcen, die wesentlich geringer sind als in Russland oder China. Dies unterscheidet Demokratien von autoritären Staaten. Konkret werden in den USA solcherart verdeckte Aktionen oder »psychologische Kriegsführung« von verschiedenen Kontrollinstanzen im Weißen Haus, dem Pentagon, aber auch dem Senat und Kongress sowie nicht zuletzt von Medien und der Zivilgesellschaft kontrolliert. Daher gelten innerhalb solcher Operationen oftmals wesentliche Beschränkungen und Restriktionen, was den Einsatz von offenen Lügen und Fälschungen angeht. Ein CIA-Mitarbeiter der Abteilung für »verdeckte Aktionen« sagte zum Beispiel über die strikten Vorgaben für solche Aktionen während des Kalten Krieges: »Anders als die Sowjets konnten wir nicht lügen. Wir durften maximal die Wahrheit und Fakten ›verbiegen‹ oder ›verzerren‹, aber nicht lügen oder einfach erfinden.« Erfolgreiche Operationen dieser Abteilung in der zweiten Hälfte des Kalten Krieges bestanden so nicht in der globalen Verbreitung von Falschmeldungen über die Sowjetunion, sondern in der Unterstützung der polnischen Opposition durch das Einschmuggeln von Druckerpressen und Materialien oder die massenhafte Übersetzung, Vervielfältigung und den Schmuggel von Alexander Solschenizyns »Archipel Gulag«.

Ein weiterer gewichtiger Unterschied zwischen den USA und den anderen beiden »big playern« in der Welt der

Desinformation entsteht durch die (in den USA im Vergleich zu Deutschland ultraliberale) Meinungs- und Pressefreiheit. So gibt es ein breites Spektrum an extrem populären und global empfänglichen privaten Medien, wie »Fox News« oder »Breitbart«, die massenhaft Populismus, Falschnachrichten, Desinformation und Hass verbreiten. Anders als in autoritären Staaten sind diese jedoch privat und nicht von der Regierung kontrolliert und verbreiten Desinformation nicht im Regierungsauftrag. In den letzten zehn Jahren haben sich diese Medien zwar als globales Problem erwiesen, da ihre Inhalte massenhaft übersetzt und online verbreitet werden, dies ist jedoch keine offizielle US-Politik oder staatliche Desinformation.

Ein ähnliches Phänomen entsteht durch andere private (und privatwirtschaftliche) Organisationen und Unternehmen in den USA. Auch hier gibt es viele reichweitenstarke Akteure, die global Desinformation verbreitet haben. Eine solche Organisation ist zum Beispiel die »Prager University« oder »PragerU«. Anders als der Name vermuten lässt, ist dies keine Universität oder Bildungseinrichtung, sondern eine vorgeblich gemeinnützige Organisation, die sich durch große, meist anonyme Spenden finanziert. Diese Organisation wurde von einem Radiomoderator und einer Drehbuchautorin gegründet und produziert massenhaft Online-Videos mit erzkonservativen politischen, wirtschaftlichen, religiösen und philosophischen Inhalten. Besonders oft werden die Themen Klimawandel und Energie, Christentum, Sklaverei und Minderheitenrechte behandelt. Die Videos sind für ihre höchstumstrittenen Inhalte bekannt, die wissenschaftliche Erkenntnisse ablehnen oder verneinen, Meinungen zu Fakten erklären oder einseitige wirtschaftliche Interessen (z. B. von Energieunternehmen) propagieren.

Ein anderes Beispiel für solche Desinformationskampagnen sind globale PR-Kampagnen von US-Unternehmen, die wissentlich falsche Studien und Informationen produzieren und global verbreiten, um ihre wirtschaftlichen Interessen zu schützen. Sowohl Tabak- als auch Erdölkonzerne waren auf

diesem Feld erwiesenermaßen in der Vergangenheit tätig. Ähnlich wie bei »PragerU« gilt jedoch auch hier: Dies waren (und sind) keine staatlichen Desinformationskampagnen, sondern sie werden von privaten Akteuren aus den USA organisiert und durchgeführt (und dienen ihren Interessen).

»Politische Kriegsführung« der CIA in den 1950er-Jahren in Berlin

Nach dem Ende des Zweiten Weltkrieges und mit Beginn der »heißen Phase« des Kalten Krieges in den 1950er- und 1960er-Jahren setzten die US-Regierungen, Geheimdienste und das Militär oft auf aggressive Informationsoperationen. Neben den Staaten Lateinamerikas und Afrikas betraf dies vor allem auch das geteilte Deutschland, vor allem in Berlin. Dort finanzierte und unterstützte die CIA beispielsweise einige Organisationen, die Flüchtlinge aus der DDR unterstützten, Informationen über Politik, Staat, Gesellschaft und Wirtschaft im Osten sammelten und ausgiebige Informations- und Propagandamaßnahmen durchführten. Ein Beispiel dafür war die »Kampfgruppe gegen Unmenschlichkeit«, die eine Reihe von Aktivitäten in West-Berlin und der DDR durchführte. Dazu gehörte das Verteilen von Postern, Flugblättern und Publikationen, durch die die Moral, der Glaube und die Unterstützung für das sowjetisch-unterstützte Regime und den Sozialismus geschwächt werden sollten.

Während die »Kampfgruppe gegen Unmenschlichkeit« in ihren Aktivitäten zur »psychologischen Kriegsführung« seltener auf Fälschungen und Falschinformationen zurückgriff, machten andere CIA-Operationen ausführlich davon Gebrauch. Eine der größten war die Operation »LCCASSOCK«. Diese Operation bestand aus der Gründung einer Tarnorganisation »Cramer Werbung« (später: Äquator Verlag) in West-Berlin, die von dem ehemaligen U-Boot Kapitän Karl-Heinz Marbach geleitet wurde. Ihr Auftrag: Offizielle DDR-Zeitschriften und Publikationen zu fälschen und mit falschen Inhalten zu versehen und sie anschließend wieder in der DDR zu verbreiten. 600.000–900.000 solcher gefälschten Publikationen soll Marbachs Büro, das zum Schluss 35 Mitarbeiter umfasste, jedes Jahr erstellt und verteilt haben. Die Kosten dieser Operation beliefen sich für die CIA auf bis zu 60.000 US-$ jährlich.

Später gingen Marbach und die CIA auch dazu über, eigene Magazine und Publikationen mit wilden Storys und Falschnachrichten zu erstellen und sie zum Beispiel an Angehörige der DDR-Armee oder Mitglieder der SED gezielt zu versenden. Auch personalisierte (und völlig erfundene) Horoskope wurden an DDR-Funktionäre und hochrangige Mitglieder des DDR-Geheimdienstes versendet. Ab 1956 produzierte das Team Marbachs auch ein Jazz-Magazin (»Schlagzeug«), das in der Bundesrepublik sehr populär wurde und auch in der DDR verteilt wurde. Das Magazin bestand zum Großteil aus normalen Musiknachrichten und Storys und wurde gelegentlich mit »subversiven« Artikeln versehen. Ab 1958 änderte die CIA die Ausrichtung ihrer »politischen Kriegsführung«, kürzte die Mittel für die Fälschungsoperationen und stellte »LCCASSOCK« schließlich 1960 ein. Ein Grund dafür war, dass sowohl die US-Regierung als auch die CIA sich mehr und mehr gegen den Einsatz von Fälschungen in der Propagandaauseinandersetzung aussprachen. Zum einen, weil dies in offensichtlichem Widerspruch zur demokratischen Tradition und den als Leitlinien des »freien Westens« propagierten Werten stand; und zum anderen waren die Strategen in Washington nicht davon überzeugt, dass Fälschungen und Lügen mehr und bessere Effekte brachten als positive Informationsarbeit. Beides stand in direktem Widerspruch zu den Strategien und Operationen der Sowjetunion.

Globale Desinformation privater Medien – »Breitbart«

»Breitbart News«, auch bekannt als »Breitbart« oder »Breitbart.com«, ist eine amerikanische Nachrichten-, Meinungs- und Kommentarwebsite der extremen Rechten. Sie wurde 2007 von dem konservativen Kommentator Andrew Breitbart gegründet. Die Inhalte der Website werden von Experten, Wissenschaftlern und Journalisten als frauen- und fremdenfeindlich und rassistisch eingeschätzt. Darüber hinaus veröffentlicht »Breitbart« regelmäßig Verschwörungstheorien und absichtlich irreführende Geschichten, zum Beispiel über Klima- und Umweltfragen, die Covid-19-Pandemie oder es verbreitet falsche Behauptungen über Wahlmanipulationen bei der Präsidentschaftswahl 2020. Trotzdem gehören Beiträge von der Breitbart-News-Face-

book-Seite zu den am weitesten verbreiteten politischen Inhalten auf Facebook.

Mit den Jahren hat sich »Breitbart News« als Sprachrohr der »Alt-Right«-Bewegung (sogenannte »Alternative Rechte«), der europäischen populistischen Rechten und der paneuropäischen nationalistischen Identitären Bewegung unter der Leitung des ehemaligen Exekutivvorsitzenden Steve Bannon ausgerichtet. Bannon erklärte die Website 2016 zu der Plattform der neuen Rechten und im Folgenden wurde Breitbart News zu einem virtuellen Sammelbecken für Unterstützer von Donald Trump.

