Journalistik. Zeitschrift für Journalismusforschung
HERBERT VON HALEM VERLAG
Heft 3/2022, S. 248-268
5. Jahrgang
ISSN 2569-152X
DOI: 10.1453/2569-152X-32022-11505-de

Aufsatz

Sahar Khamis und Khalid Al-Jaber

Digitale Gegenrevolution, Desinformation und journalistische Einschränkungen in den arabischen Medien

Abstract: **Die Verbreitung von Social-Media-Plattformen läutete eine noch nie dagewesene Ära der Kommunikation ein: Sie ist grenzenlos, unmittelbar und weitreichend, sie trotzt Beschränkungen und Zensur. Die digitale Technologie hat die Verbreitung von Demokratie und Meinungsfreiheit gefördert und 2011 zum Sturz einiger arabischer Regime beigetragen. Damals glaubte man, dass diese Plattformen den Weg zur Demokratie ebnen würden, weil die Bevölkerung damit staatliche Zensur umgehen und Aktivist:innen sich besser austauschen, vernetzen und organisieren konnten, was autoritäre Regime schwächte. Diese Annahmen waren zu optimistisch, wie Rückschläge bei der Demokratisierung und politischen Reformen in der arabischen Region mehr als ein Jahrzehnt später deutlich machen. Dieser Beitrag zeigt auf, wie autoritäre Regime neue Medien und entsprechende Gesetze und Vorschriften ausnutzen, um gegen Oppositionelle, Aktivist:innen und Journalist:innen vorzugehen, oft unter dem Deckmantel der Desinformationsbekämpfung und unter Einsatz einer Vielzahl von Techniken. Er veranschaulicht auch, wie staatlich orchestrierte Kampagnen mittels neuer Kommunikationsmittel Desinformation rasant verbreiten können, was schwerwiegende politische Folgen und hohe Risiken für Aktivist:innen und Journalist:innen birgt und zugleich Gegenrevolutionen befördert. Wir erkunden, wie diese komplexen Phänomene den arabischen Journalismus beeinträchtigen, insbesondere seit der COVID-19-Pandemie.**

1. Fake News: Ein neuer Begriff für ein altes Phänomen

Heutzutage ist »Fake News« ein gängiger Begriff für falsche oder irreführende Informationen, die auf Kosten der Wahrheit politischen oder wirtschaftlichen Interessen dienen. Dass Regierungen auf Propaganda und Fake News zurückgreifen, um ihre Gegner zu untergraben, zu stigmatisieren oder auszugrenzen, ist jedoch keineswegs ein neues Phänomen. Machthabende nutzen schon seit jeher Fehlinformationen und Desinformationen, um die öffentliche Meinung im Sinne ihrer eigenen Vorstellungen und Absichten zu beeinflussen. Ziel war dabei immer, Wahrnehmungen zu verändern, Ansichten zu verzerren, Meinungen zu beeinflussen und Emotionen zu manipulieren, um zu ernsten und wichtigen Themen Zweifel zu säen, Verwirrung zu stiften und die Bevölkerung einer Gehirnwäsche zu unterziehen.

Der amerikanische Historiker Robert Darnton von der Harvard University weist uns darauf hin, dass »das Zusammenreimen alternativer Fakten wohl kaum eine Seltenheit ist. Die Entsprechungen zu den giftigen, mundgerechten Texten und Tweets heutzutage finden sich in den meisten Epochen der Geschichte bis zurück in die Antike« (DRANTON 2017). Er verweist auf ein uraltes Beispiel aus byzantinischer Zeit, die Anekdoten des byzantinischen Historikers Procopius aus dem 6. Jahrhundert, die als früheste Beispiele medialer Desinformation gelten. Diese geheimen Proto-Blogs waren eine Schmierkampagne voll »zweifelhafter Informationen« gegen einen Herrscher und seine Skandale (DRANTON 2017).

Auch Olivier Thibaut erinnert uns daran, dass Donald Trump zwar den Ausruf »FAKE NEWS!« (in Großbuchstaben und mit Ausrufezeichen) in Hunderten von Tweets popularisierte, das Konzept allerdings schon seit Jahrhunderten existiert« (THIBAUT 2018). Er zitiert einen Hinweis von François Bernard Huyghe, Research Fellow am Institut for International and Strategic Affairs, dass mediale Desinformation im Kalten Krieg durch die »bewusste Verbreitung von Falschinformationen geprägt war, um die Meinung zu beeinflussen und den jeweiligen Feind zu schwächen«, insbesondere im westlichen Lager (THIBAUT 2018). Eines der bemerkenswertesten Beispiele war eine Propagandakampagne des sowjetischen Geheimdienstes, die 1983 mit der Veröffentlichung eines Artikels in einer indischen Zeitung begann. Darin wurde behauptet, HIV sei eine in US-Militärlabors entwickelte biologische Waffe (GRIMES 2017). Ein aktuelleres Beispiel für diese Desinformationsschlachten, diesmal aus dem Westen, ist die Behauptung, das COVID-19-Virus sei möglicherweise absichtlich in einem chinesischen Labor in Wuhan erzeugt worden und später daraus ausgetreten (RUWITCH 2021).

Ein berüchtigtes Beispiel für politisierte und irreführende Informationen in der arabischen Welt war die Berichterstattung des Radiosenders *Sawt Al Arab* [Die Stimme der Araber] über den Krieg im Juni 1967. Der ägyptische Radiomoderator

Ahmed Saeed erhielt von der ägyptischen Regierung den Auftrag, im Krieg mit Israel einen Sieg der ägyptischen Streitkräfte zu prognostizieren, was sich später als falsch herausstellte. Während er fälschlicherweise den Abschuss Dutzender israelischer Flugzeuge und die Zerstörung Hunderter israelischer Panzer meldete, endete der Krieg mit der Besetzung weiterer palästinensischer Gebiete, der Sinai-Halbinsel in Ägypten und der Golanhöhen in Syrien durch Israel (BOWEN 2017). Nach dieser militärischen Niederlage warf Ahmed Saeed das Handtuch. Vor seinem Tod gestand er, dass der Inhalt seiner Sendung von hohen Staatsbeamten diktiert wurde.

Heute besteht das Problem von Fehlinformationen und Desinformationen weiter, wenn auch in anderer Form. Dank der Kommunikationsrevolution und neuer digitaler Technologien verbreiten sie sich viel schneller und mit größerer Wirkung. In einigen Fällen beschädigt dies die Authentizität, Glaubwürdigkeit und Seriosität journalistischer Berichterstattung, da einige Medien anstelle seriöser Berichterstattung nach professionellen journalistischen Standards dem Druck der Regierung nachgeben und irreführende Propaganda, Fehlinformationen und Desinformationen verbreiten, um die Agenda des Regimes zu unterstützen (KHAMIS/EL-IBIARY 2022).

2. Soziale Medien und globale Desinformation

Sozialen Medien, insbesondere Facebook und Twitter, wird von verschiedenen Seiten mehr denn je vorgeworfen, sie würden zu Plattformen für die Verbreitung von Fehlinformationen und Desinformationen. Sie trügen zur Untergrabung der Demokratie auf der ganzen Welt bei, indem sie die politische Agenden unterstützen und Politiker:innen helfen, soziale Spaltungen zu vertiefen sowie Minderheiten und politische Rivalen zu verleumden. Dies erhöht die Gefahr, dass sich soziale Medien von nützlichen Informationsinstrumenten für die Öffentlichkeit zu gefährlichen Instrumenten sozialer Kontrolle entwickeln, manipuliert von Politiker:innen sowohl in demokratischen als auch in autoritären Regimen, wobei das Risiko unter autoritären Regierungen immer größer ist (BANJO 2019).

