Universität der Bundeswehr München

KONRAD ADENAUER STIFTUNG

Kommunikation Resilienz und Sicherheit

Hrsg:
Natascha Zowislo-Grünewald
Nils Wörmer

www.kas.de

Kommunikation, Resilienz und Sicherheit

Hrsg:
Natascha Zowislo-Grünewald
Nils Wörmer

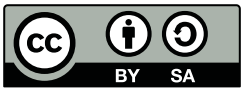
Impressum

Herausgeberin:
Konrad-Adenauer-Stiftung e. V. 2021, Berlin

Gestaltung und Satz: yellow too Pasiek Horntrich GbR
Die Printausgabe wurde bei der Druckerei Kern GmbH, Bexbach, klimaneutral produziert und auf FSC-zertifiziertem Papier gedruckt.
Printed in Germany.

Gedruckt mit finanzieller Unterstützung der Bundesrepublik Deutschland.

Eine Kooperation der Konrad-Adenauer-Stiftung e. V. mit der Universität der Bundeswehr München und dem Lehrstuhl für Unternehmenskommunikation (Strategic Communication Management).



ISBN 978-3-95721-914-5

Auf einen Blick

Die zunehmende Bedrohung freiheitlicher Gesellschaften durch Desinformationskampagnen, Fake News und anderen Formen delegitimierender Kommunikation ist nicht vergleichbar mit althergebrachten sicherheitspolitischen Konfliktlagen und auch nur mithilfe eines fundierten und systematischen Kommunikationsbegriffs fassbar. Kommunikation stellt einen zentralen Faktor für das Überleben und Gelingen von Organisationen in Wirtschaft und Politik dar. Auf Dauer werden staatliche Akteure und Organisationen daher nicht umhinkommen, der Kommunikation einen primären Stellenwert einzuräumen.

Angriffe im Informationsumfeld sind wirkmächtig, und versuchen mit dem Mittel der Desinformation, das Vertrauen der Bevölkerung in ihre eigenen Institutionen zu untergraben. Sie sind nicht-militärischer Natur, gleichwohl staatsgefährdend. Mit „objektiven Wahrheiten" oder anderen Evidenzen allein lassen sich auf Desinformation angelegte Kampagnen aber nur unzureichend begegnen. Sie bergen soziale Sprengkraft und können nur mit einem passenden Kommunikationsangebot konstruktiv bekämpft werden. Bei der Begegnung ist ein gesamtstaatlicher, kommunikativ-proaktiver Ansatz notwendig.

Im Zeitalter der Digitalisierung bleibt eine Demokratie nur dann wehrhaft, wenn es ihr mittels strategischer Kommunikation gelingt, Glaubwürdigkeit und Vertrauen aufzubauen. Vertrauen ist das wirksamste Mittel, um Widerstandskraft gegen Staat und Gesellschaft gefährdende Narrationen zu erzeugen. Dies kann jedoch nur durch ein argumentatives Werben um Akzeptanz unter Wahrung der Anschlussfähigkeit an gesamtgesellschaftliche Werte, Überzeugungen und Identitäten gelingen.

Dies bedeutet auch, überhaupt eine außen- und sicherheitspolitische Strategiedebatte zu führen und die Bedrohung des Westens als Wertegemeinschaft zu verdeutlichen. Unterstützt werden kann dies durch eine geeignete politische Medienbildung. Auf der reaktiven Seite könnte Des-

informationskampagnen außerdem durch ein sogenanntes Prebunking begegnet werden, indem Nutzer sozialer Medien durch automatisierte Warnungen auf problematische Beiträge aufmerksam gemacht werden. Proaktiv und langfristig erfolgversprechender wirken hingegen Counter-Influence-Kampagnen zur Bekämpfung kommunikativer Angriffshandlungen. Hierzu nötig ist zum einen ein Frühwarnsystem zur Identifizierung von feindlichen Akteuren, Kanälen und verwendeten Narrationen. Zum anderen ist es aber auch wichtig, gegensätzliche Narrative zu schaffen, die helfen, Echokammern zu durchbrechen und den einzelnen von manipulierten Überzeugungen zu lösen.

Die Bedrohungslage in der „Domäne der Information“ ist real und mannigfaltig. Die Bedrohung selbst ist dabei auf die innere Kohäsion unserer freiheitlichen Gesellschaft gerichtet. Eine wirksame Antwort auf diese Bedrohung muss an der Stärkung dieser Kohäsion ansetzen. Dies bedeutet letztendlich, durch ein attraktives narratives Deutungsangebot die Kraft von Desinformationskampagnen zu brechen.

Inhaltsverzeichnis

Vorwort

Digitalisierung, Globalisierung, die sich verschärfende Systemkonkurrenz mit China und das zunehmend aggressive Auftreten Russlands haben sich zu Brandbeschleunigern der weltweiten Konflikt- und Bedrohungsherde des 21. Jahrhunderts entwickelt: Dabei fungiert die Aufweichung bzw. Neuordnung der weltpolitischen Ordnung als Grundlage, auf der sich die stets beschleunigende Kommunikation – ob digital oder analog – im schlimmsten Fall zerstörerisch auswirken kann.

Kriminalität im Cyberraum, hybride Kriegführung und Datenmanipulation sind nur drei Stichworte, welche die Wirkweisen dieses zerstörerischen Potenzials aufzeigen: Die davon ausgehende Bedrohung ist permanent, unkonkret und vor dem Hintergrund einer multipolaren Weltordnung besonders offen für subjektive Bewertung und Einordnung.

Im digitalen Zeitalter steht somit alles „zur Debatte". Diesem, seiner Natur nach kommunikativen Paradigmenwechsel, lässt sich nur begegnen, indem man Kommunikation nicht nur neu denkt, sondern ihr innerhalb des eigenen Denkens eine neue Rolle zuweist.

1. Bedrohungen im Informationsraum. Wie gravierend ist das Problem?

Die Herausforderungen für Sicherheitskommunikation betreffen insbesondere die neuen und stark wachsenden Bereiche digitaler Wandel, Künstliche Intelligenz und soziale/neue Medien – und das in einer immer stärker vernetzten Welt. Die damit einhergehenden Herausforderungen und Bedrohungsszenarien werden jedoch häufig verdrängt, falsch bewertet oder gar nicht erst erkannt. So spielt, hinsichtlich der grundsätzlichen „Verhandelbarkeit" sogar fundamentaler Annahmen, das Stichwort „Resilienz" eine zentrale Rolle, sowohl in der inneren als auch in der äußeren Sicherheit. Die Akzeptanz für das westliche Werte- und Bündnissystem

ist bspw. keine Selbstverständlichkeit mehr. Das führt dazu, dass sich nicht nur Sicherheitsempfinden und -bedürfnis der Bevölkerung wandeln, sondern Fake News und propagandistische Einflussnahme viel leichter ihre Wirkung entfalten können.

Der Begriff „Fake News" entwickelte sich in den vergangenen Jahren zu einem festen Bestandteil des Sprachschatzes. Der Begriff beschreibt allgemeine kommunikative Bedrohungslagen. Umgangssprachlich wird er als Chiffre für manipulierende Falschmeldungen verwendet, die insbesondere in den Medien und v. a. im Internet und den sozialen Medien verbreitet werden. Gerade letztere besitzen aufgrund der ihnen innewohnenden, affektiv wirkenden Beschleunigungs- und Verstärkungseffekte, eine besondere Relevanz bei der Verbreitung von Fake News. Die Tätigkeiten u. a. der russischen „Trollfabrik" Glavset, die öffentliche Meinung in den westlichen Ländern durch Postings auf den verschiedenen Plattformen der sozialen Medien beeinflussen zu wollen, sind hier nur eines von vielen prominenten Beispielen, die die realweltlichen Konsequenzen von Fake News aufzeigen. Der mehrfach dokumentierte Einsatz dieser auch „Kreml-" oder „Putin-Bots" genannten Informationskrieger, sei es ab 2014 zur Unterstützung der russischen Interessen im Rahmen der Krim-Annexion oder die Einflussnahme auf die Präsidentschaftswahlkämpfe 2016 in den USA und 2017 in Frankreich, führen die sicherheitspolitische Relevanz manipulativer Kommunikation als einem essenziellen Teil der hybriden Kriegführung deutlich vor Augen.

Auch wenn die Verbreitung von Lügen, Verleumdungen oder Falschmeldungen seit jeher ein probates Mittel der Propaganda bzw. politischer Auseinandersetzungen ist, hat sich der Begriff „Fake News" erst seit einigen Jahren etabliert. Er wird v. a. in Bezug auf die quasi viralen Verbreitungsmöglichkeiten von Kommunikaten aller Art über die sozialen Medien verwendet. Diese kommunikativen Bedrohungslagen unterminieren die Glaubwürdigkeit von Unternehmen, politischen Organisationen und im Extremfall selbst der Demokratie als Staatsform. Latent oder offensiv, zufällig oder vorsätzlich – die Wirkung ist bei denjenigen, die dem nichts entgegenzusetzen haben, die also nicht resilient sind, die gleiche.

Das Fundament der eigenen Überzeugungen bröckelt. Möglich scheint alles, bis hin zur Implosion politischer Systeme. Resilienz gegenüber den zersetzenden Kommunikationswirkungen ist sicherheitspolitisch also ein strategisches Asset.

Die Glaubwürdigkeit des Behaupteten wird zur zentralen Dimension der Wirkungskraft von Fake News in kommunikativen Bedrohungslagen. Deshalb ist dieses Phänomen auch so stark mit den sozialen Medien verknüpft. Sie können durch den permanenten Rückbezug auf die Meinung anderer den Glaubwürdigkeitseffekt gleichsam potenzieren. Um die Wirksamkeit von Fake News zu beschneiden, werden Kommunikate, Botschaften, Nachrichten oder Kampagnen, die als Fake News identifiziert wurden, vielfach einem Faktencheck unterzogen, um der „Wahrheit" wieder „zu ihrem Recht" zu verhelfen. Dabei stellt sich die Frage, ob die Thematisierung der „objektiven Wahrheit" das geeignete Diskursangebot ist, wenn doch Kommunikation von deren Anschlussfähigkeit an bestehende Rahmungen und Wertanschauungssysteme abhängig ist.

In einer kommunikativen Arena, die alle fundamentalen Wahrheiten der letzten Jahrzehnte hinterfragt und auf die Probe stellt, gilt für „die Wahrheit", dass sie einfach und plausibel, letztlich v. a. glaubwürdig sein muss. Zweifel sind also begründet, ob das in der öffentlich-rechtlichen Sphäre gern thematisierte Instrument des Faktenchecks vorbehaltlos geeignet ist, Fake News zu bekämpfen und Resilienz aufzubauen.

Auch die Wirksamkeit des Ansatzes, die Verbreitung von Fake News technisch zu behindern, ist umstritten. Die Betreiber von Social-Media-Plattformen haben nach eigenem Bekunden ein Interesse daran, die Verbreitung von Falschinformationen zu bekämpfen. Doch war dazu auch politischer Druck notwendig: Haben doch bspw. Facebook, Google, Microsoft und Twitter den EU-Verhaltenskodex gegen Desinformation unterzeichnet und setzen v. a. auf die automatische Detektion von Fake News. Die geschickte Verflechtung von Wahrheit und Lüge, wie sie gerade bei wirkmächtigen Falschnachrichten und Verschwörungstheorien zu beobachten ist, setzt jedoch der Wirksamkeit der dort eingesetzten Algorithmen klare Grenzen.