»Psychologische Operationen« der US-Armee im Nahen Osten 2016–2022

2022 veröffentlichten US-Medien Informationen, die eine verdeckte Online-Propagandakampagne (»PsyOp«) des US-Verteidigungsministeriums (Pentagon) im Nahen Osten enthüllten. Diese wurde offenbar mit Kenntnis und Duldung des Kurznachrichtendienstes »Twitter« (heute »X«) durchgeführt. Ziel war es, die öffentliche Meinung in Staaten wie Jemen, Syrien, Irak und Kuwait zu beeinflussen. Als normale Nutzer getarnte Accounts des Pentagons verbreiteten dabei proamerikanische Botschaften und Narrative, twitterten gegen extremistische Gruppen und Milizen in der Region und verbreiteten negative Informationen über die Politik und Verbindungen des Iran in dieser Region. So sollten die außenpolitischen und militärischen Aktivitäten der USA in diesen Ländern unterstützt werden. Konkrete Beispiele für die von den verdeckten Konten verbreiteten Informationen betrafen z. B. die angebliche Genauigkeit von US-Drohnenangriffen in der Region, die nur Terroristen und keine Zivilisten töten würden, und riefen zur Unterstützung der von den USA und Saudi-Arabien durchgeführten Offensive gegen die Huthi-Rebellen im Jemen auf. Andere Accounts verbreiteten Botschaften zur Unterstützung der mit den USA verbündeten Gruppen und Milizen in Syrien oder beschuldigten Iran und seine Verbündeten in Syrien und dem Irak (z. B., dass sie die Wassersicherheit des Iraks bedrohen, das Land mit Crystal Meth überschwemmen und iranische Verbündete afghanische Flüchtlinge für organisierten Organhandel missbrauchen würden).

Trotz Twitters damaliger öffentlicher Haltung gegen staatlich unterstützte Propaganda wurden diese dem US-Militär zugeordneten Konten vom Unternehmen in direkter Absprache privilegiert behandelt. Das erlaubte dem Pentagon, als normale Nutzer getarnt, Botschaften zu verbreiten, die den Interessen der USA entsprachen. Die Informationen wurden 2022 öffentlich, offenbar als gezielte Veröffentlichung nach dem Kauf von Twitter durch Elon Musk.

2022 enthüllte auch Meta, der Mutterkonzern von Facebook, Instagram und Whatsapp, Informationen zu einer gezielten Einflusskampagne, die der Konzern dem US-Militär zuordnete. In der ersten Jahreshälfte 2022 löschte Meta in diesem Kontext 39 Facebook-Profile, 16 Seiten, zwei Gruppen and 26 Instagram-Accounts, die zwar versuchten ihren Ursprung zu verbergen, Meta aber dem US-Verteidigungsministerium zuordnete. Dieses Netzwerk sei in Afghanistan, Algerien, Iran, Irak, Kasachstan, Kirgistan, Russland, Somalia, Syrien, Tadschikistan, Usbekistan und Jemen aktiv gewesen und außer den Meta-Diensten auch noch auf Twitter, YouTube, Telegram und den russischen Plattformen VKontakte und Odnoklassniki gepostet. Trotz dieser breiten und cross-medialen Aktivitäten der gefunden Accounts habe die Mehrheit der Posts wenig oder überhaupt keine Interaktion und Aktivität mit echten Accounts, sprich nahezu keine Wirkung, gehabt.

Die »Neue Rechte«: Populismus, Extremismus, Verschwörungstheorien und ausländische Einflussoperationen

Die in den vergangenen Jahren massiv aufgestiegenen Bewegungen, Organisationen, Parteien und Medien rechtsnationaler, rechtspopulistischer und rechtsextremistischer Ideologie setzen Desinformation als ein strategisches Instrument ein, um ihre politischen Ziele zu erreichen. Diese bestehen nicht nur in der Propagierung eigener politischer Positionen, sondern in der Diffamierung politisch Andersdenkender, der gezielten Schwächung des Vertrauens in die Demokratie, den Rechtsstaat, die Behörden, Institutionen und traditionellen Medien. Durch die Schaffung neuer gesellschaftlicher

Spannung oder die Vertiefung bestehender Spannungen sollen diese Ziele erreicht werden. Mittel dabei sind Polarisierung, Skandalisierung, Emotionalisierung, Negativbotschaften, Angst, Hass, Verschwörungstheorien, neue und alte Feindbilder sowie eine ständige Täter-Opfer-Umkehr. Die Destabilisierung demokratischer Gesellschaften, die Verbreitung nationalistischer und xenophober Haltungen sowie die Ablehnung von Migration, Minderheitenrechten, aber auch Antihaltungen in Klima- und Umwelt- oder sozialen Fragen sind dabei wichtige Themen. Zudem wird Desinformation eingesetzt, um pro-russische Narrative zu verbreiten und die öffentliche Meinung in Bezug auf geopolitische Ereignisse, zum Beispiel den russischen Krieg gegen die Ukraine, zu beeinflussen. Diese Themen und Strategien treten dabei nicht in einzelnen Ländern auf, sondern kennzeichnen neurechte Bewegungen in den USA und in ganz Europa.

Der Einsatz von Desinformation durch Gruppierungen und Organisationen der »Neuen Rechten« in Deutschland, den USA und in Europa zeichnet sich durch eine Vielzahl von Mechanismen und Medien aus. Dabei fand und findet ein internationaler Lern- und Austauschprozess zwischen den Gruppen statt. Als Vorlage dienen zumeist die Strategien, Botschaften und Medien der amerikanischen »AltRight«. So fanden zum Beispiel Verschwörungserzählungen wie »QAnon« erst von dort ihren Weg in die Diskurse und Medien europäischer rechter Bewegungen. Unter deren Wählern und Anhängern sind sie wesentlich stärker und häufiger verbreitet als in allen anderen Gruppen. Ähnliches gilt für Falschinformationen und Verschwörungsnarrative über »gestohlene Wahlen« und Wahlfälschungen (z. B. durch digitale Wahlmaschinen statt analoger Wahlzettel). Auch diese Botschaften wurden zuerst von einschlägigen US-Medien und Social-Media-Gruppen im Umfeld der Präsidentschaftswahlen von 2020 entwickelt, getestet und verbreitet, bevor sie dann fester Bestandteil jeder Kommunikationsstrategie rechtspopulistischer Bewegungen in Europa wurden.

In Europa sind mittlerweile die russische Messengerapp »Telegram« sowie die chinesische Kurzvideo-App »TikTok« die wichtigsten Verbreitungskanäle für neurechte Propaganda und Desinformation. Während »TikTok« zum Beispiel für die Partei »AfD« immer wichtiger geworden ist, spielt »Telegram« in der Kommunikationsstrategie rechtsextremistischer Aktivisten eine zentrale Rolle, um Gewalt-, Hass- und Propagandanachrichten ungehindert zu verbreiten. Außerdem dient es als Treffpunkt für Gleichgesinnte sowie für die Organisation von Demonstrationen, Versammlungen und anderen Aktionen. Aktivierung, Rekrutierung, Indoktrinierung, Radikalisierung und Organisation sind zentrale Funktionen solcher Plattformen und Medien. Die dabei verbreiteten Narrative sprechen vor allem von Bedrohungen, »Gegenwehr« und »Widerstand«.

Die Desinformationsstrategien der »Neuen Rechten« zielen allgemein darauf ab, politische Debatten zu beeinflussen, Misstrauen gegenüber allen traditionellen Institutionen, Parteien, Politikern und Medien zu schüren und die öffentliche Meinung zu polarisieren. Im Laufe der vergangenen Jahre zeigt sich, dass dazu nahezu jedes aktuelle und gesellschaftlich relevante Thema oder Ereignis vereinnahmt und instrumentalisiert wird, auch wenn dies mit den Grundthemen und Positionen der Parteien und Organisationen nichts zu tun hat. So war in Deutschland zu beobachten, dass Parteien, Politiker, Aktivisten-Webseiten, Influencer oder Social-Media-Kanäle, die sich während der Corona-Pandemie ausschließlich mit Corona-Desinformation beschäftigten, auf einmal ihre Themen änderten und nacheinander die Flutkatastrophe im Ahrtal, den russischen Angriff auf die Ukraine, ukrainische Flüchtlinge in Deutschland, Militärhilfe für die Ukraine, Migration, Energiepreise und »Energiewende« und im Dezember 2023 und Januar 2024 schließlich die Bauernproteste behandelten. Wie Studien zeigen, traten dabei Verbindungen zwischen den Organisatoren und Aktivsten von Protesten, den Verbreitern von Online-Desinformation und neurechten Bewegungen und Parteien auf. Dabei zeigt sich ein Muster, dass sowohl bei

digitaler Desinformation als auch Protest- und anderen Aktionen rechtsextremer Akteure in den USA und Europa immer wieder zu beobachten ist: Tagesaktuelle, sensible und kontroverse Themen werden sowohl durch Online-Desinformation als auch durch Straßenaktionen vereinnahmt. Dabei wird versucht, den Eindruck zu erwecken, dass die eigenen radikalen Positionen viel größer und weiterverbreitet seien, als es tatsächlich der Fall ist. Demokratisch völlig legitimer Protest und Demonstrationen von Bauern gegen die Regierungspolitik werden durch massive Online-Kampagnen und Aktionen auf der Straße so dargestellt, als würden alle protestierenden Bauern »das System«, traditionelle Medien und Parteien etc. ablehnen und seien allesamt zu radikalen und gewaltbereiten Aktionen bereit (obwohl dies nur für eine Minderheit zutrifft).