Die Präsidentschaftswahlen in den Vereinigten Staaten im Jahr 2016 und in Brasilien im Jahr 2018 haben gezeigt, dass soziale Medien ideale Werkzeuge für die Verbreitung von Gerüchten und Desinformationen sein können, was Polarisierung und Fragmentierung gefährlich verstärkt. Nachdem Facebook bestätigt hatte, dass russische Organisationen während der US-Präsidentschaftswahlen 2016 über sein Netzwerk Wahlwerbung für Donald Trump finanziert hatten (CNN 2019), bestätigte auch Twitter, Opfer ähnlicher Kampagnen geworden zu sein. Beide Plattformen bekräftigen jedoch weiterhin ihre demokratische Grundhaltung.

Beide Plattformen beugten sich dem Druck und erklärten ihre Kooperationsbereitschaft mit dem US-Kongress bei der Untersuchung einer möglichen russischen Einmischung in die Wahl von Donald Trump. Obwohl der Kreml solche Anschuldigungen wiederholt bestritt, gab Facebook zu, von undurchsichtigen russischen Unternehmen und Institutionen getäuscht worden zu sein, die Tausende von Werbeanzeigen auf ihren Seiten veröffentlichten und sich so in die US-Präsidentschaftswahlen von 2016 einmischten, die der Republikanische Kandidat Donald Trump schließlich gewann (SHANE/GOEL 2017). Später tat Twitter das Gleiche (SWAINE 2018).

Als die amerikanische Öffentlichkeit zum ersten Mal von der Einmischung Russlands in die Präsidentschaftswahlen 2016 erfuhr, taten es viele als unglaubwürdig und unrealistisch ab. Im Laufe der Zeit erkannten jedoch immer mehr, insbesondere demokratisch, liberal oder unabhängig gesinnte Amerikaner:innen die unbequeme Wahrheit über die Rolle von Social-Media-Plattformen bei der Beeinflussung des Wahlergebnisses 2016 (SHANE/GOEL 2017; SWAINE 2018).

Laut einer Studie der Universität Oxford in 28 Ländern beschäftigen viele autoritäre Regierungen, darunter die meisten arabischen Länder, einen großen Stab technologisch versierter Mitarbeiter:innen. Diese erstellen Inhalte zur Beeinflussung der öffentlichen Meinung ihrer Bevölkerung im In- und Ausland sowie der internationalen öffentlichen Wahrnehmung dieser Länder. Die Studie kam zu dem Schluss, dass »jedes autoritäre Regime Social-Media-Kampagnen gegen die eigene Bevölkerung führt« (BRADSHAW/HOWARD 2017). Die Studie ergab, dass sich gefälschte Nachrichten, die oft ansprechender sind als verifizierte Fakten, schneller über das Internet verbreiten. Das liegt an der Geschwindigkeit, mit der sich große Mengen von Inhalten unabhängig von deren Wahrheitsgehalt online verbreiten (BRADSHAW/HOWARD 2017).

Ein weiterer Bericht von Freedom House (2017) stellte fest, dass Wahlen in 18 Ländern durch Fehl- und Desinformationen aus Online-Kampagnen kompromittiert wurden. Der Bericht zeigte auf, was Regierungen tun, um die Online-Rhetorik und öffentliche Meinung sowohl im In- als auch im Ausland zu beeinflussen. Der Bericht, der die Freiheit der Internetnutzung in 65 Ländern untersuchte und etwa 87 Prozent der weltweiten Internetnutzer:innen erfasste, erörterte außerdem, wie 30 Regierungen über soziale Medien abweichende Meinungen unterdrücken. Weltweit sind die Freiheitsindikatoren im siebten Jahr in Folge gesunken, da Regierungen verstärkte Anstrengungen unternehmen, um Online-Diskussionen, -Handlungen und -Interaktionen von Internetnutzer:innen zu beeinflussen (FREEDOM HOUSE 2017).

Angesichts dieser ansteigenden Welle medialer Desinformation intensivieren große Medienunternehmen, häufig in Kooperation mit Hightech-Unternehmen und Social-Media-Plattformen, ihre Überwachungsaktivitäten, Faktenchecks und sonstige investigative Arbeit, um faktenbasierten Journalismus

zu unterstützen. Solche Bemühungen stoßen allerdings angesichts des überwältigenden Einflusses und der weitreichenden Auswirkungen sozialer Medien sowie ihrer Ausnutzung durch staatliche und andere Akteure an ihre Grenzen.

3. Soziale Medien und Gegenrevolution: Von Befreiung zu Unterdrückung

Die Aufstände des Arabischen Frühlings 2011 stifteten große Hoffnungen auf politische Reformen und eine reibungslose Demokratisierung (LYNCH 2012; 2016), verbunden mit ebenso großen Erwartungen an das demokratisierende Potenzial der neuen Medien, von denen man glaubte, sie könnten den Weg für revolutionäre Übergänge ebnen, der freien Meinungsäußerung größeren Spielraum verschaffen und als Katalysatoren und Verstärker für politischen Wandel wirken (EL TANTAWY/WIEST 2011).

Die autoritären Regierungen in den meisten arabischen Ländern waren damals nicht gewappnet für diese neue Welle der freien Meinungsäußerung, die Social-Media-Plattformen ermöglichten, ebenso wenig wie für die verschiedenen Organisations- und Vernetzungsmöglichkeiten, die sie Aktivist:innen boten. Viele dieser Regierungen hatten jahrzehntelang durch eine Fülle direkter und indirekter Techniken und Mechanismen in die Kontrolle und Manipulation der Mainstream-Medien investiert (SAKR 2013; SEIB 2007). In Sachen technologischer Entwicklung hinkten sie den jungen Aktivist:innen in der arabischen Region hinterher.

Mehr als ein Jahrzehnt nach diesen Aufständen erleben wir in der arabischen Region jedoch eine völlig andere Realität, nämlich Hürden und Rückschläge in den Ländern des sogenannten Arabischen Frühlings. Diese reichen von religiös motivierten Unruhen und Staatenlosigkeit in Libyen und einem brutalen Bürgerkrieg in Syrien bis hin zu einem niedergeschlagenen Aufstand in Bahrain, einer Rückkehr zur Militärdiktatur in Ägypten und einem verheerenden Krieg im Jemen. Selbst das Land, das als einzige Erfolgsgeschichte galt, nämlich Tunesien, musste in letzter Zeit Rückschläge in seinem Demokratisierungsprozess hinnehmen.

Diese unerwünschten Ereignisse veranlassten Regierungen in den Ländern des Arabischen Frühlings sowie auch außerhalb davon, dieser neuen Welle des »Cyber-Aktivismus« (HOWARD 2011) dezidiert entgegenzutreten, ihre digitalen Kapazitäten auszubauen, mediale Narrative zu kontrollieren und abweichende Meinungen zu unterdrücken, wenn auch mit unterschiedlichen Techniken und aus unterschiedlichen Gründen. Die Regierungen der Länder des Arabischen Frühlings sahen sich angesichts dieser unerwünschten Entwicklungen gezwungen, mediale Narrative zu kontrollieren, um neue Wellen öffentlichen Widerspruchs und weitere Aufstände zu verhindern. In Ländern, die nicht vom

Arabischen Frühling erfasst worden waren, setzen die Regierungen ähnliche Praktiken ein, um Aufstände von vornherein zu verhindern und ähnliche Entwicklungen im eigenen Land zu vermeiden.

Dazu gehörte die Schaffung »elektronischer Armeen« mit automatisierten Konten, die von autoritären Regimen als eine Art Internet-Bereitschaftspolizei eingesetzt werden. Ein gutes Beispiel dafür ist die »Syrian Electronic Army«, mit der das syrische Regime seine Gegner:innen online effektiv aufspürt, sie trollt, hackt, sabotiert und ihre digitalen Aktivitäten blockiert. Interessanterweise wurde diese Armee aus Online-Hackern von Syriens Diktator Bashar Al Assad für ihren Patriotismus gelobt (KHAMIS/GOLD/VAUGHN 2013).

Diese digitale Repression signalisiert einen Übergang von der optimistischen oder sogar utopischen Phase der »Tech-Euphorie« zu einer neuen Phase der harten Realität des »digitalen Autoritarismus«, der in den letzten Jahren in der arabischen Welt stetig zugenommen hat (JONES 2022; KHAMIS 2020a).