Kommunikation stellt deshalb einen zentralen Faktor für das Überleben und Gedeihen von wirtschaftlichen und politischen Organisationen dar. Auf Dauer werden staatliche Akteure sowie Organisationen nicht umhinkommen, der Kommunikation einen primären Stellenwert einzuräumen. Denn es ist nicht nur Reaktion gefragt, sondern auch kommunikativ-proaktive Maßnahmen, die den Rahmen für Sicherheit und Resilienz erst bilden können. Kommunikation soll Krisen nicht nur bewältigen, sondern im Inneren wie im Äußeren auch ex ante zu vermeiden helfen. Inhaltliche Orientierungslinien bilden Fragen nach der Ausrichtung von Kommunikation auf Awareness/Sensibilisierung in der konkreten Bedrohungswahrnehmung, der Optimierung von Reaktions- und Entscheidungsfähigkeit in Krisensituationen sowie bei der Stärkung der Verteidigungsfähigkeit und -bereitschaft.

Die Konrad-Adenauer-Stiftung hat in Zusammenarbeit mit der Professur für Unternehmenskommunikation an der Universität der Bundeswehr München zu diesem Themenkomplex von Juni bis Oktober 2020 die Webinarreihe „Kommunikation, Resilienz und Sicherheit" veranstaltet. Inhaltlich konnte das Problemfeld der Bedrohung unserer freiheitlichen Gesellschaft in der „Domäne der Information" hierin bereits deutlich umrissen werden. So stellen in einer asymmetrischen und hybriden Bedrohungslage nicht allein militärische Mittel eine immer größere Gefahr dar. Dies gilt insbesondere mit Blick auf das häufig vereinfacht als Gerasimov-Doktrin bezeichnete operative Denken, das der hybriden Kriegführung Russlands zugrunde liegt. Der „klassische" Konflikt – die Drohung mit dem Einsatz militärischer Mittel – wird so zu einem „Krieg der Überzeugungen", in dem Gedanken und Ideen eine übergeordnete Position einnehmen.

Dabei ist in solchen „neuen" Konflikten die Frage nach dem jeweiligen Aggressor nur von untergeordneter Bedeutung. Ausschlaggebend ist vielmehr die Frage nach den geeigneten Abwehrmechanismen, um einen möglichen Zusammenbruch der angegriffenen Diskurse und Institutionen zu verhindern.

Geeignet scheint, ein Mix aus Hard und Soft Power zu sein. Ausgehend vom Konzept strategischer Narrationen muss Kommunikation in diesem Mix eine zentrale Rolle spielen und sich darum bemühen, eben jene grundsätzlich notwendige Glaubwürdigkeit wiederherzustellen, deren Verlust als ursächlich für den um sich greifenden Relativismus gewertet werden kann.

Das in dieser Hinsicht mangelnde Problembewusstsein der jeweiligen Akteure kann deshalb erst Recht zum Kollaps des Diskursraumes beitragen, an dessen Ende auch die reale Welt betroffen wäre. Schließlich wird für Probleme, die als solche nicht wahrgenommen werden, keine Lösung gesucht. Wichtig ist es insofern, die Gefährdungslage durch Kommunikation als real zu begreifen, um mit geeigneten Strategien Resilienz bei Institutionen und Bevölkerung zu schaffen. Dies gelingt jedoch nur, wenn den Institutionen das nötige Vertrauen zukommt. Solches Vertrauen lässt sich aber nur aufbauen, wenn die jeweiligen Rezipientinnen und Rezipienten in ihren subjektiven Befindlichkeit ernst genommen werden.

Angriffe auf freiheitliche Gesellschaften haben immer mit der Strahlkraft der Kombination aus wirtschaftlicher Prosperität und eines Wertesystems zu tun, das die Würde des Menschen achtet. Der Erfolg der demokratischen Welt stellt insofern stets eine Gefahr für autokratische Systeme dar. Deshalb ist es wichtig, die richtigen Strukturen zu schaffen, um die Bedeutung unserer Wertegesellschaft zu betonen. Glaubwürdigkeit und Vertrauen in die menschliche Kommunikation spielen dabei eine zentrale Rolle.

2. Bedrohungen im Informationsraum begegnen – aber wie?

Die Forschungslage zur sicherheitspolitischen Rolle von Kommunikation im Inneren wie im Äußeren, einschließlich der Bekämpfung propagandistischer Einflussnahme und Cyberkriminalität, ist ebenso disparat wie dispers. Das Forschungsfeld ist hochgradig aktuell, gleichzeitig wurzelt es in der bis in die Antike zurückreichenden Beschäftigung mit politischer

Kommunikation. Es berührt eine Vielzahl von Disziplinen wie z. B. die Kommunikations- und Medienwissenschaften, die Informatik, die Psychologie, die Politikwissenschaften oder die Soziologie.

Ergänzend zu der Webinarreihe „Kommunikation, Resilienz und Sicherheit" wurde daher ein Call for Papers für wissenschaftliche Arbeiten gestartet, die aus der Perspektive ihrer jeweiligen Fachdisziplin Kommunikation als Größe in der Landes- und Bündnisverteidigung thematisieren, auf kommunikative Bedrohungen fokussieren und helfen, mögliche strategische Antworten zu formulieren. Die daraus hervorgegangenen und ausgewählten Arbeiten erlauben eine fundierte Einordnung und Bewertung der Bedrohungslage in der Informationdomäne und zeigen plausible Wege auf, diese Bedrohungen einzuhegen.

Im Fokus des einleitenden Beitrags von Stefan Gruhl, Christian Bell, Falko Hark, Philipp Huber und Lion König steht die Analyse hybrider Bedrohungen, also die Verknüpfung von regulärer und irregulärer Kriegführung. Dabei skizzieren die Autoren sehr eindringlich die Wirkmächtigkeit von Angriffen im Informationsumfeld und den Versuch, mithilfe von Desinformation das Vertrauen der Bevölkerung in ihre eigenen Institutionen zu untergraben. Als Phänomene „nicht-milit*ärischer aber staatsgefährdender*" Machtausübung kann derartigen Angriffen nur mit einem gesamtstaatlichen Ansatz begegnet werden. Die Autoren plädieren nicht nur für den Aufbau von Resilienz im Sinne präventiver Potenziale, sondern hinterfragen auch die traditionelle, institutionelle Trennung zwischen innerer und äußerer Sicherheit. Eine wirksame gesamtstaatliche Sicherheitsarchitektur könne allein in Form eines ressortübergreifenden, multinational abgestimmten Ansatzes geleistet werden.

Jürgen Schulz arbeitet in seinem Beitrag *Auftragskommunikation im Dienst* heraus, dass Kommunikation für Organisationen nicht auf eine rein instrumentelle Funktion reduziert werden darf, sondern vielmehr konstitutiv ist. Er setzt sich kritisch mit dem Begriff „Resilienz" auseinander und legt anschaulich dar, dass Fake News nicht dadurch neutralisiert werden können, indem ihnen „objektive Wahrheiten" oder

Evidenzen gegenübergestellt werden. Wer dies versuche, verkenne die dahintersteckende „soziale Sprengkraft". Kommunikation ist eben kein Informationsmedium, vielmehr „*überbrückt Sprache die Distanz zwischen dem, was ist*, und dem, was sein soll." Entwickelt man diesen Gedanken von Jürgen Schulz konsequent weiter, ist Kommunikation das Mittel, Bedrohungen in der Informationsdomäne konstitutiv und konstruktiv entgegenzutreten.

Ähnlich argumentieren Natascha Zowislo-Grünewald und Julian Hajduk in ihrem Beitrag. Ausgehend von einer Analyse der Bedrohungslage im Informations- und Diskursraum durch die neue Doktrin hybrider Bedrohungen machen sie deutlich, dass eine wirklich wehrhafte Demokratie nur durch ein sicherheitspolitisches, strategisches Kommunikationsmanagement möglich ist. Sie betonen, dass der Aufbau von Vertrauen das wirksamste Mittel sei, Widerstandskraft gegen feindliche, Staat und Gesellschaft gefährdende Narrationen zu erzeugen. Dies kann jedoch nur mithilfe eines argumentativen Werbens um Akzeptanz unter Wahrung der Anschlussfähigkeit an gesamtgesellschaftliche Werte, Überzeugungen und Identitäten, also durch Kommunikation, gelingen.

Ausgangspunkt des Beitrags von Cedric Bierganns ist die grundlegende Einsicht, dass demokratische Außen- und Sicherheitspolitik nur in dem Maße umgesetzt werden kann, wie sie im Inneren von den Bürgerinnen und Bürgern mitgetragen wird. Der Autor stellt die Frage, wie kontroverse Themen, also „unbequeme Wahrheiten", kommuniziert werden können, wenn die Gefahr einer angstgetriebenen emotionalen Debatte droht. Die Antwort sieht er in einem Vergleich mit der US-amerikanischen Kultur-, Bildungs- und Informationspolitik zum NATO-Doppelbeschluss in den 1980er-Jahren, der nicht nur in Deutschland zu einer scharfen sicherheitspolitischen Kontroverse geführt hatte. Geschickte Kommunikation führte nach Cedric Bierganns dazu, die „Kohäsion und Deutungshoheit des westlichen Bündnisses auf breiter gesellschaftlicher Ebene sichergestellt zu haben". Aus diesem historischen Vergleich schlussfolgert er, dass eine außen- und sicherheitspolitische Strategiedebatte geführt werden müsse, welche die Bedrohung des Westens als Wertegemeinschaft

verdeutliche und globale Zusammenhänge in lokalen Kontexten darstellen könne. Außerdem gelte es, in der politischen Bildung Sachthemen zu „vermenschlichen" und junge Zielgruppen zu erschließen.

Jan Wilhelm Ahmling geht in seinem Beitrag davon aus, dass eine politische Medienbildung geeignet sei, Resilienz gegen die mannigfaltigen Bedrohungen im Informationsraum aufzubauen. Diese Bedrohungen manifestieren sich in Form von Mis-, Des- und *Malinformation* und können durch die Vermittlung von „Medienkompetenz im Sinne einer analytisch-kritischen Informationskompetenz" bekämpft werden. Am Fallbeispiel von Finnland, das besonders intensiv von russischen Desinformationskampagnen betroffen ist, macht Jan Wilhelm Ahmling deutlich, dass die Vermittlung von Medienkompetenz nicht allein als „Schulfach" gedacht werden dürfe, sondern nur dann die gewünschte Wirkung entfalte, wenn zusätzlich ein „gesellschaftlich getragenes Ökosystem zur Medienkompetenzvermittlung" geschaffen werde.

Auch Ulrich Schade, Florian Meißner, Albert Pritzkau und Sonja Verschitz beschäftigen sich mit konkreten Möglichkeiten der Resilienzsteigerung gegenüber Desinformation bzw. Falschmeldungen. Als Ergänzung zum klassischen Konzept der Vermittlung von Medien- und Informationskompetenz oder von Faktenchecks zur Detektion von Desinformation, des sogenannten Debunkings, schlagen sie in Bezug auf Online- bzw. soziale Medien das Konzept des Prebunkings vor. Prebunking bedeutet, die Nutzerinnen und Nutzern durch automatisierte Warnungen bereits vor dem Konsum von Fake News zu sensibilisieren. Dabei diskutieren sie zwei verschiedene technische Lösungen. Zum einen den vom Medien-Start-up NewsGuard angewandten, quellenorientierten Ansatz, die Glaubwürdigkeit und Transparenz von Nachrichten- und Informationswebseiten in Form eines redaktionellen Prozesses zu bewerten. Zum anderen stellen sie ein Verfahren des Fraunhofer-Instituts für Kommunikation, Informationsverarbeitung und Ergonomie zur automatisierten Inhaltsbewertung von Beiträgen in den sozialen Medien vor, das auf der Kombination von Emotionalitätsanalyse der verwendeten Sprache und Metadaten basiert. Die Autorin und die Autoren sehen in

einer Kombination der beiden vorgestellten Lösungsansätze ein probates Verfahren, Beeinflussungskampagnen frühzeitig erkennen zu können.