Ein anderer Aspekt rechtsextremer Desinformation ist eine immer öfter zu Tage tretende Kooperation mit bzw. Unterstützung durch ausländische(n) Einflussoperationen. Dies betrifft insbesondere Russland (und in geringerem Ausmaß China). Einerseits wurden in den letzten Jahren immer mehr direkte persönliche Verbindung und Unterstützung zwischen rechtspopulistischen und rechtsextremen Parteien und der russischen Regierung bekannt. Andererseits verfolgen beide Desinformationsmaschinerien dasselbe Ziel: Die Schwächung westlicher Gesellschaften, Medien und Politik durch das Hervorrufen und Verstärken von Spannungen, Misstrauen und Konflikten. Dies zeigte sich vor allem in Zuge des russischen Angriffskrieges gegen die Ukraine. Hier war z. B. in Deutschland zu beobachten, dass viele rechte Netzwerke, die zuvor vor allem durch Proteste, Verschwörungstheorien und Desinformation über die Corona-Pandemie aufgefallen sind, auf einmal das Thema wechselten und nun (teils wörtlich) die Informationen russischer Propaganda oder Online-Kanäle übernahmen.

Ein anderes aufschlussreiches Beispiel stammt aus den USA. Hier entbrannte im Januar 2024 ein heftiger Streit in Texas, nachdem die US-Regierung den vom dortigen Gouverneur Abbott angeordneten Stacheldraht an der Grenze zu Mexiko

entfernen ließ. Sowohl online als auch bei Protestaktionen propagierten neurechte Gruppen eine vermeintliche »Invasion« durch mexikanische Migranten und heizten die Wut auf die Regierung von Präsident Biden an. So kam es zu einem Trucker-Konvoi Richtung Grenze. Eines der Schlagworte, die rechte Gruppen online massiv verbreiteten, war »Texit« und meinten einen Austritt von Texas aus den Vereinigten Staaten. Dadurch sollten gezielt Erinnerungen an den US-amerikanischen Bürgerkrieg, aber auch den »Brexit« geweckt werden. Offizielle und inoffizielle russische und chinesische Online-Kanäle griffen die Ereignisse, aber auch den Begriff »Texit« auf, um die Nachricht eines drohenden Bürgerkriegs in den USA zu verstärken. Russland setzte dabei auf eine Mischung aus offener und verdeckter Einflussnahme, während aus China verfälschte Bilder und Videos verbreitet wurden, um die Falschmeldung einer offiziellen Kriegserklärung von Texas an die US-Regierung zu unterstützen.

Andere Staaten und private Firmen

Die Landschaft der Staaten, aber auch der nicht-staatlichen Akteure, die zunehmend in Desinformationskampagnen verstrickt sind, nimmt stetig zu. Im Gegensatz zu den oben beschriebenen großen, global aktiven Staaten, sind ihre Aktivitäten jedoch oft regional oder thematisch begrenzt.

Das islamistische Regime des Iran setzt ebenfalls aggressive Instrumente und Kampagnen in der digitalen Welt ein. Manchmal geht es dabei darum, die öffentliche Wahrnehmung in verschiedenen Ländern bezüglich außen- und geopolitischer Themen (z. B. der Konflikt mit Saudi-Arabien, die iranische Unterstützung für Milizen und Gruppen im Nahen Osten oder Jemen) zu beeinflussen; oftmals geht es jedoch um Diskreditierung, Verunsicherung oder Verleumdung exil-persischer Organisationen. Oft waren solche Desinformationskampagnen auch im Zusammenspiel mit Cyberattacken zu beobachten und manchmal auch in Kombination mit Spionage, Sabotage und Mordanschlägen.

Auch die Türkei geriet in manchen Ländern im Zusammenhang mit Desinformationskampagnen in den Fokus. Auch hier waren oft exil-türkische Oppositionsgruppen das Ziel. Andere Ziele waren Einflussnahme und ein positives Türkeibild zum Beispiel in bestimmten Ländern Südosteuropas (Albanien, Kosovo, Bosnien). Der stetig schwelende Konflikt zwischen dem türkischen Staat und der kurdischen Bevölkerung mit ihren politischen Organisationen wird ebenfalls von digitalen Propaganda- und Einflusskampagnen begleitet, wozu türkische Organisationen und Medien genutzt werden.

Katar und andere Golfstaaten tauchen ebenfalls immer wieder im Kontext von Desinformations- und Einflusskampagnen auf. Diese haben oft hybriden Charakter und beschränken sich nicht auf (digitale) Desinformation. Zielgebiete sind hier z. B. die Länder und Bevölkerungen des Nahen Ostens, aber auch arabischsprachige Exilanten und Minderheiten in anderen Ländern. Der international empfangbare Sender Al-Jazeera spielt dabei immer wieder eine Rolle. In der jüngsten Vergangenheit wurden durch interne Datenlecks und Whistleblower aus verschiedenen Firmen auch Informationen publik, nach denen diese Staaten vermehrt PR-Firmen beauftragen, um gezielt Falschinformationen und Verleumdungen zu lancieren. Katar zum Beispiel soll im Zuge der Fußballweltmeisterschaft 2022 nicht nur für positive PR viel Geld ausgegeben haben, sondern auch für Schmierkampagnen, Verleumdung und das »Übertönen« kritischer Stimmen. In mindestens einem anderen Fall vermuteten Investigativjournalisten Katar hinter einer Desinformationskampagne gegen eine deutsche Abgeordnete im Europaparlament. Inhalt der Kampagne waren Falschmeldungen, die Abgeordnete sei von den Vereinigten Arabischen Emiraten gekauft worden. Diese Vorwürfe wurden zunächst von einem realen Autor ohne Beweise in einem Blog veröffentlicht und anschließend über Social-Media-Kanäle verbreitet. Dieselben Accounts streuten danach dauerhaft falsche negative Meldungen über die Abgeordnete.

Die Vereinigten Arabischen Emirate wiederum, so zeigen abgeflossene Daten aus einer Schweizer Firma, sollen über ihre Geheimdienste jene in Genf sitzende Firma mit Desinformationskampagnen gegen einzelne Personen im Ausland beauftragt haben. Auch hier ging es offenbar um die Diskreditierung von Personen aus politischen Gründen, konkret um vermeintliche Mitglieder der Muslimbruderschaft. Dass die Emirate, wie offenbar auch Katar, auf die Hilfe von privaten Firmen angewiesen waren, deutet darauf hin, dass diese Staaten (und auch ihre Geheimdienste) – anders als die großen Akteure Russland, China oder USA – nicht selbst über die Mittel, Ressourcen und das Personal verfügen, um Desinformation auf globalem Niveau durchzuführen.

Private Firmen, PR-, Detektiv- und Sicherheitsfirmen, treten deshalb immer öfter im Kontext von Desinformation als Akteure auf. Sie werden von Staaten, anderen Firmen oder Organisationen mit Recherche, Konstruktion und Verbreitung von Falschmeldungen sowie der Einflussnahme auf Firmen, Einzelpersonen, aber auch Staaten, Politikern oder Wahlen beauftragt. Aus einer spanischen PR-Firma in die französische Presse ausgesickerten Informationen zufolge soll zum Beispiel der wiederum mit Katar verbundene Fußballverein Paris St. Germain als Kunde der Firma Desinformationskampagnen gegen eigene und fremde Spieler, Journalisten und andere missliebige Stimmen beauftragt haben. Der Verein bestritt dies jedoch.

In einem anderen Fall enthüllte ein internationales Team von Journalisten die Desinformationspraktiken einer israelischen Cybersecurityfirma genannt »Team Jorge«. Während eines vorgetäuschten Kundengesprächs mit den Journalisten soll der Chef der Firma damit geprahlt haben, über 20 Wahlen, zumeist in Afrika, aktiv für seine Kunden beeinflusst zu haben. Das Vorgehen der Firma gleicht dabei vielen der für russische und andere Geheimdienste beschriebenen Praktiken: Zunächst werden Telefone, Computer und andere Informationsträger von Politikern und anderen Personen gehackt

und die so erbeuteten Daten ausgewertet und selektiv manipuliert oder direkt veröffentlicht. Nach der Veröffentlichung, so »Team Jorge«, werden die Informationen dann über automatisierte Fake-Accounts auf Social-Media-Plattformen massiv verbreitet. In einigen Fällen, so die Eigenwerbung, hätten sich daraus auch Demonstrationen und Proteste entwickelt.