In dieser neuen Phase des »digitalen Autoritarismus« nach dem Arabischen Frühling entpuppten sich Tausende von Konten auf Twitter und Facebook als staatliche Propagandasprachrohre. Einige gehören Influencer:innen, die entweder freiwillig oder unter Zwang Propaganda für ihre autoritäre Regierung betreiben. Andere Konten waren zuvor unbekannt, gewannen aber in Rekordzeit Tausende von Followern und erhielten das Twitter-Verifizierungszeichen. Für jeden dieser Influencer:innen gibt es Hunderte kleinerer Konten, die von verschiedenen Gruppen verwaltet zu werden scheinen, die Infanterie einer gut koordinierten Online-Armee.

2019 gaben große Technologieunternehmen zu, gegen gefälschte Konten vorzugehen, die Regimekritiker:innen und regionale Rivalen zum Schweigen bringen sollen. Im August 2019 gab Facebook zu, eine orchestrierte Online-Kampagne zerschlagen zu haben, die mit der saudi-arabischen Regierung in Verbindung gebracht wurde. Insgesamt suspendierte Facebook etwa 350 Konten, die mehr als 100.000 Dollar ausgegeben hatten, um über 1,4 Millionen einzelne Follower über Werbeanzeigen zu erreichen. Während die saudi-arabische Regierung offiziell jegliche Beteiligung an der Operation bestritt, erklärte ein Vertreter von Facebook: »Wie unsere Ermittler:innen bestätigen konnten, stehen die Drahtzieher dieser Operation mit der saudi-arabischen Regierung in Verbindung … Jedes Mal, wenn wir eine Verbindung zwischen einer Informationsoperation und einer Regierung feststellen, ist das von Bedeutung und die Öffentlichkeit sollte davon erfahren.« (STUBBS 2019)

In einem separaten Vorfall, der sich etwa zur gleichen Zeit ereignete, gab Facebook zu, 350 Fake-Konten gesperrt zu haben, die mit den Regierungen Ägyptens und der Vereinigten Arabischen Emirate in Verbindung standen, wobei Facebook aber nicht so weit ging, diese Regierungen als die Drahtzieher hinter den Konten und ihren Aktivitäten zu beschuldigen. Die Konten richteten sich vor allem

gegen den regionalen Rivalen Katar während der damaligen Golfblockade und verbreiteten auch Fehl- und Desinformationen zu verschiedenen anderen Themen (STUBBS 2019).

Twitter meldete außerdem die Löschung von 5.929 Konten mit Verbindungen zu einem saudischen Unternehmen, von dem angenommen wird, dass es kritische Stimmen online verfolgt (STONE 2019). Twitter stellte später klar, dass es sich dabei nur um eine Stichprobe der 88.000 Konten handelte, die es als potenzielle saudische Propagandainstrumente gekennzeichnet hatte (MILLER 2019).

Laut Human Rights Watch verfolgen die wirtschaftlich wohlhabenden und technologisch versierten Regierungen der Länder des Golf-Kooperationsrats (GCC) die Online-Aktivitäten einiger ihrer Bürger:innen mit Überwachungstechnologien, die sie von »westlichen und israelischen Unternehmen« erworben haben (HUMAN RIGHTS WATCH 2016). Basierend auf Beweisen der Forschungsgruppe Citizen Lab in Toronto stellte der Bericht fest, dass diese Regierungen ein von der berüchtigten israelischen Spyware-Firma NSO entwickeltes »Spionageprogramm« einsetzten, mit dem sich »auf E-Mails, Textnachrichten, Anruflisten, Kontaktlisten, Dateien und möglicherweise Passwörter« zugreifen lässt. »Damit können Behörden Kameras und Mikrofone von Handys oder Laptops einschalten und ohne das Wissen des Besitzers Bilder machen oder Videos und Gespräche aufnehmen« (HUMAN RIGHTS WATCH 2016). Die Gefahr dabei ist, dass »diese Unternehmen Techniken anwenden können, die dem Niveau der US-Geheimdienste gleichwertig oder sogar überlegen sind«, so Sasha Romanosky, Politikwissenschaftler bei der RAND Corporation (ROMANOSKY 2017). Nach Angaben des Citizen Lab wurden seit 2016 etwa 175 Personen Ziel von NSO-Spionageprogrammen, darunter Menschenrechtsaktivist:innen und Dissident:innen (ZILBER 2018).

Im Jahr 2016 berichtete Citizen Lab, eine Kampagne von Spyware-Angriffen eines technologisch hoch versierten Betreibers gegen emiratische Journalist:innen, Aktivist:innen und Dissident:innen aufgedeckt zu haben (MARCZAK/SCOTT-RAILTON 2016). Der Staat Bahrain steht an der Spitze der Liste der autoritären Länder, die Spionagegeräte vom Staat Israel kaufen und damit die eigene Bevölkerung ausspionieren, wie aus einem von der israelischen Zeitung *Haaretz* veröffentlichten Investigativbericht hervorgeht (SHEZAF/JACOBSON 2018). Ein weiterer Artikel in *Haaretz* enthüllte, dass die israelische Spyware-Gruppe NSO einer saudischen Behörde Pegasus 3 verkauft hat, ein 55 Millionen Dollar teures Programm zum Hacken von Mobiltelefonen, und zwar nur wenige Monate bevor der saudische Kronprinz Mohammed bin Salman (MbS) eine harte Repressionskampagne gegen seine Gegner im eigenen Land startete (HAREL/LEVINSON/KUBOVICH 2018).

Einer der bekanntesten Fälle von Cyber-Überwachung in der Golfregion ist der der jungen saudischen Frauenrechtsaktivistin Loujain Al-Hathloul, die 2018 von der saudischen Regierung inhaftiert wurde. Einigen Berichten zufolge

erfolgte die Verhaftung von Al-Hathloul infolge einer Zusammenarbeit zwischen den saudischen Behörden und dem Projekt DREAD der VAE, einer Cyber-Überwachungseinheit, die mit Hilfe amerikanischer Ex-Geheimdienstler eingerichtet wurde (HASAN 2019).

Citizen Lab suchte im Internet nach Servern, die mit dem israelischen Spionageprogramm Pegasus verbunden waren, und fand Beweise für dessen Einsatz in 45 Ländern weltweit, darunter 17 im Nahen Osten. Der Bericht von Citizen Lab zeigt, dass Pegasus im GCC offenbar sehr intensiv genutzt wird. Insgesamt wurden mindestens sechs Betreiber mit bedeutsamer Aktivität in den GCC-Ländern ermittelt. Davon scheinen sich zwei vornehmlich auf die Vereinigten Arabischen Emirate, einer hauptsächlich auf Bahrain und ein weiterer auf Saudi-Arabien zu konzentrieren (MARCZAK et al. 2018).

Eine hitzige Kontroverse um die Social-Media-Messaging-App ToTok (nicht zu verwechseln mit TikTok), veranschaulicht die israelisch-emiratische Zusammenarbeit zur Verbreitung von Überwachungstechnologien in den VAE. Weitere Beweise deuteten darauf hin, dass die zunächst als kostenlose Video-, Sprach- und Nachrichten-App in den Vereinigten Arabischen Emiraten vermarktete Anwendung von Beginn an die Gespräche der Nutzer:innen des Dienstes ausspionieren sollte. Die App überwachte ständig den Standort und die Kommunikation der arglosen Nutzer:innen und konnte sogar über Mikrofon und Kamera Gespräche mithören (*The Guardian* 2019). Eine genauere Untersuchung ergab, dass die Messaging-App tatsächlich von ehemaligen israelischen Geheimdienstlern entwickelt wurde, die anschließend für das in Abu Dhabi ansässige Cybersicherheitsunternehmen DarkMatter arbeiteten (HAARETZ 2019). In den Tagen nach Bekanntwerden der Geschichte stand die Anwendung im Apple App Store und im Google Play Store nicht mehr zum Download zur Verfügung. Die Unternehmensleitung erklärte, diese Nichtverfügbarkeit sei nur vorübergehend und auf ein »technisches Problem« zurückzuführen (BBC 2019). Die Regierung der Vereinigten Arabischen Emirate bestritt vor allem, dass die App als Spionageinstrument konzipiert war (*The Times of Israel* 2019). Der Entwickler der App bestritt, mit einer Regierung in Verbindung zu stehen.