Amelie Stelzner und Jakob Landwehr untersuchen in ihrem Beitrag, wie die Bundeswehr aktuell mit kommunikativen Bedrohungslagen in ihren Einsätzen im Ausland umgeht. Ausgehend von einer Auseinandersetzung mit der Bedrohung durch Fake News bzw. durch Desinformation und der theoretischen Betrachtung, wie eine Prävention vor solchen kommunikativen Bedrohungslagen sowie eine angemessene Reaktion hierauf aussehen könnte, beschreiben die Autorin und der Autor die bestehenden Strukturen der Bundeswehr zur Prävention und Abwehr von Fake News in ihren Auslandseinsätzen. Im Zentrum der Darstellung stehen die Ergebnisse einer durchgeführten Fallstudie zur Bundeswehrmission in Litauen. Untersucht wird dies an Beispielen von Fake News, die gezielt Gerüchte zur Diskreditierung der Bundeswehr gestreut haben.

Im abschließenden Beitrag dieses Sammelbandes werden konkrete Verfahren der Desinformationsbekämpfung zurück auf die strategische Frage bezogen, wie Sicherheit in Anbetracht der Bedrohungen aus der Informationsdomäne möglich ist. Holger Knappenschneider und Johannes Feige machen deutlich, dass Deutschland besonders gefährdet sei und Abwehrmaßnahmen gegen gezielte Desinformationskampagnen entwickeln müsse, um zu verhindern, „dass das gesellschaftspolitische Umfeld Deutschlands von innen heraus untergraben wird." Sie schlagen dabei eine proaktive Strategie vor, um mithilfe von Counter-Influence-Kampagnen kommunikative Angriffshandlungen zu bekämpfen. Diese Strategie besteht aus zwei Elementen: Zum einen ist dies ein Frühwarnsystem zur Identifizierung von feindlichen Akteuren, Kanälen und verwendeten Narrationen im Sinne einer ersten „Verteidigungslinie der Zivilgesellschaft." Zum anderen sollen Desinformationskampagnen geschwächt werden, indem gegensätzliche Narrative geschaffen werden, die helfen, Echokammern zu durchbrechen. Dies kann Einzelnen helfen, sich von manipulierten Überzeugungen zu lösen. Dabei dürfe eine Counter-Influence-Kampagne nicht Top-down-orientiert gedacht werden, sondern müsse sich vielmehr auf einer tieferen Ebene mit der Zivilgesellschaft verbinden, also von unten

nach oben wirken. Holger Knappenschneider und Johannes Feige mahnen, vor dem Hintergrund weiter wachsender Bedrohungen, dringend den Aufbau von Resilienz gegen Desinformationskampagnen an.

3. Fazit

Insgesamt wird aus den in diesem Band zusammengeführten Beiträgen deutlich: Die Bedrohungslage in der Domäne der Information ist real und mannigfaltig. Die Bedrohung selbst ist auf die innere Kohäsion unserer freiheitlichen Gesellschaft gerichtet. Eine wirksame Antwort auf diese Bedrohung, gerade auch im Sinne der Wehrhaftigkeit unserer Demokratie, muss an der Stärkung dieser Kohäsion ansetzen. Der Aufbau von Resilienz schützt diese Kohäsion, ist aber nur ein passives Instrument und muss durch (pro-)aktive Strategien ergänzt werden. Dies bedeutet letztendlich, mithilfe attraktiver narrativer Deutungsangebote die Kraft von Desinformationskampagnen zu brechen. Die Notwendigkeit von Kommunikation und deren Neubewertung im Sinne der skizzierten Akzentuierung dieses Begriffs ist heute dringender als je zuvor.

Hybride Bedrohungen im Informationsumfeld

Herausforderung für die deutsche Sicherheitspolitik im 21. Jahrhundert

Stefan Gruhl, Christian Bell,
Falko Hark, Philipp Huber
und Lion König

01 Die Zunahme hybrider Bedrohungen in den letzten zwei Jahrzehnten lässt auf einen Paradigmenwechsel im Vorgehen sowohl staatlicher als auch nichtstaatlicher Akteure schließen. Begünstigt durch politische, technische und gesellschaftliche Entwicklungen können gegnerische Akteure im digitalen Zeitalter lokal unabhängig und verschleiert wirken. Durch die gezielte Manipulation gesellschaftlicher Diskurse kann bspw. das Erreichen wirtschaftlicher, politischer oder militärischer Ziele unterstützt werden, ohne die eigenen territorialen Grenzen physisch zu verlassen. Die perspektivische Zunahme derartiger hybrider Bedrohungen in Qualität und Quantität impliziert die Notwendigkeit einer gesamtstaatlichen Sicherheitsarchitektur, die nicht nur eine Abwehrfähigkeit abbildet. Es bedarf ebenso präventiver Potenziale, die etwa den Aufbau einer entsprechenden Resilienz fördern. Darüber hinaus scheint die institutionelle Trennung zwischen Innerer und Äußerer Sicherheit hinsichtlich der Möglichkeiten gegnerischer Akteure zum orchestrierten, dislozierten Einsatz direkt und indirekt wirkender Potenziale nicht mehr zeitgemäß. Vielmehr verlangen derartige mehrdimensionale Bedrohungen nach gesamtstaatlichen Ansätzen, die sowohl in der Analyse als auch im Aufbau von Resilienz ressortübergreifend angelegt und multinational abgestimmt sind.

Das sicherheitspolitische Umfeld 2.0

In der multipolaren Weltordnung des 21. Jahrhunderts sieht sich die deutsche Sicherheitspolitik neuen Formen konfliktärer Machtprojektion gegenüber. Die völkerrechtswidrige Annexion der Krim durch Russland im März 2014 verdeutlichte, dass Kriege und kriegerische Auseinandersetzungen nicht nur durch das Militär geführt werden.

> „Gerade die vergangenen Jahre haben gezeigt, wie bei der hybriden Kriegführung militärische und nichtmilitärische Aktivitäten kombiniert werden. Und bei Weitem nicht nur auf das gegnerische Militär zielen. Sondern vor allem auch eines wollen: Die Gesellschaft eines Landes oder eines Bündnisses destabilisieren."[1]

Diese Formulierung des Bundesministeriums der Verteidigung ist zweifelsohne auch als eine Reaktion auf das Verhalten Russlands zu verstehen, das zunehmend als Aggressor wahrgenommen wird. Die strategische Absicht Russlands, die diesem Verhalten zugrunde liegt, wird vielfach mit der sogenannten Gerasimov-Doktrin in Verbindung gebracht. Sie geht zurück auf den Generalstabschef der Russischen Föderation, Valery Gerasimov, der Ende Januar 2013 in einer Rede vor der Russischen Akademie der Militärwissenschaften unterstrich, dass in Konflikten politische, ökonomische, kommunikative, humanitäre und andere nicht-militärische Maßnahmen in Verbindung mit dem Protestpotenzial der Bevölkerung der Zielländer zum Einsatz kommen und zunehmend wichtiger als „konventionelle Feuerkraft" würden.[2] Obwohl umstritten ist, inwieweit dies die tatsächliche Grundlage russischen militärischen Handelns darstellt[3], so hat das Vorgehen in der Ukraine bestätigt, dass Russland gesamtstaatlich und auf allen von Gerasimov angeführten Feldern agiert. Zudem unterstrich dieser in einer Rede zur Militärstrategie seines Landes im März 2019, dass

es Veränderungen der militärischen Bedrohung gebe und die Auseinandersetzung im Informationsumfeld[4] immer mehr an Bedeutung gewinne.[5]

Die Bedeutungsverlagerung von der weitgehend konventionellen zur verstärkt hybriden Bedrohung wird auch in Sicherheitskreisen der EU und NATO wahrgenommen.

Bereits 2016 hat die Europäische Kommission einen „Gemeinsamen Rahmen für die Abwehr hybrider Bedrohungen"[6] aufgestellt, im Zuge dessen eine „Hybrid Fusion Cell" innerhalb des Europäischen Auswärtigen Dienstes (EU External Action Service, EEAS) eingerichtet wurde. Aufgabe dieser Zelle ist es, hybride Bedrohungen, die gegen die EU gerichtet sind, zu analysieren. Auch die NATO hat auf die veränderte Bedrohungslage reagiert: in ihrer „Londoner Erklärung" (2019) betonten die Staats- und Regierungschefs der NATO-Mitgliedstaaten die Gefahr, die von Cyberangriffen und hybriden Bedrohungen ausgeht und beschlossen, ihre Sicherheitsarchitektur entsprechend anzupassen[7]. Dementsprechend sehen zahlreiche Strategiepapiere und Grundlagendokumente der EU- und NATO-Staaten in der hybriden Kriegführung eine der größten sicherheitspolitischen Herausforderungen des 21. Jahrhunderts.[8]

Obwohl hybride Bedrohungen kein grundsätzlich neues Phänomen sind, erhalten sie im digitalen Zeitalter durch verstärkt auftretende Cyberangriffe, Informationsoperationen und Propaganda eine neue Qualität in ihrem Bedrohungspotenzial.

Der zielgerichtete und synchronisierte Einsatz von unterschiedlichen Machtpotenzialen, die Dengg und Schurian (2015) in Hard Power und Soft Power kategorisieren, setzt Akteure voraus, die über ein derartiges Portfolio verfügen und dieses gegen einen Zielstaat oder eine Organisation zur Erreichung der strategischen Absicht einzusetzen bereit sind.[9]

Das „Weißbuch der Bundesregierung" aus dem Jahr 2016 stellt hierzu fest, dass eine solche mehrdimensionale Machtprojektion gegnerischer Akteure eine gesamtstaatliche Antwort erfordert.[10] Insofern defi-

nieren Schaurer und Ruff-Stahl (2016) aus militärischer Sicht hybride Bedrohungen als den „planvolle[n], mithin nichtlineare[n] Einsatz unterschiedlicher Fähigkeiten über das gesamte DIMEFIL-Spektrum[11] hinweg mit dem Ziel, politische Wirkung unterhalb der Schwelle eines bewaffneten Angriffs zu erzielen und die Handlungs- und Reaktionsfähigkeit des Gegners zu beeinträchtigen."[12]

Da derartige gegnerische Akteure zudem die Schwelle eines „offenen" militärischen Konflikts möglichst zu vermeiden suchen, ist eine Fokussierung auf nicht primär militärische Ziele naheliegend. Diese Definition unterstreicht damit den umfassenden Charakter der hybriden Aktion, dem nicht allein mit militärischen Mitteln, sondern nur gesamtstaatlich begegnet werden kann. Hinzu kommt, dass sich die Attribuierbarkeit einzelner Phänomene oftmals als kaum möglich erweist und daher auch nicht als strategisches Handeln eines spezifischen Akteurs erkannt wird.