Gleichfalls im Bereich Desinformation und Propaganda unterwegs sind weltweite Terrororganisationen. Hier sind vor allem islamistische Gruppen wie der sogenannte »Islamische Staat« oder »Al-Qaida«, aber auch regionale Gruppen wie »Boko Haram« in Afrika oder die Hamas im Nahen Osten aktiv. Sie haben über Jahre ihre Eigenwerbung und Propaganda immer weiter verbessert und an ihre Zielgruppen angepasst. Regelmäßig filmen und fotografieren sie ihre Aktionen und Anschläge oder übertragen sie gleich live im Internet oder auf Messengerdiensten. So zum Beispiel die Hamas während ihres Überfalls auf Israel im Oktober 2023. Solche Bilder sollen vor allem Stärke und Macht vermitteln. Andererseits rekrutieren diese Organisationen aber auch über Social Media und Messengerdienste, verbreiten Texte, Reden, Image- und Rekrutierungsvideos usw. Eine – aus vielen staatlichen Desinformationskampagnen bekannte – Strategie ist dabei die Täter-Opfer-Umkehr und ein »Opfernarrativ«. Gewalt und radikale Überzeugungen (ähnlich wie Angriffskriege von Staaten) sollen so nicht als aktive eigene Position, sondern lediglich als Reaktion, Notwehr und Resultat heruntergespielt werden. Wiederum waren Social-Media-Debatten nach dem Angriff der Hamas auf Israel im Oktober 2023 ein gutes Beispiel hierfür. Massiv und millionenfach wurde teils über von Hamas & Co. selbst betriebene Kanäle und Accounts das Narrativ verbreitet, Hamas und Palästina seien die Opfer israelischer Aggression (und nicht, dass der israelische Angriff eine Folge des Hamas-Anschlags war). In diesen Debatten ließ sich erstmals der bis dahin massivste und zahlenmäßig größte Einsatz von KI-generierten Bildern feststellen.

Desinformation und die Wirtschaft – eine unterschätzte Gefahr

Desinformation ist nicht nur ein politisches oder journalistisches Thema bzw. Problem, sondern betrifft auch viele Unternehmen. In vielerlei Hinsicht unterscheiden sich Desinformationskampagnen kaum von klassischen »negativen PR-« oder »Schmierenkampagnen«. Es geht darum, durch wahre, unwahre oder aus dem Kontext gerissene oder anderweitig manipulierte Informationen einen »Gegner«, z. B. ein konkurrierendes Unternehmen, schlecht zu machen. Das Ziel der Einflussnahme ist in der Regel ein rein finanzielles. So können zum Beispiel Börsenkurse manipuliert, Übernahmen oder Kooperationen verhindert oder erschwert, Umsätze geschmälert oder gezielt Proteste, Boykotts usw. hervorgerufen werden. Auf der Täterseite stehen dabei keineswegs nur konkurrierende Unternehmen, sondern immer öfter auch Staaten. Während der Corona-Pandemie zum Beispiel verzeichnete die Spionageabwehr des Verfassungsschutzes gezielte Falschmeldungen gegen deutsche Bio-Technologie-Unternehmen, die sie Russland zuordneten. Die Meldungen zielten vor allem darauf ab, Zweifel und negative Meldungen über Impfstoffe im Online-Raum zu verbreiten. In einem anderen Fall machten ein deutscher und ein französischer Social-Media-Influencer öffentlich, dass eine PR-Agentur in London mit Verbindungen nach Russland eine hohe Summe geboten hätte, wenn sie in ihren Beiträgen Sorgen und Horrormeldungen über angebliche Todesfälle in Verbindung mit einem bestimmten Corona-Impfstoff verbreitet hätten. Während diese zwei Influencer ablehnten, nahmen andere in Brasilien und Indien diesen Auftrag an. »Schlechtmachen« und das Schüren von Angst vor bestimmten

Produkten sind ein häufiges Mittel solcher negativen Kampagnen, auch wenn es um staatliche Auftraggeber geht. In einem anderen Fall stellte eine Studie eine erstaunliche Häufung von Negativberichten über sogenannte »genetisch manipulierte Lebensmittel« in den russischen Sendern »RT« und »Sputnik« just zu dem Zeitpunkt fest, als ausländische Firmen in dieser Sparte auf dem russischen Markt aktiv werden wollten. Bei einem anderen Beispiel in Deutschland lag ein Russlandbezug zwar auf der Hand, jedoch gab es keine konkreten Anhaltspunkte: Im Frühsommer 2022, wenige Monate nach Beginn des russischen Krieges gegen die Ukraine, wurden gezielt Bilder falscher Werbeposter und -bilder über Social Media verbreitet, die angeblich an einem deutschen Hauptbahnhof gesichtet wurden. Auf diesen war typische Werbung großer Konzerne zu sehen. Ihnen gemeinsam war, dass die Werbetexte sexistische und herabwürdigende Inhalte gegen ukrainische Flüchtlinge transportierten. Tatsächlich existierten diese Poster und Bilder nur als Online-Fakes, die offenbar gezielt sowohl ukrainischen Flüchtlingen als auch den Unternehmen schaden sollten. Es liegt nahe, dass sich hier politische und wirtschaftliche Zielsetzungen überschnitten haben, ein Urheber der Kampagne konnte jedoch nicht ausgemacht werden. So auch in einem ähnlichen Fall in den USA, wo eine Kaffeekette ebenfalls zum Opfer einer gezielten Kampagne von Online-Fakes wurde. Hier verbreiteten Social-Media-Profile massenhaft falsche Meldungen inklusive gefälschter Poster und Bilder, die einer bestimmten Gruppe illegaler Einwanderer kostenlosen Kaffee versprachen. Auch hier vermischten sich politische Ziele mit wirtschaftlichen Motiven.

Eine andere Form der gezielten Wirtschaftsdesinformation sind zumeist hochprofessionell aufgebaute Angriffe, um einzelne Börsenkurse zu beeinflussen. 2015 zum Beispiel manipulierten Unbekannte kurzzeitig den Aktienkurs von »Twitter«, indem sie dieselbe Desinformationstaktik anwandten, die auch bei politischen Einflussoperationen schon vorkam (vgl. Infokasten: Operation »Doppelgänger«). Sie bauten die

Webseite eines bekannten Nachrichtenportals täuschend echt nach und publizierten dort einen echt klingenden Bericht über ein angebliches milliardenschweres Kaufangebot für das Unternehmen. Dieser Bericht verbreitete sich massenhaft, bevor er widerlegt werden konnte, und produzierte innerhalb einer knappen halben Stunde einen Kursgewinn von mindestens 8 %. Im Januar 2024 wiederholte sich ein ähnlicher Angriff, diesmal jedoch noch ausgeklügelter: Unbekannte hackten das Social-Media-Konto der US-Börsenaufsicht SEC auf »X« (vormals Twitter) und setzten falsche Nachrichten über eine baldige Zulassung von Fonds der Kryptowährung »Bitcoin« ab. Die Nachricht sorgte kurzzeitig für einen massiven Kursanstieg. Ähnlich wie bei staatlichen Einflussoperationen vermischen sich hier aggressive Cyber-Angriffe mit gezielt gestreuten Falschinformationen, die dazu dienen, Aktienkurse und Unternehmenswerte gezielt zu manipulieren, um daraus finanziellen Nutzen zu erzielen.

Ein wiederum anderer Bereich gezielter Manipulation mittels falscher Informationen sind gefälschte Rezensionen, Bewertungen und Kommentare. Diese finden sich hauptsächlich auf den großen Online-Kundenportalen wie Amazon, Google Maps oder Tripadvisor sowie auf Buchungs- und Vergleichsportalen. Das massenhafte Verfassen und Veröffentlichen von Bewertungen war dort schon lange ein Geschäft für PR-Agenturen, die dazu – ebenso wie sogenannte staatliche Trollfabriken – entweder menschliche »Klickarbeiter« bezahlten oder automatisierte Bot-Programme einsetzten. Mit dem Aufkommen großer und öffentlich verfügbarer KI-Anwendungen, insbesondere den sogenannten »Großen Sprachmodellen« wie ChatGPT, vervielfachte und automatisierte sich das Geschäft mit gefälschten Bewertungen und Empfehlungen nochmals. Bereits wenige Monate nach der Veröffentlichung von ChatGPT fanden Forscher auf »X« und Amazon innerhalb eines kurzen Zeitraums rund 20.000 falsche Bewertungen, die eindeutig KI-Generatoren zugeordnet werden konnten. Hier geht es um die massenhafte und automatisierte Manipulation der

Kaufentscheidungen von Kunden sowie um Einfluss auf das Image von Marken und Produkten.