In einem verspäteten Versuch der ethischen und juristischen Schadensbegrenzung entfernte Twitter 2019 vor allem in Ägypten, Saudi-Arabien und den Vereinigten Arabischen Emiraten gefälschte und zwielichtige Konten, die irreführende Informationen über politische und militärische Konflikte im Nahen Osten verbreiteten (NPR 2019). Twitter sperrte außerdem 4.258 »Fake-Accounts aus den VAE«, die im Verdacht standen, falsche Nachrichten über den Jemenkrieg zu verbreiten, in dem Saudi-Arabien seit 2015 ein Militärbündnis gegen die vom Iran unterstützten Houthis anführt (*News* 1 2019).

Eine der arabischen Regierungen, die dafür bekannt ist, ihre Gegner:innen online zu verfolgen, ist Saudi-Arabien. Bei einem berüchtigten Vorfall, der als

»Twitter-Spionageskandal« bekannt wurde, wurden zwei ehemalige Twitter-Mitarbeiter vom Justizministerium der Vereinigten Staaten angeklagt, im Auftrag der saudi-arabischen Regierung spioniert zu haben (NAKASHIMA/BENSINGER 2019). Während ihres Beschäftigungsverhältnisses gelang es ihnen, Tausende Twitter-Nutzerdatensätze zu durchsuchen, um Gegner:innen und Kritiker:innen des Königreichs zu identifizieren. Einige der von den beiden Spionen aufgespürten Konten gehörten Aktivist:innen, die zum Schutz der eigenen Identität und persönlichen Sicherheit und zur Vermeidung staatlicher Repressalien unter Pseudonymen twitterten. Eine dritte Person wurde außerdem beschuldigt, als Verbindungsperson zwischen saudischen Amtsträgern und den beiden ehemaligen Twitter-Mitarbeitern vermittelt und die unrechtmäßige Datenverletzung ermöglicht zu haben (BBC 2019).

Diese Geschichte ist deswegen so bedeutend, weil Verbindungsleute eines arabischen Golfstaates ihre Position als Twitter-Mitarbeiter erfolgreich ausnutzen konnten, um auf große Datenbanken zuzugreifen und persönliche Informationen einiger Regierungskritiker:innen abzuschöpfen. Das ist deswegen gefährlich, weil soziale Medien eigentlich für die Bevölkerung Saudi-Arabiens sowie anderer arabischer Staaten ein sicheres Forum für andernorts verdrängte Themen sein sollten. Nun sind sie zu einem Ort geworden, wo saudische Behörden ihre Gegner:innen aufspüren und kritische Stimmen unterdrücken können (BLOOMBERG 2019). Durch solche Maßnahmen seitens autoritärer Regime, einschließlich der Offenlegung der Identitäten hinter anonymen Konten, werden soziale Medien zu einem zunehmend gefährlichen und unsicheren Ort für die Kritiker:innen arabischer Regime, da immer mehr dieser Regierungen Anstrengungen unternehmen, Informationen über ihre Dissident:innen und Gegner:innen online zu sammeln, um sie ins Visier zu nehmen und zum Schweigen zu bringen (KHAMIS 2019).

Die schockierenden Sachverhalte hinter diesem Skandal werfen ernste Fragen hinsichtlich der doppelten Rolle sozialer Medien auf, als zweischneidiges Schwert, das zugleich der Befreiung und der Unterdrückung dienen kann (BRUMFIELD 2019). Sie werfen außerdem Fragen der Datenverwaltung, der Internetfreiheit und der Ausnutzung riesiger Social-Media-Datenbanken durch ausländische Regierungen auf. Der komplexe Kontext, in dem dieser Skandal entstand, nämlich eine Mischung aus illegalen Aktivitäten wie Bestechung, Korruption und Ausbeutung, weist außerdem auch interessante, jedoch beunruhigende Parallelen zu anderen Vorfällen auf (KHAMIS 2019).

Zum Beispiel zeigt der »Twitter-Spionageskandal« die Gefahr auf, dass eine ausländische Macht über amerikanische Social-Media-Plattformen kritische Stimmen identifiziert und unterdrückt. Hier lässt sich eine Parallele zur russischen Einmischung in die US-Präsidentschaftswahlen 2016 ziehen. Auch wenn sich die Fälle in Bezug auf Kontext, Ziele und Umfang unterscheiden, waren

doch beide Male ausländische Regierungen beteiligt und beide erfolgten online durch erfolgreich angewandte Cyberspace-Taktiken und -Techniken, einschließlich Hacking (CNN 2019).

Es gibt auch einige Parallelen zwischen dem saudischen Twitter-Skandal und dem Datenschutzskandal bei Facebook und Cambridge Analytica, bei dem der Schutz persönlicher Daten und privater Informationen einer Vielzahl von Facebook-Nutzer:innen verletzt wurde (*South China Morning Post* 2018). Beide Vorfälle machten auf die Gefahren von Datenschutzverletzungen und Bedrohungen der Online-Datensicherheit aufmerksam, was das Vertrauen vieler Nutzer:innen in soziale Medienplattformen erschütterte und deren Glaubwürdigkeit schwer beschädigte.

Besonders bedeutsam ist hier, dass offenbar mindestens eine der in den Gerichtsakten des Twitter-Skandals benannten Personen eine Kontaktperson saudischer Amtsträger war. Die CIA geht mit hoher Wahrscheinlichkeit davon aus, dass diese die Ermordung des bekannten Journalisten Jamal Khashoggi im Jahr 2018 angeordnet haben (HARRIS/MILLER/DAWSEY 2018).

Die *New York Times* berichtete in einem Artikel, Saudi-Arabien habe den im saudischen Konsulat in Istanbul grausam ermordeten Journalisten Jamal Khashoggi und andere Twitter-Kritiker:innen des saudischen Regimes mit einer »elektronischen Armee« ins Visier genommen und dabei über Twitter angeworbene Spione eingesetzt. Der Artikel deutete an, Khashoggis Online-Angreifer seien Teil einer breit angelegten Aktion von Kronprinz Mohammed bin Salman (MbS) und seinen engen Beratern, um Kritiker:innen innerhalb und außerhalb des Königreichs zum Schweigen zu bringen. Ein aus Hunderten von Personen bestehendes »elektronisches Komitee« mit Sitz in der Hauptstadt Riad arbeitete daran, die öffentliche Meinung gegen Dissident:innen zu wenden (BENNER et al. 2018).

Darüber hinaus gehörte eines der 6.000 Twitter-Konten, die im Auftrag der saudischen Regierung gehackt wurden (MORRIS 2018), dem prominenten saudischen Dissidenten und Regimekritiker Omar Abdulaziz. Der im kanadischen Exil lebende junge Blogger pflegte eine enge Freundschaft mit Jamal Khashoggi und kündigte an, die von seinem verstorbenen Freund begonnene Reise fortzusetzen und sich für Reformen in seinem Heimatland einzusetzen (KHAMIS/FOWLER 2020).

Auch der berüchtigte Fall des grausamen Mordes an dem Journalisten Jamal Khashoggi hat seinen Ursprung in saudischer Cyber-Überwachung. Laut dem Saudi-Kritiker und prominenten Blogger Omar Abdulaziz wurde seine regimekritische Kommunikation mit seinem verstorbenen Freund Khashoggi vom saudischen Regime überwacht, ohne dass er davon wusste (BRAGA 2018). Deshalb verklagte Abdulaziz das berüchtigte israelische Spionageunternehmen NSO, das diese Spionagefunktion angeblich an die Saudis verkauft hatte (*The Times of Israel* 2018).