Es ist somit nicht nur die Vermischung von Elementen der regulären und irregulären Kriegführung, die den eigentlichen „Charakter des Hybriden" ausmacht. Vielmehr ist es ein mehrdimensionales verdecktes Agieren, das die „Zuschreibung einzelner Gewalthandlungen und Beiträge zur Kriegführung im Unklaren lässt."[13] Treffender ließe sich also von „verdeckter Kriegführung"[14] sprechen, was für den Angegriffenen sowohl die Analyse als auch die Bekämpfung hybrider Aktionen erschwert.[15]

Die wesentliche Herausforderung für Staaten wie die Bundesrepublik Deutschland, die Ziel hybrider Bedrohungen sind, besteht also darin, diese „in ihrer gesamten Bandbreite zu erkennen und geeignete, akkordierte Gegenmaßnahmen einzuleiten."[16] Damit wird bestätigt, dass im Rahmen gesamtstaatlicher Sicherheitsvorsorge nicht die Fähigkeit zur Detektion einzelner Phänomene, sondern das Erkennen einer mehrdimensionalen Umsetzung der strategischen Absicht eines Akteurs die zentrale Herausforderung darstellt. Folglich muss diese Erkenntnis auch auf Frühwarnsysteme und deren zugrundeliegende Indikatoren übertragen werden.

Eine der Reaktionen der deutschen Bundesregierung auf die wachsenden Herausforderungen durch hybride Bedrohungen war die Cyber-Sicherheitsstrategie, die einen „ressortübergreifenden strategischen Rahmen“[17] darstellen soll, um Bedrohungen im Cyberraum frühzeitig erkennen und ihnen begegnen zu können. Das Strategiepapier fokussiert allerdings vorrangig auf die technische Sicherheit gegenüber Angriffen. Das Informationsumfeld wird dagegen kaum adressiert, auch wenn dem Mittel der Desinformation in hybriden Bedrohungsszenarien ein hohes Gefährdungspotenzial zuerkannt wird.[18]

Die Essenz der Cyber-Sicherheitsstrategie wie auch des Weißbuches bleibt jedoch, dass es nicht die *eine eindimensionale* hybride Bedrohung gibt, sondern Gegner mit einer strategischen Absicht verschiedene Elemente zur Gewaltanwendung und Machtprojektion miteinander verknüpfen und sich daraus unterschiedlichste hybride Bedrohungsszenarien ergeben können.[19] Hinsichtlich einer Kategorisierung potenzieller gegnerischer Akteure kann in diesem Kontext angenommen werden, dass staatliche Akteure wie Russland über ein vergleichbar breiteres und größeres Arsenal an Potenzialen verfügen als etwa nichtstaatliche Terrororganisationen wie der „Islamische Staat“. Anders als im Kalten Krieg stellt sich heute in Zeiten hybrider Phänomene im Rahmen einer gesamtstaatlichen Sicherheitsvorsorge daher viel mehr die Frage, von welchem potenziellen Gegner neben einer Gefahr der Gewaltprojektion auch eine konzertierte Projektion nichtmilitärischer, aber durchaus staatsgefährdender Machtausübung ausgehen kann.

Hybride Phänomene im Informationsumfeld

Versuche zur Manipulation gesellschaftlicher Diskurse sind bei allen Unterschieden in Strategie und Vorgehensweise ein wesentliches Merkmal hybrider Bedrohungen, die unterhalb der Schwelle von direkter Gewaltanwendung durch einen gegnerischen Akteur bleiben. Durch die Steuerung von Diskussionen in sozialen Netzwerken oder der Platzierung von manipulativen Informationen auf Nachrichtenseiten können potenziell „per Knopfdruck" ganze Bevölkerungsteile getäuscht, gespalten, polarisiert, abgelenkt oder im Sinne der eigenen Ziele mobilisiert werden. Dabei sind es nicht ausschließlich Desinformationen im Sinne von falschen bzw. unwahren Informationen, die durch gegnerische Akteure zur Manipulation der öffentlichen Meinung verwendet werden.[20] Ebenso sind es teilwahre oder durch den Zeitpunkt und Ort der Veröffentlichung gezielt irreführende Informationen, die im Rahmen eines Agenda Settings[21], einer meist subtilen thematischen Trendmanipulation innerhalb von Diskursen, die öffentliche Wahrnehmung und Einstellungen beeinflussen sollen.

Dem gesamten Spektrum hybrider Phänomene im Informationsumfeld kann eine besondere Rolle hinsichtlich hybrider Bedrohungen im Allgemeinen zugewiesen werden, da sie ihre Wirkung sowohl unabhängig von anderen derartigen Bedrohungen, als auch flankierend oder katalysierend als Multiplikator entfalten können.[22]

Zur Nutzung der „Wirkdimension" Informationsumfeld stehen gegnerischen – auch nichtstaatlichen – Akteuren zahlreiche Mittel zur Verfügung, um ihre Ziele zu erreichen. Der Sachverhalt, dass Informationskampagnen mit strategischem Entfaltungspotenzial sowohl umfassende technische und finanzielle Ressourcen als auch versierte Planungskapazitäten voraussetzen[23], deuten an, dass die Steuerung oder zumindest die Orchestrierung von Manipulationsversuchen der öffentlichen Meinung eher staatlichen Akteuren zuzuweisen ist. Während sich die Entwicklung von „einfachen"

Social Bots bereits mit rudimentären Programmierkenntnissen durch wenig potente Akteure umsetzen lässt, setzen strategisch handelnde Akteure häufig auf anspruchsvollere und schwerer detektierbare Mittel wie Trolle oder sogenannte Hybride bzw. Cyborgs.[24] Die manipulative Einflussnahme der von Russland gesteuerten sogenannten Internet Research Agency (die auch als „Troll-Fabrik" bezeichnet wird) auf Diskurse in der westlichen Welt ist bereits durch diverse Studien belegt[25]. Die regelmäßige Unterstützung manipulativer Informationskampagnen durch professionelle Nachrichtenseiten[26] erhärtet den Verdacht einer staatlichen Orchestrierung.

Hauptargumente zur Nutzung von digitalen und sozialen Medien/Plattformen zur Manipulation von gesellschaftlichen Diskursen sind sowohl die Möglichkeit des dislozierten Wirkens als auch die Gewährleistung der Anonymität und die damit einhergehende Verschleierung der Urheberschaft. Technische Entwicklungen im Bereich der Sprach- und Textverarbeitung sowie Bildbearbeitung werden die Verschleierung perspektivisch expansiv erleichtern[27] und so die Gefahr für demokratische und pluralistische Gesellschaften exponentiell erhöhen. Die Vorstellung, welche nachhaltigen und strategischen Konsequenzen ein professionell erstelltes und am Vorabend einer Wahl viral verbreitetes Deepfake-Video[28] eines politischen Amtsträgers oder einer politischen Amtsträgerin haben könnte, vermag das Gefährdungspotenzial derart professioneller Desinformation anzudeuten. Aktuelle Forschungsergebnisse legen nahe, dass unterschiedliche Wirkmittel bereits heute verwendet werden, um manipulativ in demokratische Prozesse einzugreifen.[29]

Die verschwimmenden Grenzen zwischen Innerer und Äußerer Sicherheit, die v. a. für das Informationsumfeld unbestreitbar sind, werden vermutlich bewusst durch gegnerische Akteure als „Einfallstor" missbraucht. Dies erschwert es den einzelnen staatlichen Sicherheitsbehörden, die Verbindung zwischen einem Akteur im Ausland mit einer von ihm erzielten Wirkung im Inland herzustellen und derartigen Bedrohungen zielführend zu begegnen.[30]

Nichtstaatliche Institutionen wie die gemeinnützige Organisation Correctiv[31] oder Unternehmen wie Facebook[32] befassen sich bereits systematisch und z. T. international vernetzt mit solchen primär desinformativen Phänomenen. Im Zuge einer gesamtstaatlichen Sicherheitsvorsorge erfolgt dies in Deutschland eher institutionell abgegrenzt, um den Zuständigkeiten für Innere und Äußere Sicherheit sowie dem Spannungsfeld von Sicherheit und Überwachung der eigenen Bevölkerung zu genügen.[33] Die Frage, wie und wo hybride Phänomene im Informationsumfeld etwa als Teil einer mehrdimensionalen gegnerischen Vorgehensweise durch staatliche Sicherheitsorgane erkannt, bewertet und in ein ressortübergreifendes Lagebild als Entscheidungsgrundlage für staatliches Handeln zusammengeführt werden, scheint daher nicht abschließend beantwortet zu sein. Gleiches ist in diesem Kontext auch für die internationale Vernetzung Deutschlands anzunehmen.

Resilienz

Wirksames Begegnen von hybriden Phänomenen im Informationsumfeld kann nicht auf das Detektieren und Durchführen von reaktiven Gegenmaßnahmen begrenzt sein. Wie die nationale Cyber-Sicherheitsstrategie von 2016 der Bundesregierung feststellt, sind v. a. präventive und damit proaktive Maßnahmen erforderlich, um eine gewisse „Grundimmunisierung" einer Gesellschaft gegen die Wirksamkeit von manipulativen hybriden Einflüssen zu erreichen. Diese wäre etwa dann gegeben, wenn eine Gesellschaft durch die Information über das Vorhandensein ebensolcher Phänomene informiert ist und entsprechende Schlüsselkompetenzen[34] für eine kognitive Widerstandsfähigkeit und Resilienz[35] etabliert sind. Das Strategiepapier beschränkt sich in den darin genannten „vier Handlungsfeldern"[36] allerdings nahezu ausschließlich auf den technischen Aspekt von Resilienz. Ein „sicheres und selbstbestimmtes Handeln in einer digitalisierten Umgebung"[37] bedeutet jedoch mehr als den handlungssicheren Umgang mit technischen Endgeräten sowie deren Schutz. Vielmehr impliziert Resilienz im Verständnis hybrider Bedrohungen im Informationsumfeld auch die Fähigkeit zur kritischen Bewertung von Inhalten.

Dass eine erhöhte Medienkompetenz zur Steigerung der kognitiven Resilienz einer Gesellschaft führen kann, zeigt das Beispiel Finnlands in der Begegnung russischer manipulativer Informationsoperationen. Die für die finnische Gesellschaft festgestellte hohe Resilienz gegenüber extern initiierten Versuchen zur Manipulation der öffentlichen Meinung wird dort weitgehend auf das gute Bildungssystem zurückgeführt.[38] „Egal ob Studenten und Schüler, Lehrer, Journalisten oder auch Politiker – jeder in Finnland lernt, wie man falsche von tatsächlichen Nachrichten unterscheiden kann."[39] Die Feststellung, dass ältere Menschen häufiger Fake News verbreiten[40], unterstützt die Überlegung, dass Medienkompetenz ebenso einen festen Platz in der Erwachsenenbildung verdient. In der Bundesrepublik Deutschland wäre in diesem Kontext bspw. die politische Bildung in den Streitkräften nicht nur in Hinblick auf die Mündigkeit der Soldatinnen und Soldaten als Staatsbürgerinnen und Staatsbürger in Uniform,

sondern auch auf eine kognitive Resilienz gegenüber Manipulationsversuchen im Informationsumfeld zu sehen.

Die zunehmende Kritik an wissenschaftlichen Erkenntnissen sowie das schwindende Vertrauen in etablierte Informationsquellen[41] zeigen, vergleichbar mit der im Rahmen der Cyber-Sicherheitsstrategie beschriebenen „kritischen Infrastruktur", die zentrale Rolle von Medien sowie Journalistinnen und Journalisten für die allgemeine Meinungsbildung. Schon jetzt leisten sie mit verschiedenen Verifizierungsangeboten oder „Faktenchecks"[42] gesellschaftliche Aufklärungsarbeit. Dennoch scheint auch hier in den vergangenen Jahren ein Vertrauensverlust eingesetzt zu haben: Stand 2020 halten ca. 30 Prozent der Deutschen sogenannte Verschwörungsmythen für glaubwürdig.[43]

Ein entsprechendes „Gefährdungspotenzial" lässt sich u. a. an den immer öfter stattfindenden Protestkundgebungen ablesen. Eine dabei geäußerte grundlegende Skepsis gegenüber Institutionen der Bundesrepublik Deutschland muss als Einfallstor für gegnerische Akteure wahrgenommen werden, die eine Destabilisierung oder Spaltung der Gesellschaft für eigene Ziele instrumentalisieren.