Auch wenn der finanzielle und wirtschaftliche Schaden von Desinformation für Unternehmen schwer zu messen ist, schätzte eine US-amerikanische Sicherheitsfirma, dass allein 2022 über 78 Milliarden (sic!) US-Dollar direkter Verluste für Unternehmen weltweit durch Informationsattacken dieser Art zu verzeichnen waren. Dazu addieren sich noch Kosten für Krisenmanagement und Gegenmaßnahmen. Desinformation ist in der digitalen Welt nicht nur ein Mittel politischer Manipulation, sondern eben auch ein Milliardengeschäft.

Krankheiten und Desinformation

Die Geschichte der Desinformation und Verschwörungstheorien zeigt, dass Krankheiten und Gesundheitsthemen besonders häufig zum Thema und Gegenstand gemacht werden. Schon im Mittelalter lautete eine gängige Verschwörungstheorie, die von politischen und kirchlichen Akteuren gezielt zur Ablenkung und Manipulation der Bevölkerung verbreitet wurde, dass »die Juden« die Pest-Plage durch Brunnenvergiftungen hervorgerufen hätten. Damit lieferte diese Verschwörungserzählung ein Grundmuster, dass bis in unsere Gegenwart immer weitergesponnen wird: Neue, zunächst unverständliche und plötzlich auftretende Krankheiten, vor allem, wenn sie tödlich sind und sich schnell verbreiten, werden durch absichtliches menschliches Handeln, also eine künstliche Herstellung und Verbreitung aus unlauteren Motiven, erklärt. Andere Beispiele dafür waren die Erzählungen, die Franzosen hätten die Syphilis (»französische Krankheit«) nach Deutschland gebracht, die Epidemie der »spanischen Grippe« nach dem Ersten Weltkrieg sei auf deutsche Biowaffen zurückzuführen oder dass die CIA und/oder die US-Armee in den 1950er-Jahren Kartoffelkäfer als Schädlinge in die DDR gebracht hätte(n), um Ernten zu vernichten.

Dem US-Pentagon wurde besonders häufig die Herstellung und Verbreitung von neu auftretenden Krankheiten zugeschrieben: In den 1980er-Jahren bei AIDS (siehe Infokasten) und bereits in den 1970er-Jahren bei Ebola und bei Lyme-Borreliose. Das Narrativ ist immer dasselbe: Alle diese Krankheiten seien von der US-Armee im Labor als biologische Waffen entwickelt worden und dann über Menschenversuche (besonders oft an Gefängnisinsassen und/oder ethnischen Minderheiten) in die Welt gesetzt worden. Abseits von Regierungen und Militär ist ein weiteres krankheitsbezogenes Dauerthema gezielter

Desinformation, dass Impfungen generell eine Marketing- und Verkaufsstrategie der Pharmaindustrie seien.

Die (vorerst) größte Kulmination zeigte sich allerdings zwischen 2020 und 2022 während der globalen Corona-Pandemie. Hier traten besonders viele und facettenreiche Desinformationsnarrative auf. Der künstliche Ursprung als Biowaffe kursierte Anfang 2020 noch in verschiedenen Versionen, manchmal in China, manchmal in den USA und manchmal in Russland. Später war die »Wuhan-Lab-Theory« das vorherrschende Narrativ, wenn es um den künstlichen Ursprung des Virus ging. Andere Narrative, die entweder die Existenz der Krankheit an sich verneinten, Regierungsmaßnahmen als »Umsturz« oder »Diktatur« bezeichneten oder aber in verschiedener Form die Schutzimpfungen angriffen (z. B. Mikrochips oder als tödliche Gefahr), wurden entwickelt und verbreitet. Die Desinformation im Zusammenhang mit Corona war sicherlich ein Unikum in der Geschichte der Desinformation; noch nie zuvor gab es so viele so unterschiedliche Falschinformationen, die so präsent waren und so massiv gestreut wurden. Nach dem Ende bzw. der Beruhigung der Pandemielage zeigte sich auch, dass politische und andere Akteure die Professionalisierung von Desinformation so weit vorangetrieben hatten, dass sich dieselben Akteure nun mit neuen Themen wie Naturkatastrophen, Migration, Wahlen und militärischen Konflikten beschäftigten oder versuchten, Corona-Desinformation 1:1 auf andere Krankheiten, wie die Affenpocken, zu übertragen.

Dabei gibt es eine Reihe von Faktoren, die erklären, warum gerade Krankheiten so oft im Fokus von Desinformation und Verschwörungstheorien stehen und welche Verbindungen bestehen:

Emotionalität und Irrationalität: Krankheiten betreffen jeden persönlich, weshalb emotionale und irrationale Reaktionen bei diesem Thema häufig sind. Dies macht Menschen anfälliger für Desinformation und Verschwörungstheorien.

Unsichtbarkeit und Unfassbarkeit: Krankheiten und Erreger, ebenso wie Ursprung und Verbreitungswege von Krankheiten,

sind zumeist unsichtbar und für Laien oft nicht einfach nachzuvollziehen. Bei sich rapide ausbreitenden, neuen Krankheiten sind verlässliche Informationen oft nicht vorhanden, was Unsicherheit und Panik befördert und Verschwörungstheorien attraktiv macht.

Mangelndes Wissen und wissenschaftliches Verständnis: Ein begrenztes Wissen über biologische, chemische und medizinische Prozesse macht Zielgruppen anfälliger für pseudowissenschaftliche Erklärungen. Dies wiederum ist ein fruchtbarer Boden für Desinformation, die ohnehin oft mit pseudowissenschaftlichen Erklärungen und/oder gefälschten oder gekauften »Experten« arbeitet.

Scheinbar unpolitische Natur von Krankheiten: Krankheiten werden oft als neutrale, unpolitische Themen wahrgenommen. Publikum und Zielgruppen von Desinformation erwarten deshalb oft nicht, dass diese Themen überhaupt zum Gegenstand politisierter Auseinandersetzungen und Einflussmaßnahmen gemacht werden. Dies wiederum erleichtert die Verbreitung und Aufnahme von Desinformation.

Schadenspotenzial: Gezielte Desinformationskampagnen zielen oft darauf ab, Misstrauen gegenüber Regierungen, Unternehmen oder bestimmten sozialen Gruppen zu schüren. Dies lässt sich durch Verschwörungserzählungen über Krankheiten recht einfach mit einem hohen Schadenspotential erreichen. Bestimmten Gruppen wie Ethnien, Konzernen oder Politikern kann leicht Schaden zugefügt werden, indem ihnen die Urheberschaft einer Krankheit zugeschrieben wird; dem Staat und seinen Organen kann darüber hinaus allgemein Schaden zugefügt werden, da ihm Versagen bei der Kontrolle und Eindämmung vorgeworfen werden kann. Und durch die zuvor beschriebenen Faktoren der Emotionalität, der allgemeinen Betroffenheit und der Unfassbarkeit von Krankheiten, ist auch die Zielgruppe wesentlich höher als bei anderen Themen.

Seit der gestiegenen Wahrnehmung von und Berichterstattung über Desinformation im öffentlichen Raum zeigt sich darüber hinaus noch eine weitere Verbindung mit dem Thema

Krankheit: Sowohl in der Forschung als auch im medialen und politischen Raum wird die Verbreitung und Wirkung von Desinformation häufig mit Begriffen aus der medizinischen Pathologie beschrieben (z. B. »Desinformation verbreitet sich wie ein Virus«, »Desinformation als digitale Seuche oder Pest« oder »Informationsimpfungen gegen Desinformation« etc.). Diese häufigen Analogien erscheinen als Sprachbild und, wie Forschungen zeigen, auch bei der Verbreitung von Desinformation als durchaus zutreffend; sie bauen aber auch eine Gewöhnung und einen unterschwelligen Zusammenhang zwischen beiden Themen auf, der die Wirkung von Desinformation über Krankheiten verstärken kann. Doch auch insgesamt zeigt der Zusammenhang zwischen Desinformation und Verschwörungstheorien im Kontext von Krankheiten eine komplexe und gefährliche Dynamik, die sowohl die individuelle als auch öffentliche Gesundheit beeinträchtigen kann.

Die AIDS-Verschwörung

Corona-Desinformation und Verschwörungstheorien waren nicht der Anfang, sondern ein Glied in einer Kette. In den 1980er-Jahren war AIDS, damals eine neue, unbekannte und tödliche Krankheit, die schnell um sich griff und sich über die ganze Welt ausbreitete, Gegenstand einer der größten und leider erfolgreichsten Desinformationskampagnen aller Zeiten. Bereits 1983 begann der sowjetische Geheimdienst KGB gezielt die Falschinformation zu verbreiten, AIDS sei ein künstlich im Labor hergestelltes Virus. Als Urheber wurde das Labor der US-Armee Fort Detrick in Maryland genannt. Zeitungsartikel mit diesem Inhalt tauchten zuerst in KGB-nahen Zeitungen in Pakistan und Indien auf, bevor sie ab 1985 erst in der sowjetischen und dann auch in der DDR-Presse, in der Bundesrepublik, Großbritannien und anderen Staaten lanciert wurden. Die Verbreitung von AIDS nahm zu, und 1985 entschied sich Moskau, mit Unterstützung der sozialistischen Geheimdienste, insbesondere durch den in der DDR lebenden Stasi- und KGB-Informanten und Biologie-Professor Jakob Segal, eine großangelegte Desinformationskampagne gegen die USA zu starten.