Ein weiterer Fall betraf den erfolgreichen saudischen Twitter-Aktivisten Ghanem Almasarir, der vermutlich mit derselben israelischen Technologie von den Saudis gehackt wurde. In beiden Fällen wurden den Nutzern verdächtige Textnachrichten mit Links geschickt. Beim Klick darauf konnte die Spionagesoftware in ihre Geräte eindringen und auf die Kameras und Mikrofone ihrer Mobiltelefone zugreifen (SILVERSTEIN 2019).

Solche Vorfälle erinnern eindringlich daran, dass in der Phase nach dem Arabischen Frühling die Kritiker:innen arabischer Regime, seien es Aktivist:innen, Oppositionelle oder wahrheitssuchende Journalist:innen, nicht vor staatlicher Überwachung, Verfolgung, Trolling, Hacking und letztlich vor Vergeltungsmaßnahmen sicher sind, selbst wenn sie versuchen, sich im freiwilligen Exil in der Diaspora in Sicherheit zu bringen (KHAMIS/FOWLER 2020).

4. Die COVID-19-Ära und der Kampf um die Wahrheit

Die digitale Gegenrevolution in der arabischen Region verschärfte sich während der COVID-19-Pandemie, da verschiedene arabische Regime begannen, neuartige Instrumente einzusetzen und innovative Mechanismen zu nutzen. Dies sollte gewährleisten, dass die offizielle, staatlich orchestrierte Darstellung der Pandemie alle Medienplattformen dominierte, ohne von journalistischen Quellen in Frage gestellt zu werden. Das zunehmende Informationsbedürfnis der Bevölkerung in Bezug auf die Pandemie beunruhigte viele autoritäre Regierungen in der Region, da jeder Versuch, sich Informationen über nicht staatlich kontrollierte Stellen zu beschaffen, sofort als Bedrohung angesehen wurde, die es zu beseitigen galt (KHAMIS 2020b).

Arabische Regierungen rangen daher darum, die offizielle Darstellung der COVID-19-Pandemie in ihrem eigenen Sinne zu kontrollieren und definieren, darunter auch Infektionszahlen und Todesraten. Dies wirkte sich auf zweierlei Weise aus. Einerseits verstärkten diese Bemühungen die Abhängigkeit von manipulierten, staatlich kontrollierten offiziellen Medien als Hauptkommunikationsmittel. Andererseits gingen die Regimes in ihrem Streben nach »maximaler narrativer Kontrolle« aber auch gegen lokale wie internationale Medien und Journalist:innen vor, die es wagten, die offizielle Darstellung in Frage zu stellen (*Middle East Eye Correspondent* 2020). Diese neue Phase der »bewaffneten Zensur« führte in vielen arabischen Ländern zum Niedergang der freien Meinungsäußerung und journalistischer Freiheit (MARZOUK 2020). So gingen einige arabische Regierungen unter dem Vorwand der Desinformationsbekämpfung hart gegen lokale und ausländische Medien vor, um nicht regierungskonforme Berichterstattung über COVID-19 abzustrafen (KHAMIS 2020b).

Einige Beispiele dafür sind die Verhaftung von Lina Attalah, Chefredakteurin des letzten unabhängigen Medienorgans Ägyptens, der Website Mada Masr; sowie des Journalisten Hassan Mahgoub und des Redakteurs Atef Hasballah. Diese Verhaftungen erfolgten im Kontext einer zunehmenden Welle von Repressalien gegen die Pressefreiheit im Zusammenhang mit COVID-19-Berichterstattung (MICHAELSON 2020). Ein berüchtigter Fall war der des verstorbenen 65-jährigen ägyptischen Journalisten Mohamed Mounir, von dem angenommen wird, das das Coronavirus ihn »gleich zweifach ermordete« (MYERS 2020). Einmal, als er zum Ärger der ägyptischen Behörden darüber zu berichten wagte, und ein weiteres Mal, als er aufgrund dieser Berichterstattung verhaftet wurde, sich in einem überfüllten ägyptischen Gefängnis mit dem Virus infizierte und einige Tage nach seiner Entlassung an Komplikationen verstarb (KHAMIS 2020b). Auch internationale Reporter:innen und Auslandskorrespondent:innen waren gegen diese Welle staatlicher Repressionen nicht gefeit. Ein Beispiel dafür war der berüchtigte Fall der Guardian-Korrespondentin Ruth Michaelson, die ihre Presseakkreditierung verlor und aus Ägypten ausgewiesen wurde, nachdem sie in einem Artikel eine höhere Zahl von COVID-19-Fällen in Ägypten nannte, als von der ägyptischen Regierung offiziell angegeben (SANDERS IV 2020).

Die von den autoritären arabischen Regimen angewandten Techniken reichten von der Sperrung von Websites über die Verhaftung lokaler Journalist:innen und den Ausschluss internationaler Korrespondent:innen bis hin zum Einsatz von Strafgesetzen wie »Cybercrime Laws« und anderer restriktiver Maßnahmen. So sollten unter dem Deckmantel der Bekämpfung von »Desinformation« alle Medien verstärkt kontrolliert werden. Diese neuen Gesetze und Verordnungen sind oft so weit gefasst, unklar und vage, dass sich damit jede Berichterstattung kriminalisieren lässt, die dem Staat nicht genehm ist oder der offiziellen, staatlichen Darstellung der Pandemie widerspricht. Solche Berichterstattung wurde oft als Verbreitung von »Falschnachrichten« im Internet kriminalisiert, was in einigen arabischen Ländern, wie Ägypten, mit fünf Jahren Gefängnis und hohen Geldstrafen geahndet werden kann (ASSOCIATED PRESS 2020).

Darüber hinaus setzten einige arabische Regierungen neuartige Online-Überwachungsinstrumente und -techniken ein. Dazu zählen auch Anwendungen zur digitalen Kontaktverfolgung, um COVID-19-Fälle zu überwachen und den Aufenthaltsort, die Bewegungen und sozialen Kontakte positiv getesteter Personen zu ermitteln. Solche fortschrittlichen digitalen Anwendungen werden in den wohlhabenden und technologisch besser entwickelten arabischen Golfstaaten häufiger genutzt (NAFIE 2020). Eigentlich dienen sie der Eindämmung der Pandemie, doch bergen sie zahlreiche Gefahren, wie z. B. Hacking-Aktivitäten, Einsatz von Spyware-Tools und Verletzung der Privatsphäre seitens arabischer autoritärer Regime. Diese unter dem Vorwand der Pandemieverfolgung und -bekämpfung sanktionierten und legitimierten digitalen Werkzeuge lassen

sich auch wirksam einsetzen, um Regimegegner:innen und -kritiker:innen aufzuspüren, darunter Aktivist:innen und wahrheitssuchende Journalist:innen (KHAMIS 2020b). Das Committee to Protect Journalists (CPJ) hat einen Bericht mit Landkarte zum Thema »Covid-19 and Press Freedom« erstellt, der Art und Ort verschiedener COVID-19-bezogener Bedrohungen dokumentiert. Der Bericht enthält zahlreiche und weit verbreitete Verstöße arabischer Regime gegen die Pressefreiheit in der gesamten Region während der Pandemie, einschließlich der Sperrung zahlreicher Websites, Zugriffsbeschränkungen auf Websites, oder der Verhaftung von Journalist:innen (CPJ 2020).

Insgesamt umfasste das Instrumentarium staatlicher Repressalien während der Pandemie in der arabischen Welt Gesetze gegen »Fake News«; Inhaftierung von Journalisten; Aussetzung der freien Meinungsäußerung; »stumpfe« Zensur; Bedrohung von und Mobbing gegen Journalist:innen; Verweigerung von Akkreditierungsanträgen; Einschränkung der Bewegungsfreiheit; eingeschränkter Zugang zu Informationen; Ausweisungen und Visabeschränkungen; Überwachung und Rückverfolgung von Kontakten; sowie Notfallmaßnahmen (JACOBSEN 2020).