Die Verbesserung der kognitiven Resilienz einer Gesellschaft darf daher nicht nur auf Rezipienten von Informationen begrenzt sein. Insbesondere das Phänomen der indirekt wirkenden Trendmanipulation lässt einen Schluss zu: Personen mit einem aktiven Anteil am Meinungsbildungsprozess sollten in Bezug auf ihre mögliche Instrumentalisierung durch gegnerische Akteure sensibilisiert werden.

Thesen

Die dargestellten zunehmenden Herausforderungen durch hybride Bedrohungen in der vernetzten und digitalen Gesellschaft des 21. Jahrhunderts offenbaren Defizite in Bezug auf ein systematisches, institutionelles Vorgehen zur Analyse und zur Begegnung hybrider Bedrohungen im Informationsumfeld. Hierzu werden für den weiteren wissenschaftlichen Diskurs folgende drei Thesen abgeleitet.

These 1: Das Begegnen hybrider Bedrohungen mit gesamtstaatlicher Relevanz erfordert einen akteurbasierten und ressortübergreifenden Ansatz.

Das strategische Vorgehen gegnerischer Akteure und die dafür genutzten Mittel zur Machtprojektion müssen ganzheitlich erfasst werden, um das Zusammenwirken von Maßnahmen in verschiedenen Dimensionen erkennen zu können. Dies erfordert klare Zuständigkeiten mit institutionellen Übergabepunkten sowie ein ressortübergreifendes steuerndes Element. Eine Trennung zwischen Innerer und Äußerer Sicherheit ist im Kontext hybrider Bedrohungen nicht mehr zeitgemäß und bedarf einer Neubewertung, u. a. auch der institutionellen Zuständigkeiten staatlicher Sicherheitsorgane.

Erst eine akteurbasierte Analyse hybrider Bedrohungen ermöglicht eine qualitative Bewertung von Einzelphänomenen mit Blick auf eine gesamtstaatliche Sicherheitsrelevanz.

These 2: Zukünftige Sicherheitsarchitekturen und sicherheitspolitische Konzepte werden nicht an der Kompatibilität mit staatlicher Aufgabenteilung und Zuständigkeiten zu messen sein, sondern wie wirksam sie auf hybride mehrdimensionale Bedrohungen ausgerichtet sind.

Feindliche Akte gegen einen Staat dürfen nicht primär als Anwendung von unmittelbarer Gewalt durch einen gegnerischen Akteur verstanden werden. Dementsprechend sollten staatliche Gegenmaßnahmen ebenso wenig eindimensional und ressortspezifisch limitiert verstanden werden.

Westliche Demokratien bieten aufgrund ihrer offenen und pluralistischen Gesellschaften – und der damit einhergehenden schützenswerten Meinungs- und Pressefreiheit – eine besonders große Angriffsfläche für hybride Bedrohungen im Informationsumfeld. Das sachkundige Auswerten, Verstehen und Nutzen dieser verschiedenen Medienangebote muss deshalb integraler Bestandteil von Bildung sein. Die Existenz hybrider Phänomene im Informationsumfeld muss als gegeben verstanden werden, um den vermeintlichen Wahrheitsgehalt verschiedener Informationen kritisch reflektieren zu können.

Die öffentlich-rechtlichen Medien sind in diesem Kontext dahingehend zu bewerten, inwieweit der Medienstaatsvertrag als Teil staatlicher Anstrengungen zur kognitiven Resilienzbildung dient.

These 3: In einer globalisierten Welt muss Deutschland institutionelle Lösungsansätze zur Begegnung hybrider Bedrohungen auf nationaler und multinationaler Ebene finden.

Zur Begegnung hybrider Bedrohungen scheint eine strukturelle Nachjustierung der betroffenen staatlichen Institutionen geboten, für die das bestehende Nationale Cyber-Abwehrzentrum als ressortübergreifendes steuerndes Element herangezogen werden könnte. Auch denkbar wäre die Einrichtung einer Institution vergleichbar der eines Nationalen Sicherheitsberaters nach US-amerikanischem Vorbild[44] – eine zentrale Stelle, welche die Arbeit verschiedener Sicherheitsorgane koordiniert und die Regierung in Fragen der nationalen Sicherheit berät.

Neben einer national ausgerichteten Steuerung dieser Aufgabe muss gleichermaßen eine institutionalisierte Zusammenarbeit in multinationalen Organisationen wie der EU und NATO etabliert werden. Die Bündelung bereits vorhandener Fähigkeiten gilt es dabei ebenso vorzunehmen, wie die Abstimmung des Aufbaus neuer Fähigkeiten. Den Willen zum Teilen sensitiver Informationen vorausgesetzt, gilt es, diese Entwicklungen aus nationaler Sicht proaktiv mitzugestalten, um mehrdimensionalen hybriden Bedrohungen gemeinsam begegnen zu können.

1 Bundesministerium der Verteidigung 2020. Auftrag: Landes- und Bündnisverteidigung (Berlin: BMVg), S. 14.

2 Siehe hierzu auch: Hanna Grininger und Christoph Biban 2019. „Die ‚Gerasimov-Doktrin' und die russischen Militärwissenschaften", in: Military Power Revue der Schweizer Armee, Nr. 1, S. 13–28.

3 Unter Verteidigungsexpertinnen und -experten herrscht Uneinigkeit darüber, inwieweit es sich bei der Aussage um eine „Doktrin" im engeren Sinne handelt. So argumentiert Gregor von Kursell in der Zeitschrift für Innere Führung, dass sich Gerasimov mit seiner Aussage nicht auf die Ausrichtung der künftigen russischen Kriegführung bezieht. Vielmehr verweise er auf den potenziellen Gegner, ‚den Westen', der solche Methoden im Rahmen der sogenannten ‚farbigen Revolutionen' schon lange anwende. Vgl. Gregor von Kursell (2018) „Berufsarmee oder Massenheer? Die russischen Streitkräfte zwischen Reform und Tradition" in IF *Zeitschrift für Innere Führung*, Nr. 4, S. 5.

4 Das Informationsumfeld wird als der Anteil des Cyber- und Informationsraums verstanden, in dem Informationen zur Meinungsbildung aufgenommen, verarbeitet und weitergegeben werden. Aus militärischer Sicht ist es der Handlungsraum, in dem Truppenführerinnen und Truppenführer mit Informationen die Wahrnehmung sowie die Einstellung von anderen Akteuren gezielt zu Zwecken des Operationserfolgs beeinflussen.

5 Entwicklungsrichtungen der Militärstrategie. Rede des Chefs des Generalstabes der Streitkräfte Russlands zur Jahresversammlung 2019 der Akademie der Militärwissenschaften der Russischen Föderation, am 2.3.2019, in: Rainer Böhme (Hrsg.) 2019. Dialog und Abschreckung versus Entmilitarisierung: Zum sicherheitspolitischen Denken im Generalstab der Streitkräfte Russlands, dgksp-diskussionspapiere, S. 10–23.

6 Europäische Kommission 2016. Joint Framework on Countering Hybrid Threats: A European Union Response https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52016JC0018&from=en (letzter Zugriff: 15.12.2020).

7 NATO 2019. Londoner Erklärung. https://www.nato.int/cps/en/natohq/official_texts_171584.htm?selectedLocale=en (letzter Zugriff: 13.12.2020).

8 Siehe EU Strategic Agenda, 2019–2024. https://www.consilium.europa.eu/en/eu-strategic-agenda-2019-2024/ (letzter Zugriff: 15.12.2020). U. K. Ministry of Defence. 2015. Strategic Trends Programme: Future Operating Environment 2035. Sowie: Turkish National Defense University 2017. Shifting Paradigm of War: Hybrid Warfare (Hrsg. Yücel Özel und Ertan Inaltekin). Bundesministerium

der Verteidigung 2019. Steuerung der Zukunfts- und Weiterentwicklung in der Bundeswehr: Future Operating Environment 2035.

9 Anton Dengg und Michael Schurian (Hrsg) 2015. Vernetzte Unsicherheit: Hybride Bedrohungen im 21. Jahrhundert (Wien: Landesverteidigungsakademie), S. 69.

10 Bundesministerium der Verteidigung 2016. Weißbuch zur Sicherheitspolitik und zur Zukunft der Bundeswehr (Berlin: BMVg), S. 38.

11 Das Akronym DIMEFIL steht für Diplomatic [Political], Information, Military, Economic, Financial, Intelligence, Legal. Es schließt also alle wesentlichen staatlichen und nichtstaatlichen Bereiche und Institutionen einer modernen Gesellschaft mit ein.

12 Florian Schaurer und Hans-Joachim Ruff-Stahl 2016. „Hybride Bedrohungen: Sicherheitspolitik in der Grauzone“ (Bonn: Bundeszentrale für Politische Bildung), S. 3. Die Autoren definierten den Begriff in ihrer Funktion als Referenten im Bundesministerium der Verteidigung.

13 Wolfgang Schreiber 2016. Der Neue Unsichtbare Krieg? Zum Begriff der ‚hybriden‘ Kriegführung (Bonn: Bundeszentrale für politische Bildung), S. 6.

14 Ebd.

15 Siehe auch: Sean Monaghan 2019. Countering Hybrid Warfare: Conceptual Foundations and Implications for Defence Forces, in: PRISM 8, No. 2, S. 82–98. Monaghan betont die Schwierigkeit, hybriden Bedrohungen entgegenzutreten: „hybrid threats are designed to prevent decisive responses in the first place. This makes detection more important, and countering more difficult“, S. 90.

16 Dengg/Schurian 2015, S. 75.

17 Bundesministerium des Innern 2016. Cyber-Sicherheitsstrategie für Deutschland (Berlin: BMI), S. 5.

18 Ebd. S. 7.

19 Vgl. Schreiber 2016, S. 8.

20 BMI 2016. Cyber-Sicherheitsstrategie, S.7.

21 Agenda Setting umfasst im Verständnis dieses Artikels die gesteuerte Platzierung und Verbreitung von Informationen zur thematische Schwerpunktsetzung innerhalb von Diskursen. Die adressierten Themen haben häufig lediglich indirekt mit dem eigentlichen Diskurs zu tun, sind jedoch durch eine „emotionale Ladung“ geeignet, um die Diskursteilnehmerinnen und Diskursteilnehmer zu spalten oder vom eigentlich diskursrelevanten Thema abzulenken.

22 Vgl. Dengg/Schurian 2015, S. 71.

23 Tabea Wilke 2020. Informationsbedrohungen – Herausforderungen

für den europäischen Informationsraum (München: Hanns-Seidel-Stiftung e. V.), S. 19.

24 Nir Grinberg, Kenneth Joseph, Lisa Friedland, Briony Swire-Thompson und David Lazer 2019. Fake News on Twitter during the 2016 U. S. Presidential Election https://science.sciencemag.org/content/363/6425/374.full (letzer Zugriff: 27.10.2020).