Dieser konstruierte eine pseudowissenschaftliche Theorie, die den Ursprung von AIDS in ein US-Militärlabor verlegte und behauptete, es sei dort absichtlich an Gefängnisinsassen und Minderheiten getestet worden. Die anerkannte These, dass AIDS von Tieren in Afrika auf den Menschen übertragen wurde, nannte er eine rassistische US-Verschwörung. Obwohl Segals Publikationen in der DDR verboten waren, fanden sie weltweit Verbreitung, unterstützt von der Stasi und dem KGB. Auch im Westen, vor allem unter anti-amerikanischen Kreisen, fand die Theorie Anhänger. Die *taz* veröffentlichte beispielsweise 1987 ein Interview mit Segal, und der WDR strahlte 1989 eine Dokumentation aus, die Segals These unterstützte. Der wahre Schauplatz für diese Desinformationskampagne waren jedoch die Länder in Afrika, Indien und Lateinamerika. Trotz späterer Widerrufungen und Enthüllungen durch ehemalige sowjetische Geheimdienstmitarbeiter bleibt die AIDS-Verschwörungstheorie bis heute in vielen Teilen der Welt virulent und wird von einigen offiziellen Stellen sogar neu belebt. Ähnlich wie bei Corona hat ein breites Netz an überzeugten Desinformanten und unwissenden Helfern die Verbreitung dieser Desinformation befördert und so die Bekämpfung der Krankheit erheblich erschwert.

Künstliche Intelligenz (KI) – eine neue Waffe zur Manipulation?

Seit dem Aufkommen und der massenhaften Verbreitung sogenannter »generativer« (also Inhalte produzierender) KI Ende 2022 diskutieren Forscher, Experten, aber auch Politiker und Journalisten über den Einfluss von KI auf Politik, Medien und digitale Informationsräume sowie über die mögliche Bedeutung von KI für Desinformation. Aufgrund der sich unglaublich schnell entwickelnden Anwendungsmöglichkeiten von KI lässt sich bislang darüber kaum ein abschließendes Urteil fällen. Grundsätzlich festgehalten werden muss jedoch, dass jede neue Informations- und Kommunikationstechnologie, wie z. B. der Buchdruck oder das Internet, auch einen direkten Effekt auf Propaganda und Desinformation hatte. Gerade digitale Technologien machten Desinformation schneller, billiger, einfacher und viel weitreichender (aber nicht immer zwangsläufig auch effektiver). Da KI wiederum Informationen viel leichter, schneller und passgenauer produzieren kann als alle Technologien zuvor, fürchten manche Experten, dass KI eine »Waffe der Massentäuschung« sein könnte.

In der Tat bieten die neuen KI-Tools viele Möglichkeiten für Desinformation und Manipulation. Sogenannte »große Sprachmodelle (LLMs)« und die darauf basierenden Chatbots wie ChatGPT oder Googles »Gemini« können auf Knopfdruck Texte in nahezu jeder Sprache und mit jedem beliebigen Inhalt generieren. Ein grundlegendes Problem von Textgeneratoren ist z. B. ihre Neigung zu sogenannten »Halluzinationen«. Verfügt die KI nicht über eine passende und zutreffende Information, »halluziniert« sie eine herbei, indem sie Wörter aneinanderreiht, die zwar einen sinnvollen Satz ergeben und überzeugend

klingen, aber faktisch falsch sind. Dies hängt mit der grundlegenden Funktionsweise dieser Modelle zusammen, die Texte nicht nach inhaltlichem Sinn erstellen, sondern lediglich auf Basis riesiger Trainingsdaten und Milliarden von Parametern berechnen, welche Wörter aufeinander zu folgen haben. Fordert man so ein Modell auf, einen Zeitungsartikel zu schreiben ohne aber genaue Informationen zu übermitteln, produziert die KI einen sinnvoll klingenden Text ohne Faktenbasis. Dies kann als »Misinformation«, also die unwissentliche und unabsichtliche Verbreitung falscher Informationen, bezeichnet werden. Ein anderes Beispiel war, dass nur kurze Zeit nachdem ChatGPT online ging, Forscher und Journalisten bereits Tausende von falschen Bewertungen und Kommentaren auf Online-Plattformen wie Amazon oder Twitter fanden. Gleichfalls fanden US-Forscher im Sommer 2023 ein Netzwerk von über 1000 Twitter-Profilen, die vollständig und automatisiert durch KI-Sprachmodelle betrieben wurden. Sie gehörten zu einem Betrugsnetzwerk, dass ständig Links postete, die Nutzer zu betrügerischen Finanzgeschäften und Spekulationen bringen sollten. In wieder anderen Fällen fanden Journalisten Hunderte von angeblichen Nachrichtenportalen, deren Artikel sämtlich aus KI-produzierten Inhalten bestanden, die teilweise jahrealte Nachrichtenartikel einfach neu umschrieben. Da sich Texte, die mit solchen KI-Tools erstellt wurden, nur sehr schwer finden und zweifelsfrei nachweisen lassen (siehe unten), lässt sich hier überhaupt nicht abschätzen, wie viel Falschinformation schon heute auf diese Art produziert wird.

Doch KI kann heute nicht nur Texte erstellen, sondern auch audiovisuelle Inhalte, sprich Bilder, Ton- und Videodateien. Auch dies wird bereits aktiv für die Verbreitung von Falschinformation genutzt. Forscher fanden so z. B. Tausende von falschen Social-Media-Profilen, die dadurch auffällig waren, dass ihre Profilbilder zwar echt aussahen, allerdings allesamt KI-generierte Gesichter zeigten. Auf der Kurzfilm-Plattform TikTok entdeckten Journalisten 2024 ganze Netzwerke von Nutzerprofilen, die mit KI-Bildern und KI-generierten Texten

Videos zu Verschwörungstheorien aller Art verbreiteten und sich darüber in anderen Chat-Foren ausführlich absprachen. Dabei ging es offenbar nicht um politische Motive, sondern um das Betreiben von Verschwörungskanälen als lukratives Geschäftsmodell.

Ein anderes Beispiel aus dem politischen Bereich sind Online-Debatten auf Social Media während des Krieges in Gaza nach dem Überfall der Hamas auf Israel. Millionenfach wurden hier KI-generierte Bilder erstellt und verbreitet. Manche davon kamen von professionellen Akteuren aus dem Umfeld der Hamas, die Mehrzahl jedoch von nicht-professionellen pro-palästinensischen Nutzern, die massenhaft falsche Bilder über Explosionen und die leidende Zivilbevölkerung zeigten. Hier ging es nicht so sehr um die Manipulation einzelner Ereignisse oder Personen, sondern um die Beeinflussung und das Einrahmen der Wahrnehmung des Konfliktes an sich. Oftmals waren diese Bilder relativ leicht als KI-Bilder zu erkennen; doch in den emotionalen Debatten, in denen die Bilder ohnehin nicht als direktes Abbild eines einzelnen Ereignisses oder Schicksals dienten, sondern als symbolischer Ausdruck von Emotionen, spielte das kaum eine Rolle.

Vergleichsweise neu sind hingegen KI-generierte Tondateien, die für manipulative Zwecke eingesetzt werden. Seit dem Sommer 2023 verzeichneten zum Beispiel deutsche Polizeibehörden immer mehr Fälle von Trickbetrügereien, bei denen am Telefon mit KI erstellte Stimmen von Angehörigen der Opfer benutzt werden, um Geld zu erpressen. Für politische Manipulationen kam diese Technologie bereits zum Einsatz: Kurz vor dem Wahltag zum slowakischen Parlament 2023 kursierte über Facebook ein angeblicher Telefonmitschnitt eines der Kandidaten. Laut dieser Fälschung besprach der Politiker angeblich mit einer Journalistin, wie am Wahltag möglichst effektiv Stimmen gekauft werden könnten. In einem anderen Fall kam es in den USA 2024 zu Tausenden von automatisierten Anrufen vor einer Vorwahl zu den Präsidentschaftswahlen. Am Telefon war niemand geringeres als die mit KI erstellte Stimme

des amtierenden Präsidenten Joe Biden zu hören, der Wähler aufforderte, nicht zur Wahl zu gehen.