5. Abschließende Bemerkungen: Wie es weitergeht

Im weiteren Konflikt zwischen den arabischen Regimen und wahrheitssuchenden Journalist:innen, Kritiker:innen und Aktivist:innen, die deren Verfehlungen anzuprangern wagen, wird sich höchstwahrscheinlich auch der Kampf um Inhalte und die Kontrolle darüber fortsetzen, sowohl über herkömmliche als auch digitale Medien.

Die weite Verbreitung von Propaganda und die Flut irreführender Informationen über soziale Medienplattformen manipuliert und täuscht die öffentlichen Meinung im In- und Ausland. In den Händen autoritärer Regime ist dies eine wertvolle Waffe. Daher ist es entscheidend, die über diese Plattformen verbreiteten Nachrichten zu validieren, um solche schädlichen Auswirkungen einzudämmen, insbesondere, weil sich vor allem junge Menschen zunehmend auf soziale Medien als Informationsquellen verlassen.

Laut einer Umfrage des Pew Research Center (2021) nutzen etwa sieben von zehn Amerikaner:innen soziale Medien zur Pflege ihrer sozialen Kontakte, für ihren Nachrichtenkonsum, zum Informationsaustausch und zur Unterhaltung. Die neue Generation verlässt sich voll auf soziale Medien. 61 Prozent der Befragten entwickeln ihre politischen Ansichten aufgrund von Facebook-Inhalten, während nur 31 Prozent auf herkömmliche Medien wie das Fernsehen vertrauen. Auch in der arabischen Welt hat die Nutzung sozialer Medien in den letzten Jahren deutlich zugenommen. So nutzen 98 Prozent der saudi-arabischen

Bevölkerung das Internet. 82 Prozent nutzen soziale Medien in hohem Maße für Nachrichten und Unterhaltung (*Global Media Insight* 2022). In den Vereinigten Arabischen Emiraten lag die Nutzung sozialer Medien im Januar 2022 bei erstaunlichen 106 Prozent (einzelne Nutzer:innen können mehr als ein Konto in sozialen Medien haben) (DATA REPORTAL 2022).

Daher sollte die Bevölkerung auf sozialen Medien korrekte Informationen und überprüfte Nachrichten aus zuverlässigen Quellen verbreiten und erhalten können, anstatt Desinformation und Propaganda ausgesetzt zu sein.

In einer Zeit, in der Cyberkriege zwischen Regierungen und ihren Gegner:innen immer mehr eskalieren, zeigen erschreckende Vorfälle wie der »Twitter-Spionageskandal« und viele andere, dass diejenigen, die sich aktivistisch, kritisch oder journalistisch gegen repressive Regime auszusprechen wagen, realen Gefahren und Lebensbedrohungen ausgesetzt sind (AKKAD 2019). Die soziale Verantwortung und Glaubwürdigkeit der Social-Media-Branche stehen nunmehr in Frage, da solche Vorfälle freilich Bedenken aufkommen lassen, ob Silicon Valley überhaupt in der Lage ist, private Nutzerdaten allgemein, und insbesondere die von Dissident:innen und Gegnern repressiver Regierungen, zu schützen. Social-Media-Unternehmen sehen sich heute mit verschiedenen Herausforderungen konfrontiert, darunter auch die Entwicklung von Schutzmechanismen für ihre Daten, nicht nur vor Hackerangriffen, sondern auch vor skrupellosen Mitarbeiter:innen (*South China Morning Post* 2019). Social-Media-Giganten wie Facebook und Twitter müssen unbedingt neue Richtlinien entwickeln, wer auf welche Weise auf ihre Datenbanken zugreifen darf (TIFFANY 2019). Außerdem müssen sie klare Regeln und Vorschriften aufstellen, um ihre Daten gegen Manipulation zu sichern und zu schützen, sei es durch ausländische Regierungen und andere Stellen oder durch ihre eigenen Mitarbeiter:innen und Insider.

Diese vielschichtigen Bedrohungen und Herausforderungen lassen sich nur mit ebenso vielschichtigen Strategien bekämpfen. Eine Möglichkeit, solchen Bedrohungen in Zukunft zu begegnen, ist die Beteiligung von Silicon Valley-Unternehmen an der Ausarbeitung und Umsetzung wirksamer und transparenter neuer politischer Maßnahmen. Dies könnte das Vertrauen der Öffentlichkeit in die Integrität und Glaubwürdigkeit der Social-Media-Giganten wiederherstellen.

Ein weiterer, ebenso wichtiger Punkt ist die Vermittlung der dringend benötigten Medienkompetenz an die Öffentlichkeit durch entsprechende Bildungs-, Schulungs- und Sensibilisierungskampagnen. Viele Internetnutzer:innen sind leider nicht in der Lage, zwischen gefälschten Inhalten und korrekten Nachrichten zu unterscheiden. Wenn das Online-Publikum nicht über das nötige Bewusstsein verfügt, birgt dies viele Risiken, von der Gefahr, Opfer staatlicher Propaganda zu werden, bis hin zur Rekrutierung durch extremistische oder terroristische Gruppen im Internet.

Wenn all diese und andere Maßnahmen wirksam umgesetzt werden, besteht Hoffnung, dass sich einige der Risiken und Gefahren dieser neuen Phase des digitalen Autoritarismus und der digitalen Gegenrevolution in der arabischen Region und andernorts überwachen, bekämpfen, minimieren oder sogar verhindern lassen.

Über die Autor:innen

Dr. Sahar Khamis ist außerordentliche Professorin im Fachbereich Kommunikation und Associate Professor im Fachbereich Women's Studies an der University of Maryland in College Park. Sie ist Expertin für arabische und muslimische Medien und ehemalige Leiterin der Abteilung für Massenkommunikation an der Universität Katar. Dr. Khamis hat einen Doktortitel in Massenmedien und Kulturwissenschaften von der Universität Manchester in England. Sie ist Mitautorin der Bücher: *Islam Dot Com: Contemporary Islamic Discourses in Cyberspace* (Palgrave Macmillan, 2009) und *Egyptian Revolution 2.0: Political Blogging, Civic Engagement and Citizen Journalism* (Palgrave Macmillan, 2013). Sie ist die Mitherausgeberin des Buches: *Arab Women's Activism and Socio-Political Transformation: Unfinished Gendered Revolutions* (Palgrave Macmillan, 2018).

Dr. Khalid Al-Jaber ist Direktor des MENA-Zentrums in Washington D.C. und Assistenzprofessor für politische Kommunikation am Gulf Studies-Programm der Universität Katar. Zuvor arbeitete er am Al-Sharq Studies & Research Center und war Chefredakteur von *The Peninsula*, der führenden englischsprachigen Tageszeitung Katars. Al-Jaber ist Wissenschaftler für Arabistik und Golfstudien. Seine Forschungsschwerpunkte sind Politikwissenschaft, öffentliche Diplomatie, internationale Kommunikation und internationale Beziehungen. Er hat mehrere wissenschaftliche Bücher veröffentlicht und Beiträge für mehrere Fachzeitschriften geschrieben. Dr. Al-Jaber promovierte an der University of Leicester im Vereinigten Königreich und erwarb einen MA an der University of West Florida in den USA.

Dieser Text wurde mit finanzieller Unterstützung der Otto Brenner Stiftung übersetzt. Übersetzung: Kerstin Trimble

Literatur

AKKAD, DANIA (2019): Twitter's Saudi Spy Network Leaves Activists Living in Fear. In: *Middle East Eye*, 18. November 2019.