25 Vgl. Renee Di Resta et al. 2018. The Tactics & Tropes of the Internet Research Agency. New Knowledge (https://cdn2.hubspot.net/hubfs/4326998/ira-report-rebrand_FinalJ14.pdf) sowie Alexander Spangher et al. 2018. „Analysis of Strategy and Spread of Russia-sponsored Content in the US in 2017" https://arxiv.org/abs/1810.10033 (letzer Zugriff: 10.12.2020).

26 Wilke 2020, S. 46.

27 Ebd. S.12.

28 Unter einem Deepfake-Video wird in diesem Kapitel ein durch Künstliche Intelligenz manipuliertes Video verstanden, bei dem bspw. auf einer Videoaufnahme das Gesicht von Person A durch das Gesicht von Person B „ersetzt" wird (vgl. Face-Swap). Für die Betrachterin oder den Betrachter scheint es, dass die Videoaufnahme Person B zeigt.

29 Vgl. Grinberg et al. 2019. Fake News on Twitter during the 2016 U. S. Presidential Election, in: Science, 363, S. 374–378, sowie: DiResta et al. 2018.

30 Als Beispiel hierfür sei die Frage nach der Zuständigkeit hinsichtlich der manipulativen Einflussnahme durch einen ausländischen Akteur in deutschsprachigen Diskursen auf deutschsprachigen Plattformen genannt.

31 www.correctiv.org. (letzer Zugriff: 10.12.2020).

32 Jen Weedon, William Nuland und Alex Starnos 2017. Information Operations and Facebook (Menlo Park: Facebook Inc.) sowie: Nathaniel Gleicher 2019. Removing More Coordinated Inauthentic Behavior From Iran and Russia. (Menlo Park: Facebook Inc.) https://about.fb.com/news/2019/10/removing-more-coordinated-inauthentic-behavior-from-iran-and-russia/ (letzter Zugriff: 10.12.2020).

33 Vgl. Henning Lahmann und Phillipp Otto 2020. Kriminalität, Sicherheit und Freiheit, in: Informationen zur politischen Bildung 344, (Bonn: Bundeszentrale für Politische Bildung) S. 57.

34 Vgl. Wilke 2020, S. 49.

35 Resilienz wird in diesem Kapitel als die Fähigkeit von Gesellschaften verstanden, externe Störungen zu verkraften, ohne dass sich ihre wesentlichen Systemfunktionen ändern. Vgl. Sabine Blum, Martin

Endreß, Stefan Kaufmann, Benjamin Rampp 2016. Soziologische Perspektiven, in: Rüdiger Wink (Hrsg.): Multidisziplinäre Perspektiven der Resilienzforschung. (Wiesbaden: Springer VS), S. 151–177.

36 Vier Handlungsfelder der Cyber-Sicherheit 1.) Sicheres und selbstbestimmtes Handeln in einer digitalisierten Umgebung 2.) Gemeinsamer Auftrag Cyber-Sicherheit von Staat und Wirtschaft 3.) Leistungsfähige und nachhaltige gesamtstaatliche Cyber-Sicherheitsarchitektur 4.) Aktive Positionierung Deutschlands in der europäischen und internationalen Cyber-Sicherheitspolitik.

37 BMI 2016. Cyber-Sicherheitsstrategie, S. 9.

38 Reid Standish. 2017. „Why Is Finland Able to Fend Off Putin's Information War?", in: Foreign Policy, 01. März https://foreignpolicy.com/2017/03/01/why-is-finland-able-to-fend-off-putins-information-war/ (letzter Zugriff 10.12.2020).

39 Carsten Drees 2019. „Finnland macht vor, wie man den Kampf gegen Fake-News gewinnt". https://www.mobilegeeks.de/artikel/finnland-macht-vor-wie-man-den-kampf-gegen-fake-news-gewinnt/ (letzter Zugriff: 10.12.2020).

40 Andrew Guess, Jonathan Nagler und Joshua Tucker 2019. „Less than you think: Prevalence and Predictors of Fake News Dissemination on Facebook", in: Science Advances, 5 (1), S. 1–8.

41 Mazarr, Michael J. et al. 2019. The Emerging Risk of Virtual Societal Warfare: Social Manipulation in a Changing Information Environment (Santa Monica: RAND Corporation).

42 Vgl. https://www.correctiv.org (letzter Zugriff: 10.12.2020).

43 Jochen Roose 2020. Sie sind überall: Eine repräsentative Umfrage zu Verschwörungstheorien. (Berlin: Konrad-Adenauer-Stiftung e. V.).

44 In den USA ist der Nationale Sicherheitsberater der Assistent des Präsidenten für alle Belange der nationalen Sicherheit https://de.usembassy.gov/de/welche-aufgaben-hat-ein-nationaler-sicherheitsberater/ (letzter Zugriff: 10.12.2020). Die Aufgaben und Befugnisse gehen dabei weit über die des deutschen Beauftragten für die Nachrichtendienste des Bundes sowie des Koordinators der Nachrichtendienste des Bundes hinaus.

Auftrags-kommunikation im Dienst

Worüber sprechen wir, wenn wir von Sicherheitspolitik sprechen?

Jürgen Schulz

02 Der Beitrag definiert die konstitutive Rolle der Kommunikation für Institutionen und Organisationen. Die Frage nach Existenzberechtigung und Auftrag beantwortet die Auftragskommunikation. Strategischer Ansatz ist die Selbstvergewisserung. Diese unterscheidet die sachliche, soziale und zeitliche Sinndimension als Gestaltungsgrundlage. Sicherheitspolitik ist (wie jede Politik) Kommunikation!

Hard Power vs. Soft Power

Öffentlichkeitsarbeit, Informationsarbeit, Public Relations, Media Relations, Social Media Relations – wer kennt die Disziplinen und nennt die Namen des Instrumentariums strategischer Kommunikation? Üblicherweise wird dabei unterschieden zwischen Hard Facts und softer Kommunikation.

„Politik ist Kommunikation" schreibt Dirk Baecker (2018: 97) über „Politik im Schatten des Krieges" (ebd.: 95). Clausewitz' Einschätzung vom Krieg als „bloße Fortsetzung der Politik mit anderen Mitteln" folgend, wird Kommunikation damit zum Gegenstand militärischer Überlegungen. Die epochalen Entwicklungen digitaler Medien lassen den Schluss zu, dass durch Informationstechnologie ermöglichte Cyberwars eine Fortsetzung des Krieges mit anderen Mitteln sind.

Problemorientierung kennzeichnet die Haltung dieses Beitrags. Im Gegensatz dazu agiert die Politik tendenziell zweck- bzw. lösungsversessen. Dabei ist die Aufgabe der Wissenschaft in Erinnerung an Decartes' Diktum „Dubito, ergo cogito" (Ich zweifele, also denke ich) v. a., vermeintlich gültige Annahmen infrage zu stellen.

Der Beitrag klärt über ein anderes Verständnis institutioneller Kommunikation auf und formuliert dazu einen möglichen Handlungsrahmen: „Die Maxime lautet: Kommunikation ist für Unternehmen und Institutionen konstitutiv und gestaltend, nicht instrumentell." (Schulz/Galling-Stiehler/Müller 2020: XIII)

Dabei geht es um „die Rolle der Selbstvergewisserung" (ebd.) der eigenen Existenzberechtigung. Worüber sprechen wir also, wenn wir über Verteidigung, Bedrohung etc. sprechen? Zur Beantwortung dieser Frage taugt bspw. das Modewort Purpose wenig. Statt um das „Why" geht es vielmehr um das „What".

Sicherheit als Problem

Für die Ex-Innenminister Otto Schily (SPD) und Hans-Peter Friedrich (CSU) war Sicherheit erklärtermaßen ein „Supergrundrecht" der Verfassung. Für das Zukunftsinstitut gehört Sicherheit aktuell zu den zwölf Megatrends. Die dazugehörige Illustration einer „Megatrend-Map" ist gestaltet wie ein Nahverkehrsliniennetz mit Stationen, die verschiedene Aspekte des Trends abbilden sollen. Auf der Megatrendlinie Sicherheit wirkt nur die Haltestelle „Cybercrime" bedrohlich. Um andere Unannehmlichkeiten wie Pandemien, Klimawandel, Flüchtlingsströme oder digitaler Transformation fährt die Trendlinie Sicherheit einen großen Bogen. Entsprechend beschreibt die Landeszentrale für Politische Bildung Baden-Württemberg (2019) „Sicherheit […] als Abwesenheit einer existenziellen Bedrohung […]."

Dabei ist Sicherheit eigentlich ein Phänomen der Vormoderne. Der Mensch konnte sich sicher sein, dass die substanziellen Entscheidungen in der Macht höherer Instanzen lagen. Es gab Orakel und Prophezeiungen, deren Nichteintreten den Glauben daran kaum infrage stellten. Ungläubigkeit und Unglaubwürdigkeit waren frevelhaft.

„Dass in den Kirchen gepredigt wird, macht deswegen die Blitzableiter auf ihnen nicht unnötig […]" notiert der erste deutsche Professor für Experimentalphysik Georg Christoph Lichtenberg 1796 in sein „Sudelbuch". Zu diesem Zeitpunkt sind die Seemächte Italien, Spanien und England längst mit einem Ersatzkonzept für Sicherheit unterwegs. Risiko ist lateinischen Ursprungs („risicare") und bereits zu finden in italienischen Handelsdokumenten des 12. und 13. Jahrhunderts im Zusammenhang mit dem Umschiffen von Klippen. Sicher ist nur, was gewesen ist. Für die Zukunft gibt es mehr oder weniger evidente Spekulationen, aber keine Sicherheit. Obendrein kann Sicherheit eine paradoxe Zielvorgabe sein. „Der [sichere] Hafen ist keine Alternative zum Schiffbruch; er ist der Ort des versäumten Lebensglücks", schreibt der Philosoph im Ausguck Hans Blumenberg (1979: 39). Das Gerede über Sicherheit gaukelt uns etwas vor,

was es nicht gibt. Die Frage ist also, wie mit Unsicherheiten zu verfahren ist. In der Organisations- und Entscheidungsforschung geht es deshalb auch um Unsicherheitsabsorption. Damit ist insbesondere die Fähigkeit lebender Systeme gemeint, sich auch im Angesicht einer riskanten, krisenhaften und sich wandelnden Umwelt selbst zu reproduzieren bzw. nicht unterzugehen.

Unsicherheitsabsorption durch Resilienz?

Resilienz ist die Hoffnungsvokabel und in den Strategiepapieren nicht nur der Sicherheitspolitik längst ein Thema. Der Begriff Resilienz (von lat. resilire: abprallen, zurückfedern oder nicht anhaften) stammt ursprünglich aus der Werkstoffwissenschaft. Dabei geht es um die Verformbarkeit und wie die Elastizität von Materialien der Verformung standhalten kann. Der Elastizitätsmodul ist der Materialkennwert, der das Verhältnis von Spannung und Dehnung bei der Verformung beschreibt.

Gesellschaftsfähig wurde die Idee der Resilienz aber v. a. in psychologischen Studien mit Kindern. Diese entwickeln überraschenderweise Fähigkeiten, traumatische Situationen unbeschadet für ihre weitere Entwicklung zu überstehen. Seit einem halben Jahrhundert steigen die Erwartungen an Resilienz als Allheilmittel bzw. Wunderwaffe der individuellen Krisenbewältigung.