Diese Art der KI-basierten audiovisuellen Manipulationen, »deep fakes« genannt, gelten als eine der gefährlichsten Arten von KI-Manipulation und Desinformation. Dies gilt insbesondere für Videos. Hier lassen sich mit kurzen Originalaufnahmen von Stimmen und Videos in wenigen Minuten komplett neue Inhalte erstellen. Massiv eingesetzt wird dies bereits seit Jahren im Bereich der Pornografie; seit 2023 lässt sich der Einsatz dieser Fakes jedoch auch immer öfter im Bereich der organisierten Kriminalität (im Falle des Trickbetrugs) und der politischen Einflussnahme nachweisen. Betrüger benutzten so zum Beispiel Aufnahmen der ARD-Tagesschau, um die Moderatoren in Fake-Videos für betrügerische Anlageverfahren werben zu lassen. Zuletzt stand jedoch der politische Einsatz dieser Art der Fälschungen im Vordergrund. Russland zum Beispiel nutzte solche KI-generierten »deep fakes«, um falsche Videos des ukrainischen Präsidenten Selenski zu erstellen, in denen er seine Truppen zur Kapitulation aufrief oder Drohnen in der Türkei abbestellte. Andere zeigten Hollywood-Filmstars mit Ukraine-kritischen Botschaften. In vielen anderen Fällen weltweit tun Politiker in »deep fakes« Dinge, die sie nie getan haben. In Afrika zum Beispiel gab es ein »deep fake«, in dem der amtierende Präsident Simbabwes ankündigte, nicht wieder zur Wahl anzutreten; in Bulgarien warb der Premierminister in einem solchen Fake-Video für ein krudes Investmentgeschäft und in Argentinien benutzten 2023 beide Präsidentschaftskandidaten im Wahlkampf sowohl automatisierte KI-Bots und KI-erstellte Wahlkampfplakate als auch Deep-Fake-Videos, in denen zum Beispiel einer der Kandidaten organisierten Organhandel unterstützte.

Eine grundsätzliche Herausforderung von KI-Fakes ist, dass sie nicht ohne Weiteres als solche zu erkennen sind. Zwar existieren einige Software-Programme als vermeintliche »KI-Detektoren«, doch diese produzieren zu viele Falschmeldungen, erkennen also Inhalte fälschlich als KI-generiert oder erkennen

umgekehrt KI-generierte Inhalte nicht. Dies gilt insbesondere für KI-Texte. Bei Bildern und Videos gibt es zwar leistungsfähigere Programme, allerdings bieten auch sie keine wirkliche Sicherheit. Nichtsdestoweniger sind KI-Bilder und Videos derzeit noch um einiges leichter zu erkennen, da sie oftmals optische oder akustische Fehler beinhalten. Diese werden jedoch in naher Zukunft verschwinden (wobei gleichfalls mit Hochdruck an Erkennungsprogrammen gearbeitet wird).

Gerade im globalen »Super-Wahljahr 2024«, in dem in über 50 Ländern rund zwei Milliarden Menschen, darunter in den größten Demokratien, wählen, wurde KI-basierte Falschinformation als eine der größten globalen Gefahren bezeichnet. Eine abschließende Bewertung dessen, was KI für Manipulation und Falschinformation bedeutet und wie sich die Realität tatsächlich entwickeln wird, fällt jedoch nach wie vor schwer. Die schlimmsten Befürchtungen und Untergangsszenarien traten bislang nicht ein. Viele theoretische Möglichkeiten und Potentiale von KI-Technologie im Bereich der Manipulation waren bislang noch nicht in der Praxis zu beobachten gewesen oder zeigten nicht die erwartete desaströse Wirkung. Gleichzeitig treten täglich mehr und mehr Fälle von KI-Manipulation auf, die systematisch an Bedeutung gewinnt. Ebenso sind die mittel- und langfristigen Folgen aufgrund der rasanten Entwicklung immer noch nicht absehbar. KI-Technologie ermöglicht Falschinformationen immer schneller und mit immer besserer Qualität zu erstellen und zu verbreiten. Bislang unklar ist, ob diese Art der Desinformation auch zwangsläufig »erfolgreicher« und überzeugender ist. Gleichfalls sind die Langzeiteffekte der Beschleunigung und Überflutung mit KI-generierten Inhalten und Falschinformationen noch überhaupt nicht absehbar. KI wird also ab sofort mit Sicherheit eine immer wichtigere Rolle in der Welt der Desinformation spielen (offen bleibt, worin und wie entscheidend diese Rolle ist).

Gleichzeitig ist es nicht so, dass Politik, Gesellschaft, Medien, Social Media und KI-Hersteller dem Problem vollkommen hilflos gegenüberstehen würden. An einigen technischen

Lösungen wie die Kennzeichnung von KI-erstellten Inhalten und digitalen Wasserzeichen wird bereits gearbeitet. Vorschriften wie zum Beispiel jene des EU-KI-Gesetzes machen solche Kennzeichnungen und die Nachvollziehbarkeit, ob Inhalte mit KI-erstellt wurden, gleichfalls in der Europäischen Union verpflichtend. Darüber hinaus werden Bildungsmaßnahmen, also Aufklärung über und Sensibilisierung für KI-Fakes, und der Aufbau von Widerstandskräften gegen solche Manipulationen durch Trainings, Schulungen und Kurse als besonders hilfreich erachtet. Im Zuge der US-Wahlen 2024 erließen auch alle großen westlichen Social-Media-Plattformen neue Regeln in Bezug auf KI-Inhalte (auch wenn diese, wie schon bei anderen Falschinformationen, in der Praxis selten massenhaft bzw. streng angewendet werden). Darüber hinaus bieten dieselben KI-Technologien auch große Möglichkeiten im Bereich der automatisierten Erkennung, Kennzeichnung und Moderation von KI-Fakes auf Social-Media-Plattformen.

Was tun gegen Desinformation? Gegenmaßnahmen

Desinformation ist ein komplexes System, bei dem viele unterschiedliche Faktoren ineinandergreifen und viele Akteure mit großen Ressourcen agieren; trotzdem sind Staaten, Gesellschaften und der einzelne Bürger nicht hilf- und wehrlos. Wissenschaft, Experten und mit dem Thema befasste staatliche Institutionen haben eine große Bandbreite an Gegen- und Abwehrmaßnahmen erarbeitet. Das Problem ist oftmals nicht, dass es keine Möglichkeiten oder Ideen für solche Abwehrmaßnahmen gibt, sondern dass sie entweder nicht oder nicht ausreichend geplant, koordiniert und umgesetzt werden (können).

Ähnlich wie in Kapitel 1 mit Blick auf die Urheber und Akteure, Medien, Formen und Zielgruppen beschrieben wurde, können auch die Abwehrmaßnahmen gegen Desinformation an diesen Punkten ansetzen. Das heißt, es gibt Abwehrmaßnahmen, die nur von bestimmten Stellen, z. B. staatlichen Behörden, durchgeführt werden können. Andere wiederum können von Medien und Journalisten, Social-Media-Plattformen oder von deren Nutzern umgesetzt werden. Manche Maßnahmen setzen bei den Zielgruppen von Desinformation (siehe Kapitel 1) an, manche bei den Urhebern hinter Desinformation, manche bei den benutzten Medien und manche bei den unterschiedlichen Formen von Desinformation.

Die Liste an Einzelmaßnahmen gegen Desinformation, die Forscher, Experten und Politiker in den letzten Jahren vorgeschlagen haben, umfasst mehr als 20 Punkte. Manche davon sind hochgradig spezialisiert, manche hingegen allgemein. Grundsätzlich kann unterschieden werden zwischen

»positiven« und »negativen« Abwehrmaßnahmen, also solchen, die versuchen, bestehende Desinformation zu widerlegen, zu löschen und zu bekämpfen, und solchen, die entweder die Wirkung von Desinformation beim Publikum verringern oder Desinformation durch andere, bessere Informationsangebote wirkungslos machen sollen.

Darüber hinaus gibt es rechtliche Maßnahmen, also Regelungen und Gesetze, die die Verbreitung und Veröffentlichung von Desinformation verbieten bzw. verhindern sollen. Ein Ansatz ist dabei, die Betreiber von großen Social-Media-Plattformen dazu zu zwingen, entsprechende Beiträge umgehend zu löschen, zu kennzeichnen oder ihre automatische Vervielfältigung zu verhindern. Beispiele dafür sind das »Gesetz über Digitale Dienste« (DSA) der EU, das Plattformbetreiber genau dazu zwingen will. Andere, eher negative Beispiele, sind Anti-Desinformationsgesetze in Staaten wie der Türkei oder Russland, die zumeist dazu genutzt werden, den autoritären Anspruch des Staates durchzusetzen.

Sicherheitspolitische Maßnahmen beziehen sich auf die Rechtsdurchsetzung von Sicherheits-, Strafverfolgungs- und Justizbehörden gegen Urheber und Verbreiter von Desinformation. Ausländische Propaganda und Einflussversuche aufzudecken, die Akteure bzw. ihre Mittelsmänner und Stellvertreter zu finden und ihre Arbeit zu stoppen, war traditionell eine Domäne von Geheimdiensten und Polizeibehörden (insbesondere, weil diese Art der Desinformation häufig von ausländischen Geheimdiensten durchgeführt wurde). Die Maßnahmen umfassen dabei ein regelmäßiges Monitoring von Desinformation, die Untersuchung ihrer Ursprünge, Ziele, Finanzströme und Hintermänner, die Aufdeckung von Fälschungen und gegebenenfalls die Ergreifung von Sicherheitsmaßnahmen wie Verhaftungen oder das Schließen von Medienkanälen.