ASSOCIATED PRESS (AP) (2020):Egypt arrests doctors, silences critics over virus outbreak. In: *The Washington Post*, 6. Juli 2020. https://www.washingtonpost.com/health/egypt-arrests-doctors-silences-critics-over-virus-outbreak/2020/07/06/65eb7984-bf50-11ea-8908-68a2b9eae9e0_story.html

BANJO, SHELLY: Facebook, Twitter and the Digital Disinformation Mess. In: *The Washington Post*, 2 October 2019. https://www.washingtonpost.com/business/facebook-twitter-and-the-digital-disinformation-mess/2019/10/01/53334c08-e4b4-11e9-b0a6-3d03721b85ef_story.html

BBC (2019): Ex-Twitter Employees Accused of Spying for Saudi Arabia. In: BBC, 7. November 2019.

BBC (2019): Google and Apple Remove Alleged UAE Spy App ToTok. In: BBC, 23. Dezember 2019. https://www.bbc.com/news/technology-50890084

BENNER, KATIE; MAZZETTI, MARK; HUBBARD, BEN; ISAAC, MIKE (2018): Saudi's Image Makers. A Troll Army and a Twitter Insider. In: *The New York Times*, 20 October 2018. https://www.nytimes.com/2018/10/20/us/politics/saudi-image-campaign-twitter.html

BLOOMBERG (2019): Two Ex-Twitter Employees Charged With Spying for Saudi Arabia. In: *Bloomberg*, 7. November 2019.

BOWEN, JEREMY (2017): 1967 War: Six Days that Changed the Middle East. In: BBC, 5. Juni 2017. https://www.bbc.com/news/world-middle-east-3996046

BRADSHAW, SAMANTHA; HOWARD, PHILIP N. (2017): Troops, Trolls and Troublemakers: A Global Inventory of Organized Social Media Manipulation. In: *Oxford University Research Archive.* https://ora.ox.ac.uk/objects/uuid:cef7e8d9-27bf-4ea5-9fd6-855209b3e1f6/download_file?file_format=pdf&safe_filename=Troops-Trolls-and-Troublemakers.pdf&type_of_work=Report

BRAGA, MATHEW (2018): A Quebecer spoke out against the Saudis – then learned he had spyware on his iPhone. In: *CBC News*, 1 October 2018. https://www.cbc.ca/news/science/omar-abdulaziz-spyware-saudi-arabia-nso-citizen-lab-quebec-1.4845179

BRUMFIELD, CYNTHIA (2019): Twitter Spy Scandal a Wake-Up Call For Companies to Clean up their Data Access Acts. In: *CSO*, 12. November 2019.

CNN (2019): 2016 Presidential Campaign Hacking Fast-Facts. In: *CNN,* 31 October 2019.

COMMITTEE TO PROTECT JOURNALISTS (CPJ) (2020): *Covid-19 and press freedom*. https://cpj.org/covid-19/

DARNTON, ROBERT (2017): The True History of Fake News. In: *The New York Review of Books*, 13 Februar 2017. https://www.nybooks.com/daily/2017/02/13/the-true-history-of-fake-news/

DATA REPORTAL (2022): Digital 2022: The United Arab Emirates. In: *Data Reportal*, 9 Februar 2022. https://datareportal.com/reports/digital-2022-united-arab-emirates

EL TANTAWY, NAHED; WIEST, JULIA B. (2011): Social media in the Egyptian revolution: Reconsidering resource mobilization theory. In: *International Journal of Communication*, 5, S. 1207-1224.

FREEDOM HOUSE (2017): New Report - Freedom on the Net 2017: Manipulating Social Media to Undermine Democracy. In: *Freedom House*, 14. November 2017. https://freedomhouse.org/article/new-report-freedom-net-2017-manipulating-social-media-undermine-democracy

GLOBAL MEDIA INSIGHT (2022): Saudi Arabia Social Media Statistics 2022. In: *Global Media Insight*, 17. Juni 2022. https://www.globalmediainsight.com/blog/saudi-arabia-social-media-statistics/

GRIMES, DAVID ROBERT (2017): Russian fake news is not new: Soviet Aids propaganda cost countless lives. In: *The Guardian*, 14. Juni 2017. https://www.theguardian.com/science/blog/2017/jun/14/russian-fake-news-is-not-new-soviet-aids-propaganda-cost-countless-lives

HAARETZ (2019): Popular Messaging App Is UAE Spy Tool, Developed By Firm Employing Ex-NSA and Israeli Intel Officers. In: *Haaretz*, 23. Dezember 2019. https://www.haaretz.com/middle-east-news/popular-app-is-uae-spy-tool-made-by-firm-employing-ex-israeli-intel-officers-1.8304528

HAREL, AMOS; LEVINSON, CHAIM; KUBOVICH, YANIV (2018): Isreali Cyber Firm Negotiated Advanced Attack Capabilities Sale with Saudis. In: *Haaretz*, 25. November 2018. https://www.haaretz.com/israel-news/.premium-israeli-company-negotiated-to-sell-advanced-cybertech-to-the-saudis-1.6680618

HARRIS, SHANE; MILLER, GREG; DAWSEY, JOSH (2018): CIA Concludes Saudi Crown Prince Ordered Jamal Khashoggi's Assassination. In: *Washington Post*, 16. November 2018.

HASAN, MEHDI (2019): Don't Forget that Saudi Arabia is Imprisoning and Torturing Women's Rights Activist Loujain Al-Hathloul. In: *The Intercept*, 24. Dezember, 2019.

HOWARD, PHILIP N. (2011): *The digital origins of dictatorship and democracy: Information technology and political Isla*m. Oxford: Oxford University Press.

Human Rights Watch (2016): Arab Gulf States: Attempts to Silence 140 Characters. In: *Human Rights Watch*, 1. November 2016. https://www.hrw.org/news/2016/11/01/arab-gulf-states-attempts-silence-140-characters

JACOBSEN, KATHERINE (2020): Amid Covid-19, the Prognosis for press freedom is dim. Here are 10 symptoms to track. In: COMMITTEE TO PROTECT JOURNALISTS

(CPJ). https://cpj.org/reports/2020/06/covid-19-here-are-10-press-freedom-symptoms-to-track/

JONES, MARC OWEN (2022). *Digital authoritarianism in the Middle East: Deception, disinformation and social media*. London: C Hurst & Co Publishers Ltd.

KHAMIS, SAHAR (2019): The Twitter Spy Scandal: Context, Parallels, Threats, and Responsibilities.« In: *Gulf International Forum*, 9. Dezember 2019. https://gulfif.org/the-twitter-spy-scandal-context-parallels-threats-and-responsibilities/

KHAMIS, SAHAR (2020a): Between »digital euphoria« and »cyber-authoritarianism:« Technology's two faces. In: *Oasis. Christians and muslims in the global world*, (16) 31, 2020, S. 94-102.

KHAMIS, SAHAR (2020b): A battle of two pandemics: Coronavirus and digital authoritarianism in the Arab World. In: SEXTON, MICHAEL; CAMPBELL, ELIZA (eds.): *Cyber War & Cyber Peace in the Middle East*. Washington, DC: Middle East Institute, S. 145-162.

KHAMIS, SAHAR; EL-IBIARY, RASHA (2022): Egyptian women journalists' feminist voices in a shifting digitalized journalistic field. In: *Digital Journalism*. https://www.tandfonline.com/doi/full/10.1080/21670811.2022.2039738

KHAMIS, SAHAR; FOWLER, RANDALL (2020): Arab resistance in the diaspora: Comparing the Saudi dissident and the Egyptian whistleblower. In: *Journal of Arab & Muslim Media Research*, 13(1), S. 31-49.

KHAMIS, SAHAR; GOLD, PAUL B.; VAUGHN, KATHERINE (2013): Propaganda in Egypt and Syria's 'cyberwars': Contexts, actors, tools, and tactics. In: AUERBACH, JONATHAN; CASTRONOVO, RUSS (Hrsg.): *The Oxford handbook to propaganda studies*. New York: Oxford University Press, S. 418-438.

LYNCH, MARC (2012): *The Arab uprising: The unfinished revolutions of the new Middle East*. New York: Public Affairs.

LYNCH, MARC (2016): *The new Arab wars: Uprisings and anarchy in the Middle East*. New York: Public Affairs.