Wo Trends entstehen, sind auch gegensätzliche Positionen nicht fern. Über das Trendthema Psychoanalyse schrieb Karl Kraus 1913: „Psychoanalyse ist jene Geisteskrankheit, für deren Therapie sie sich hält." Kraus' Kritik an dem damaligen Modethema Psychoanalyse ist humorvoll gedacht. Der Verweis ist v. a. eine Chiffre, denn Karl Kraus demonstriert damit die Umkehrung der üblichen Denkfigur von Ursache und Wirkung bzw. Mittel und Zweck. Eine vermeintliche Lösung wird zum Problem. Diese Umkehrung der Kausalität von Problem und Lösung charakterisiert auch die Debatten über Resilienz.

Zunehmend wird moniert, dass Resilienz krisenhafte bis katastrophale Zustände bereits unterstellen würde. Dass also die Folgen, nicht aber die Ursachen Gegenstand der Behandlung sind.

Dazu kommt der Vorwurf der individuellen Hinnahme, dass die Folgen individuell zu ertragen sind. Die Herausforderung für das Individuum bestünde dann darin, sich persönliche Eigenschaften anzutrainieren, „um Krankheiten, Verluste, Überbelastungen, Probleme im Privat- oder Berufsleben bessern meistern zu können" (Wellensieck/Galuska 2014: 23). Hans-Jürgen Arlt konstatiert entsprechend: „Anpassen und funktionieren sind Schlüsselwörter des Resilienzkonzepts" (Arlt 2016: 119). Der Resilienztrend wäre damit ein weiteres Indiz gesellschaftlicher Zerfallserscheinungen der Individualisierung bzw. Singularisierung. Arlt folgert provokant: „Aufstehen ohne Aufstand ist das Resilienz-Rezept" (Arlt 2016: 119). Überhaupt nimmt im Umgang mit krisenhaften Ausnahmesituationen der Eindruck zu, politische Akteure würden der Bearbeitung und Vermeidung der Ursachen weniger Aufmerksamkeit widmen, sich aus der Affäre ziehen und die Bürgerinnen und Bürger die salzige Suppe dann auslöffeln lassen.

Als Merkmal bzw. Prozess der Persönlichkeitspsychologie ist Resilienz berühmt, aber auch angreifbar geworden. Gleichzeitig beschäftigten sich andere Disziplinen mit Resilienz als Fähigkeit von Ökosystemen, Veränderungen erfolgreich zu absorbieren (vgl. Holling 1973). Resilience Engineering betrachtet Resilienz nicht als festgeschriebenes essentialistisches Merkmal, sondern als Prozess lebender Systeme im Umgang mit Störungen. Für das Resilience Engineering ist die Antizipation von Krisen ein erklärtes Ziel und damit auch die Fähigkeit, Ereignisse zu managen, bevor sie eingetreten sind. Dieser präventive Anspruch vertreibt vielleicht den Hautgout, Resilienz diene nur als Fitnessprogramm der individuellen Psyche im Umgang mit Katastrophen.

Resilience-Engineering erscheint zunächst wie alter Wein in neuen Schläuchen. Handelt es sich also nur um eine geschickte Wortwahl? Als Etikettierung erscheint Resilienz ansehnlicher als das Issues Management, das sich als weiche Kommunikationsdisziplin der Früherkennung und Behandlung konfliktärer Themen trotz ausgefeilter Methoden nie richtig hat durchsetzen können, weil es die Eigenheiten von Organisation und Management zu wenig berücksichtigt (vgl. Schulz 2001). Resilience Engineering dagegen, das ist der entscheidende Unterschied, fußt auf der

Eigentümlichkeit lebender Systeme und setzt an ihren Prozessen an. Für das Resilience Engineering ist Kommunikation konstitutiv und nicht wie beim Issues Mangement störender Faktor der Hard Facts.

In der Sicherheitspolitik bereitet die psychische Vulnerabilität Sorgen. Die Moral der Truppe und ggf. auch der Gesellschaft insgesamt steht unter kommunikativem Beschuss. Die intendierten Trefferwirkungen sind Irritation, Unsicherheit, Angst und Chaos. Die Frage ist, ob sich das Resilienzkonzept übertragen lässt auf Gesellschaften, Öffentlichkeit und öffentliche Meinungen ohne in längst diskreditierte Vorstellungen der Massenkommunikation und Massenpsyche zurückzufallen. Aber worüber sprechen wir eigentlich, wenn wir über Kommunikation als Bedrohung sprechen?

Kommunikation als Bedrohung und Waffe

„Die meisten Nachrichten sind falsch, und die Furchtsamkeit der Menschen wird zur neuen Kraft der Lüge und Unwahrheit. In der Regel ist jeder geneigt, das Schlimme eher zu glauben als das Gute" (von Clausewitz [1832–1834] 1980: 1. Buch, Kap. 6). Kommunikative Bedrohungslagen werden abstrakt und diffus erlebt. Die alltagsweltliche Vorstellung von Kommunikation als Informationsübertragungen wird solchen Herausforderungen nicht mehr gerecht. Es sei daran erinnert, dass die wissenschaftlichen Vorstellungen von Kommunikation als Informationsaustausch bzw. Nachrichtenübertragung stark durch die militärische Nutzung von Aufklärung und Auftrag motiviert wurden. Das Akronym Hi-Fi (High Fidelity) erinnert in der Unterhaltungselektronik noch an das Ziel einer originalgetreuen Signalübertragung.

Gegenwärtige Phänomene wie Desinformation, Fake News und alle mit der Vorsilbe „Cyber" markierten digitalen Irritationen setzen an dieser lebensweltlichen Vorstellung von Kommunikation als originalgetreuer Übertragung an, um sie letztlich ad absurdum zu führen.

Niklas Luhmann hat zum Kommunikationsbegriff in einem Disput mit Jürgen Habermas einen bemerkenswerten Satz geschrieben: „Es geht bei Kommunikationen demnach nicht um eine Verteilung von Beständen, sondern um eine Dosierung von Überraschungen" (Luhmann 1971: 43). Wie ist das zu verstehen?

Mit Beständen meint Luhmann, dass üblicherweise über fehlende Kommunikation, Daten und Information so gesprochen wird, als ob es Informationen gäbe, die man haben bzw. nicht haben könne. Diese materielle Vorstellung von Kommunikation verkennt, dass Kommunikation eine Selektionsleistung (vgl. Luhmann 1995) ist. Gregory Bateson macht an dieser Selektionsleistung die Spezifik des Informationsbegriffs

fest: „Was wir tatsächlich mit Information meinen – die elementare Informationseinheit – ist ein Unterschied, der einen Unterschied ausmacht“ (Bateson 1992: 582).

Trotzdem muss man sich fragen, wie konstruierte Scheinwelten und abstruseste Verschwörungsgeschichten im 21. Jahrhundert gesellschaftliche Resonanz finden können. Dazu muss man zunächst verstehen, dass auch Desinformation eine Form des Informiert-seins ist. „Wer den extrinsischen Einfluss als hinreichende Bedingung betrachtet, kann aus der Sprech- und Denkweise ‚ich informiere dich‘ jederzeit die nicht minder (unzu-)lässige Abkürzung ‚ich desinformiere dich‘ machen“ (Arlt et al. 2017: 220). Fake News, Lügen etc. erfüllen das Kriterium der Information, einen Unterschied zu machen, besonders gut. Desinformationen überraschen zunächst unsere Vorstellungen von der Wirklichkeit. Die Überraschung ereignet sich zweifach, nämlich nicht nur für Anhängerinnen und Anhänger im engeren Sinne, sondern auch für Beobachterinnen und Beobachter, die sich über ihre Mitmenschen wundern, die bestimmte Informationen selegieren.

Kommunikation im Zeitalter der Digitalisierung ist ein anschauliches Beispiel für Selektion. Soziale Netzwerke entscheiden über die Relevanz von Beiträgen nach dem Kriterium Meaningful Interaction. Je mehr Aufrufe, Comments, Shares und Likes sich häufen, desto relevanter selegiert der Algorithmus diese Beiträge. Nicht Inhalte, sondern Klickraten und Follower bestimmen die Relevanz und die Anschlusskommunikation. Soziale Netzwerke fungieren wie ein Konformitätsexperiment, in dem die Masse den Ton angibt. Und diese Masse kann leicht getäuscht werden durch Roboter (Bots), die Nutzerverhalten massenhaft simulieren und suggerieren (vgl. Serrano et al. 2019).

Dieses künstliche Aufblähen fungiert wie eine sich selbst erfüllende Prophezeiung: Je mehr Kommunikate in den sozialen Netzwerken Aufsehen erregen, desto mehr springen die Algorithmen der Plattformen darauf an und die Inhalte werden nach vorn gespielt. Davon bleiben auch die Selektionsmechanismen des Journalismus nicht unberührt.

Wenn dann Mediennutzerinnen und Mediennutzer erst einmal einen Weg eingeschlagen haben, kann es passieren, dass sich ein schräges Kommunikationsangebot an das nächste anschließt. „Kommunikation im Kaninchenloch" ist ein geflügeltes Wort in Anlehnung an eine Erzählung von Lewis Carroll.

Der Trend zu Kurzmitteilungen gerade auch in der politischen Kommunikation erleichtert die Selektionsmöglichkeiten, weil dadurch haltlose Behauptungen und Lügen leicht unters Volk gebracht werden. Massenmediale Anschlussfähigkeit können die Informationskriegerinnen und -krieger in den sozialen Vergemeinschaftungen des weltweiten Netzes schamlos ausnutzen.

Sicherheitspolitik ist als Problem der Kommunikation längst erkannt worden (Zowislo-Grünewald et al. 2011). Das Erzählerische hat als „Strategic Narratives" (Freedman 2006) sogar Einzug gehalten in die strategischen Überlegungen der Verteidigungspolitik. Narrativ und Narration fungieren allerdings wie Resilienz häufig noch als Schlagwörter mit Klärungsbedarf. Fraglich ist, ob die ästhetische Funktion des Poetischen ausreichend berücksichtigt wird. Damit ist nicht die geläufige Vorstellung vom Schönen und Ansehnlichen, sondern im Sinne Baumgartens (1750) das Wahrnehmungsvermögen gemeint.

Wahrnehmung besitzt dabei eine Eigenheit; denn „was man wahrnimmt, nimmt man für wahr. Es gibt ja kein Falschnehmen. Es sind ja immer nur die anderen, die behaupten, man sähe nicht recht, man wäre das Opfer einer Illusion, wenn sie was anderes sehen" (von Foerster 1985: S. 35). Was man sieht (bzw. nicht sieht) ist dabei unweigerlich das Ergebnis einer Unterscheidung.

Nun ist die Fähigkeit des Menschen, sich eine wahre Erkenntnis von der Wirklichkeit zu verschaffen, bekanntlich begrenzt. Wie geht man mit diesem Nichtwissen um? Der Aufklärer Immanuel Kant unterscheidet Meinen, Glauben und Wissen als unterschiedliche Formen des „Fürwahrhaltens" (Kant [1787] 1968: 533). Die Meinung ist im Gegensatz zum Wissen in

seinen Augen noch objektiv wie subjektiv unzureichend. Im Grundgesetz verankert, muss um den Respekt für die freie Meinung neuerlich gekämpft werden. Der Glaube ist in der Menschheitsgeschichte sicher die wirksamste Form im Umgang mit Nichtwissen. Wie Aristoteles im Zusammenhang mit der Dichtkunst (Poetik) feststellt, „verdient das Unmögliche, das glaubwürdig ist, den Vorzug vor dem Möglichen, das unglaubwürdig ist" (Aristoteles 1994: Kap. 25).