Institutionelle Maßnahmen beziehen sich auf die Einrichtung zentraler (zumeist staatlicher) Stellen für die Organisation, Koordination und Durchführung von Maßnahmen gegen Desinformation. Viele Staaten und auch die EU haben dazu in

den letzten Jahren eigene, nachgeordnete staatliche Behörden, Einheiten oder Expertengruppen gebildet. Diese übernehmen Aufgaben wie das Überwachen und Analysieren ausländischer Desinformation, berichten an Entscheidungsträger oder entwerfen Gegenmaßnahmen und setzen diese um. Die Stärken dieser Institutionen liegen in der Verfügbarkeit staatlicher Ressourcen, Autorität, Netzwerke und Zugang zu speziellem Wissen sowie Technologie.

Technologische Maßnahmen: Da der Großteil moderner Desinformation im digitalen Raum stattfindet, spielen digitale Technologien eine Schlüsselrolle bei ihrer Bekämpfung. Dazu gehören automatisierte Softwarelösungen für die Erkennung und Kennzeichnung von fragwürdigem Inhalt und Konten, das Entfernen solcher Inhalte und das Verändern von Inhaltsvorschlagsalgorithmen. Viele dieser Lösungen basieren auf künstlicher Intelligenz, jedoch treten hier Herausforderungen wie unzureichende Genauigkeit und mangelnde Ressourcen großer Plattformen auf.

Wirtschaftliche Maßnahmen zielen darauf ab, in das Wirtschaftssystem hinter Desinformation und die damit verbundenen Geschäftsmodelle einzugreifen. Dazu gehören die Regulierung von Werbung in Verbindung mit Desinformation und Sanktionen gegen Einzelpersonen oder Organisationen, die Desinformation finanzieren und ermöglichen. Zivilgesellschaftliche Organisationen veröffentlichten zuletzt vermehrt Namen von Unternehmen, die neben oder auf Desinformationsseiten oder Accounts werben, um öffentlich auf das Problem aufmerksam zu machen und um Druck auszuüben.

Kommunikationsmaßnahmen: Da Desinformation auf Kommunikation beruht, gibt es viele Ansätze, die ebenfalls verschiedene Arten von Kommunikation nutzen, um Desinformation zu bekämpfen. Dazu gehört zum Beispiel die Förderung von guter politischer Kommunikation und von Qualitätsjournalismus. Dies kann das Vertrauen der Öffentlichkeit stärken und den Spielraum für Desinformation verringern. Unterstützung von Qualitätsjournalismus, Faktenprüfung und vorbeugende

Maßnahmen sind wesentliche Werkzeuge im Kampf gegen Desinformation.

Dasselbe gilt für Bildungsmaßnahmen. Bildung ist eine wichtige Ressource im Kampf gegen Desinformation. Einerseits gilt gute Allgemein- und Breitenbildung als Basis, um breite Bevölkerungsschichten widerstandsfähig gegen manipulative Einflussversuche und Desinformation zu machen; andererseits ist spezialisierte Bildung, zum Beispiel im Bereich der Medienkompetenz, nützlich, um die Anfälligkeit von Social-Media-Nutzern für Desinformation zu verringern. Vorbeugende Aufklärung über die Ziele, Wirkung und Vorgehensweise von Desinformation haben sich hier ebenfalls als effektiv erwiesen, um das Publikum gegen Desinformation zu »immunisieren«.

Im Einzelnen gibt es folgende Maßnahmen:

1. Sicherheitspolitik (Untersuchung, Aufdeckung, Schließung, Löschung, Strafverfolgung)
2. Sanktionen gegen Individuen und Desinformationsmedien
3. Verbote von Desinformation oder bestimmten Medien
4. Social-Media- und Plattform-Regulierung
5. Regulierung von Algorithmen bei Inhaltsauswahl und Vorschlägen
6. Regulierung von Werbung auf/neben Desinformationskanälen
7. Anti-Desinformationsbehörden oder Einrichtungen
8. Monitoring und Analysis von Desinformation
9. Debunking, also das zeitnahe Überprüfen, Widerlegen und Zurückweisen durch offizielle Stellen
10. Fact-Checking, also das zeitnahe Überprüfen, Widerlegen und Zurückweisen durch Medien, Journalisten etc.
11. Automatisierte Erkennung, Kennzeichnung, Löschung oder Nebeneinanderstellung von Desinformation durch Software
12. Einführung digitaler Wasserzeichen zur Überprüfung des Ursprungs einer Information

13. Strategische Kommunikation
14. Prebunking, also präventive Aufklärung und Bildung über Desinformation, z. B. durch »Inoculation« (»Informationsimpfung«)
15. Vertrauensbildende Maßnahmen von Medien, Journalismus und politischer Kommunikation
16. Medienbildung
17. Allgemeinbildung
18. (Unterstützung für) Qualitätsjournalismus
19. (Gesellschaftliche und individual-psychologische) Resilienzbildung
20. Reichweitenverringerung von Desinformation, z. B. durch Netzwerke (»Elfen«), die Desinformation gezielt suchen, melden und positive Gegeninformationen vorschlagen

Diese Fülle verschiedener Maßnahmen zeigt auch, dass Maßnahmen gegen Desinformation nicht von einer Stelle allein durchgeführt werden können. Stattdessen müssen sowohl Regierungen und Behörden, zivilgesellschaftliche Akteure, Medien und Journalisten sowie Social-Media-Plattformen und andere Unternehmen alle gleichzeitig tätig werden. Dies verdeutlicht auch, dass Gegenmaßnahmen gegen Desinformation komplexe Prozesse sind, die strategisch geplant und koordiniert werden müssen.

Literatur

Jessikka Aro: Putins Armee der Trolle. Der Informationskrieg des Kreml gegen die demokratische Welt. Goldmann, München 2022.

Lukas Bernhard, Leonie Schulz, Cathleen Berger, Kai Unzicker: Verunsicherte Öffentlichkeit.

Superwahljahr 2024: Sorgen in Deutschland und den USA wegen Desinformation, Gütersloh, 2024 (https://www.bertelsmann-stiftung.de/de/publikationen/publikation/did/verunsicherte-oeffentlichkeit).

Arista Beseler, Alexandra Heidsiek: Interview: Deutsche Alternativmedien und russische Propaganda, in: Dekoder, 2024 (https://www.dekoder.org/de/article/deutsche-alternativmedien-russische-propaganda).

European Commission: Code of Practice on Disinformation', 2018 (https://ec.europa.eu/digital-single-market/en/news/code-practice-disinformation).

Strategic Communications, Task Forces and Information Analysis (STRAT.2) (hg.): 1st EEAS Report on Foreign Information Manipulation and Interference Threats Towards a framework for networked defence, Brüssel, 2023 (https://www.eeas.europa.eu/eeas/1st-eeas-report-foreign-information-manipulation-and-interference-threats_en).

DFRLab (hg.): Doppelganger targets Ukrainian and French audiences via Facebook ads, 2024 (https://dfrlab.org/2024/03/12/doppelganger-operation-targets-ukraine/).

DFRLab (hg.): Two-pronged approach to Africa pays dividends for Russia, 2024 (https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/two-pronged-approach-to-africa-pays-dividends-for-russia/).

Typen von Desinformation und Misinformation. Verschiedene Formen von Desinformation und ihre Verbreitung aus kommunikationswissenschaftlicher und rechtswissenschaftlicher Perspektive. Ein Gutachten im Auftrag der Gremienvorsitzendenkonferenz der Landesmedienanstalten (GVK), Berlin, 2020.

Hybrid CoE (hg.): Strategic Analysis 23: One China under media heaven: How Beijing hones its skills in information operations, Helsinki, 2020.

Matthias Koring / Fabian Zimmermann: Fake News als aktuelle Desinformation (https://www.bpb.de/themen/medien-journalismus/digitale-desinformation/290561/fake-news-als-aktuelle-desinformation/), 2019.

Paula Matlach & Sara Bundtzen: Fruchtbarer Nährboden für extreme Rechte und Verschwörungsideologien? Die Bauernproteste in Deutschland, hg.: ISD Germany, 2024 (https://isdgermany.org/die-bauernproteste-in-deutschland/).

Christopher Nehring / Douglas Selvage: Die AIDS-Verschwörung. Das Ministerium für Staatssicherheit und die AIDS-Desinformationskampagne des KGB, Berlin, 2014.

Thomas Rid: Active Measures. The Secret History of Disinformation and Political Warfare, New York, 2020.

Shultz, R. & Godson, R.: Dezinformatsia: Active Measures in Soviet Strategy, Washington D. C., 1984.

Hybrid CoE (hg.): Research Report 7: Foreign information manipulation and interference defence standards: Test for rapid adoption of the common language and framework ›DISARM‹, Helsinki, 2022.

Bastian Schlange: Das einzig wahre Faktencheckbuch, Berlin, 2023.

Matthias Schulze: Desinformation: Vom Kalten Krieg zum Informationszeitalter, in: bpb.de, 2019 (https://www.bpb.de/themen/medien-journalismus/digitale-desinformation/290487/desinformation-vom-kalten-krieg-zum-informationszeitalter/).