MARCZAK, BILL; SCOTT-RAILTON, JOHN; MCKUNE, SARAH; ABDUL RAZZAK, BAHR; DEIBERT, RON (2018): Hide and Seek: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries. In: *Citizen Lab*, 18. September 2018. https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/

MARCZAK, BILL; SCOTT-RAILTON, JOHN (2016): The Million Dollar Dissident: NSO Group's iPhone Zero-Days used against a UAE Human Rights Defender. In: *Citizen Lab*, 24. August 2016. https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/

MARZOUK, HORRIYA (2020): Weaponized censorship: The final demise of free expression in Egypt's media. In: *The New Arab*, 2 July 2020. https://english.alaraby.co.uk/english/indepth/2020/7/2/the-final-demise-of-free-expression-in-egypts-media

MICHAELSON, RUTH (2020): Egyptian editor briefly detained in Covid-19 reporting crackdown. In: *The Guardian*, 17. Mai 2020. https://www.theguardian.com/world/2020/may/17/egyptian-editor-held-in-covid-19-reporting-crackdown

MIDDLE EAST EYE CORRESPONDENT (2020): Fear is overcoming me: Egypt cracks down harder on media amid pandemic. In: *Middle East Eye*, 21. Juni 2020. https://www.middleeasteye.net/news/fear-overcoming-me-egypt-steps-crackdown-media-amid-pandemic

MILLER, MAGGIE (2019): Twitter Removes 88k Accounts Tied to Saudi Arabia. In: *TheHill*, 20. Dezember 2019. https://thehill.com/policy/cybersecurity/475488-twitter-takes-down-88k-accounts-tied-to-saudi-arabia

MORRIS, LOVEDAY (2018): Secret Recordings Give Insight Into Saudi Attempts to Silence Critics. In: *The Washington Post*, 17 October 2018.

MYERS, ELISABETH R. (2020): Egyptian journalist Mohamed Mounir murdered by Coronavirus. In: *Inside Arabia*, 25. August 2020. https://insidearabia.com/egyptian-journalist-mohamed-mounir-murdered-by-coronavirus/?fbclid=IwARobgj32CYLOiAuVQFpgNyJD7R_QVnpx9G_GKcxLqMrOp75WdKcqFws3bog

NAFIE, MUHAMMED (2020): UAE's coronavirus tracing app-Is it compulsory and other questions answered. In: *Al Arabiya English*, 20. April 2020. https://english.alarabiya.net/en/coronavirus/2020/04/20/UAE-s-coronavirus-tracing-app-Is-it-compulsory-and-other-questions-answered

NAKASHIMA, ELLEN; BENSINGER, GREG (2019): Former Twitter Employees Charged With Spying for Saudi Arabia by Digging Into the Accounts of the Kingdom's Critics. In: *The Washington Post*, 6. November 2019.

NEWS 1 (2019): Twitter closes thousands of pro-Saudi accounts in Egypt and UAE for spreading misleading news. In: *News 1*, 20. September 2019. https://www.news1.news/sa/2019/09/twitter-closes-thousands-of-pro-saudi-accounts-in-egypt-and-uae-for-spreading-misleading-news.html

NPR (2019): Twitter Removes Thousands of Accounts For Manipulating Its Platform. *NPR*, 20. September 2019. https://www.npr.org/2019/09/20/762799187/twitter-removes-thousands-of-accounts-for-manipulating-their-platform

PEW RESEARCH CENTER (2021): Social Media Fact Sheet. https://www.pewresearch.org/internet/fact-sheet/social-media/

ROMANOSKY, SASHA (2017): Private-Sector Attribution of Cyber Attacks: A Growing Concern for the U.S. Government?« In: *Law Fare*, 21. Dezember 2017. https://www.lawfareblog.com/private-sector-attribution-cyber-attacks-growing-concern-us-government

RUWITCH, JOHN (2021): *NPR*, 31. März 2021. https://www.npr.org/2021/03/31/983156340/theory-that-covid-came-from-a-chinese-lab-takes-on-new-life-in-wake-of-who-report

SAKR, NAOMI (2013): *Transformations in Egyptian journalism*. New York: Palgrave Macmillan.

SANDERS IV, LEWIS (2020): Egypt expels British journalist over coronavirus coverage. In: DW, 27. März 2020. https://www.dw.com/en/egypt-expels-british-journalist-over-coronavirus-coverage/a-52942136

SEIB, PHILIP (2007): New media and prospects for democratization. In: SEIB, P. (Hrsg.): *New media and the new Middle East.* New York, NY: Palgrave Macmillan, S. 1-17.

SHANE, SCOTT; GOEL, VINDU (2017): Fake Russian Facebook Accounts Bought $100,000 in Political Ads. In: *The New York Time*s, 6. September 2017. https://www.nytimes.com/2017/09/06/technology/facebook-russian-political-ads.html

SHEZAF, HAGAR; JACOBSON, JONATHAN (2018): Revealed: Israel's Cyber-spy Industry Helps World Dictators Hunt Dissidents and Gays. In: *Haaretz*, 20 October 2018. https://www.haaretz.com/israel-news/.premium.MAGAZINE-israel-s-cyber-spy-industry-aids-dictators-hunt-dissidents-and-gays-1.6573027

SILVERSTEIN, RICHARD (2019): Israeli Tech's Dirty Ops. In: *Jacobin*, 6. Juni 2019, https://jacobinmag.com/2019/06/whatsapp-hacking-ngo-group-israel

SOUTH CHINA MORNING POST (2018): How Cambridge Analytica Exploited Facebook Users' Data, and Why it's a Big Deal. In: *South China Morning Post*, 28. März 2018.

SOUTH CHINA MORNING POST (2019): Twitter Spy Case Shines Spotlight on Rogue Staff. In: *South China Morning Post*, 9. November 2019.

STONE, JEFF (2019): Twitter Removes Nearly 6,000 Accounts Spreading Saudi Propaganda. In: *Cyberscoop*, 20. Dezember 2019.

STUBBS, JACK (2019): Facebook Says it Dismantles Cover Influence Campaign Tied to Saudi Government. In: *Reuters*, 1. August 2019. https://www.reuters.com/article/us-facebook-saudi/facebook-says-it-dismantles-covert-influence-campaign-tied-to-saudi-government-idUSKCN1UR50J

SWAINE, JON (2018): Twitter admits far more Russian bots posted on election than it had disclosed. In: *The Guardian*, 19. Januar 2018. https://www.theguardian.com/technology/2018/jan/19/twitter-admits-far-more-russian-bots-posted-on-election-than-it-had-disclosed

THE GUARDIAN (2019): Popular Chat App ToTok is Actually a Spying Tool of UAE Government – Report. In: *The Guardia*n, 23. Dezember 2019. https://www.theguardian.com/world/2019/dec/23/totok-popular-chat-app-spying-tool-uae-government

THE TIMES OF ISRAEL (2018): Saudi Dissident Sues Israel Spyware Firm Over Khashoggi Killing. In: *The Times of Israe*l, 3. Dezember 2018. https://www.timesofisrael.com/saudi-dissident-sues-israeli-spyware-firm-over-khashoggi-killing/

THE TIMES OF ISRAEL (2019): UAE Denies Developing Popular Middle East App as Spy Tool. In: *The Times of Israel*, 28. Dezember 2019. https://www.timesofisrael.com/uae-denies-developing-popular-middle-east-app-as-spy-tool/

THIBAUT, OLIVIER: Before Trump, the long history of fake news. In: *Yahoo News*,12. Juli 2018. https://sg.news.yahoo.com/trump-long-history-fake-news-045226919.html

TIFFANY, KAITLYN (2019): A Timeline of High-Profile Tech Apologies. In: *Vox*, 26. Juli 2019.

ZILBER, NERI (2018): The Rise of the Cyber-Mercenaries. In: *Foreign Policy*, 31. August 2018. https://foreignpolicy.com/2018/08/31/the-rise-of-the-cyber-mercenaries-israel-nso/