Für die Narratologie sind Glaubwürdigkeit und der Umgang mit Wahrheitsdefiziten wesentliche Herausforderungen. Bemerkenswert ist Philip Sidneys Apologie der Poesie aus dem 16. Jahrhundert (Sidney 1595). Über die Bühne der Fiktion, „Tagtraumhaftes Heldentum" und ihre „psychoanalytischen Lesarten" berichtet Andreas Galling-Stiehler (2017). „Die bereitwillige Aussetzung des Unglaubens", ein Diktum des Dichters und Theoretikers Samuel Taylor Coleridge ([1817] 1907: 6), erscheint in Anbetracht der gegenwärtigen Verfallserscheinungen öffentlicher Kommunikation aktueller denn je. Wird die Aussetzung der Ungläubigkeit moralisch belegt, werden damit nicht nur weitere Diskussion und Untersuchung im Keim erstickt.

Durch die moralische Kontextualisierung wird Glaubwürdigkeit zu einer sozialen Unterscheidung. In seiner Rede anlässlich der Verleihung des Hegelpreises 1989 definiert Niklas Luhmann Moral entsprechend als „eine besondere Art von Kommunikation, die Hinweise auf Achtung oder Mißachtung mitführt" (1990: 17f.). Aus Missachtung wird leicht Feindschaft. Die „Unterscheidung von Freund und Feind" (Schmitt 1932: 26) ist die demokratiefeindliche Definition des Politischen.

Die kursorischen Überlegungen verdeutlichen die Risiken von Kommunikation. Information ist keine Ware mit verderblichem Wahrheitsgehalt. Wer Fake News ausschließlich als manipulierte Falschmeldungen versteht, die mit objektiven Wahrheiten, Authentizität, Informationsarbeit, Evidenz etc. geheilt werden können, verkennt die soziale Sprengkraft.

Wenn der Glaube an alles Mögliche, an Lug und Trug, droht kommunikativ außer Kontrolle zu geraten, ist die Verteidigung gefragt. Der Historiker Timothy Snyder erinnert an eine Warnung Hannah Arendts. „Die Lüge erfordert Gewalt" (Snyder 2021), um die Unwahrheit zu verwirklichen.

Was Sinn macht – Selbstvergewisserung als Methode

„Armee ohne Auftrag“, heißt eine Bestandsaufnahme des Politikwissenschaftlers Wilfried von Bredow (2020). Das Buch schildert umfassend die Misere von Bundeswehr und Verteidigungspolitik – wie der Titel verrät – mit ihrem Auftrag. Auch der Einsatz im von Politikerinnen und Politikern gern ausgerufenen Kampf gegen Corona oder gegen die Unbill des Klimas werden in der Öffentlichkeit mehr geliebt als intern geschätzt. Von Auftragslosigkeit kann aber nach Ansicht des britischen Ex-Generals Richard Barrons nicht die Rede sein (Der Spiegel 2020). Barrons beschreibt eine komplexe Gemengelage geopolitischer Interessen vor dem Hintergrund der von den Vereinten Nationen formulierten 17 Zielen der Agenda 2030 für nachhaltige Entwicklung. Eine besondere Rolle spielt zudem die Transformation der Waffentechnologie mit den gesteigerten kostengünstigen Möglichkeiten der Digitalisierung. Milliardenschwere Waffensysteme, ehemals Aushängeschilder militärischer Stärke, sind verletzliche Saurier im digitalen Wandel.

Barrons Lagebeschreibung muss aber v. a. als Beitrag zur „Selbstvergewisserung“ (Schulz et al. 2020: 18 f.) über die Next Practice der Sicherheits- und Verteidigungspolitik gelesen werden. Die Methode der Selbstvergewisserung ist eine vorausschauende analytische Methode, die in folgenden drei Prozessschritten Antworten findet für diese Next Practice.

1. Forschung beantwortet die Frage: Worüber sprechen wir, wenn wir über uns und unsere Leistungen sprechen?
2. Interaktion beantwortet die Frage: Warum sprechen wir mit wem worüber?
3. Gestaltung beantwortet die Frage: Wie sprechen wir mit welchen Worten und Zeichen? (Schulz et al. 2020: 19)

Zu 1. Forschung

Voraussetzung für die Selbstvergewisserung ist die Selbstbeschreibung. Nicht Experten und Expertinnen, die wie das Wort verrät „Ex-", also draußen bzw. außen vor sind, geben in der Forschung den Ton an, sondern die Menschen in den Institutionen und Organisationen selbst. Besagtes Interview mit General Barrons ist ein journalistisches Format, das aber einen Eindruck verschafft über die Potenziale ethnografischer Feldforschung in Institutionen und Organisationen und die Zugänge zu persönlichen und unmittelbaren Erfahrungen. Ziel der ethnografischen Methode ist das Erkunden, Aufspüren und Zur-Sprache-bringen, um es in den weiteren Prozessschritten zu verarbeiten.

Zu 2. Zukunftsbeschreibung als „Sinndimensionen im Austausch"

Das essentialistische Wesens- oder Identitätsverständnis sucht nach einem Kern der Existenz. Über Jahrzehnte war für die Identität der Bundeswehr der Kalte Krieg mit festen territorialen Freund-Feind-Unterscheidungen identitätsstiftend. Das Problem ist, dass mit dem Verlust des Zwecks auch die Existenz infrage gestellt ist.

Eine zeitgemäße Strategie der Zukunftsbeschreibung sucht stattdessen nach Sinn und unterscheidet zwischen sachlicher, zeitlicher und

sozialer Sinndimension. Der Clou von Sinn als Orientierungsform ist das „laufende Aktualisieren von Möglichkeiten" (Luhmann 1984: 100). In Anlehnung an einen Buchtitel von Michel Houellebecq aus einem ganz anderen Zusammenhang geht es also um die *„Ausweitung der Kampfzone".* Gleichzeitig reduziert Sinn im Entscheidungsfall die Komplexität. Eine exzellente Strategie zeichne sich dadurch aus, dass sie laufend Möglichkeiten generiert. Ausweglosigkeit ist Kapitulation und damit das Ende der Strategie. Einen groben Eindruck vermittelt die nachfolgende Auswahl verschiedener Sinnoptionen.

Sachdimension

In der Sachdimension wird, wie oben erläutert, die Rolle der Kommunikation angemessen bewertet. Dabei erscheint die tradierte Konzentration auf strategische Räume (Land, Wasser, Unterwasser, Luft, Weltraum) anachronistisch im Verhältnis zu transzendentalen Kommunikationsräumen. Ich habe in den Überlegungen zur Kommunikation das Problem moralisch definierter Glaubwürdigkeit erläutert. Glaubenskriege werden durch Kommunikation geschürt und tangieren längst nicht mehr nur theologische und mystische Positionen.

Es überrascht trotzdem, wie sehr Desinformationen und Fake News noch zu überraschen vermögen. Doktrinen wie die russische Gerasimov-Doktrin legen unverhohlen die Strategien offen. Über geopolitische Strategien und Informationspolitik Chinas wäre man weniger verwundert, wenn man die entsprechenden Spielregeln studiert hätte. In den 36 Strategemen, dem berühmt berüchtigte Arsenal von Listen und Kunstgriffen (von Senger 1999), finden sich fast ausschließlich kommunikationsstrategische Ansätze. Mithilfe von Simulationsstrategemen wird Wirklichkeit fingiert, während Dissimulationsstrategien Wirklichkeit zu verbergen suchen. Auch für die Aufklärung gibt es explizite Informationsstrategeme.

Darüber hinaus gibt es zahlreiche Ausmünzungsstrategeme. Im Gegensatz zum zweckrationalen Ansatz der Zielverfolgung geht es bei diesen Strategemen um das Ausnutzen und Gestalten von Möglichkeiten und Situationspotenzial (Jullien 1996). Auch Überlegungen zur Ausrichtung

von Entscheidungsprogrammen im Rahmen der Strategie (vgl. Arlt/Schulz 2019: 9 f.) schließen sich an. Konditionalprogramme (ebd.) böten nicht zuletzt Alternativen zum dominant zweckrationalen Vorgehen.

Sozialdimension

In dieser Sinndimension geht es um das soziale Gefüge. Arbeiterschaft, Mitarbeiterinnen und Mitarbeiter, Kolleginnen und Kollegen – für Beschäftigte gibt es unterschiedliche Bezeichnungen. Im Militärischen wird der soziale Zusammenhalt dagegen als Kameradschaft definiert. Selbstvergewisserung ist dringend nötig, um in einem funktional ausdifferenzierten Tätigkeitsfeld den Sinn von Kameradschaft, Autorität und Beruf zu fassen. Insbesondere über Menschenbilder (vgl. Müller 2019) ist zu reden. Eine besondere Herausforderung für die Sozialdimension ist die für militärische Auseinandersetzungen konstitutive Unterscheidung von Freund und Feind. Kann die Demokratie, die ja angetreten ist, um Agonie durch Antagonismus bzw. Feindschaft durch Gegnerschaft zu ersetzen, das überhaupt sehen und ist sie dafür gewappnet? Die Angriffe auf die Parlamente in Washington und Berlin zeugen eher von Ratlosigkeit. Feindliche Bewegungen sind im Vormarsch (ausführlich dazu Schulz 2020). Die Unterscheidung von Freund und Feind als Motiv politischen Handelns gewinnt dadurch an Aktualität und wird zur Herausforderung demokratisch verfasster Staaten.

Zeitdimension

Die Zeitdimension ist eine besondere Herausforderung, insbesondere, weil die Zukunft immer unsicher ist und sich jedes Erleben in der Gegenwart abspielt. Die Vergangenheit beeinflusst dieses Erleben. Streitkräfte sind nicht geschichtslos, sondern kultivieren ihre Vergangenheit. Für die existenziell wichtige Beschäftigung mit der Zukunft, für Wandel, Innovation und Veränderung, gibt Luhmann eine Unterscheidung zu bedenken zwischen der vermeintlichen Sicherheit einer „gegenwärtiger Zukunft“ und „zukünftigen Gegenwarten, die immer genau so sein werden wie sie sein werden und nie anders“ (Luhmann 1992: 140). Die Herausforderung ist, wie es gemeinschaftlich gelingt, sich auf die Zukunft und nicht auf die Vergangenheit zu beziehen.

Zu 3. Gestaltung selbstvergewissernder Kommunikation

Zwischen Waffen und Kommunikation gibt es einen Zusammenhang, den der Philosoph Hans Blumenberg anthropologisch deutet. Der Mensch ist ein physisch verletzliches Wesen, das sich Feinde auf Distanz halten muss. Als die Fluchträume nicht mehr ausreichten, kam es zu einer „Drehpunktsituation" (Blumenberg 2007: 13), in der sich der Mensch durch „Handlung auf Entfernung, der *actio per distans,* in der Handlung des Wurfes" (ebd.) zu erwehren lernt. Analog zu Waffen und Fallen, die dem Menschen in sachlicher und zeitlicher Sinndimension Raum- und Zeitgewinn ermöglichten, überbrückt Sprache die Distanz zwischen dem, was ist und dem, was sein soll. Kommunikation ist – auch wenn ich mich wiederhole – keine Informationsübertragung.

Literatur

A Aristoteles (1994). Poetik. Zweisprachige Ausgabe, übersetzt und herausgegeben von Menfred Fuhrmann. Stuttgart: Reclam.

Arlt, Hans-Jürgen (2016). Konfliktkompetenz statt Resilienz. Wider die Trivialisierung von Individualität. In: Heinrich-Böll-Stiftung (Hrsg.): Grünbuch soziale Teilhabe in Deutschland (S. 119–126). Berlin: Heinrich-Böll-Stiftung.

Arlt, Hans-Jürgen/Mühl-Benninghaus, Wolfgang (2017). Medienvielfalt = Meinungsvielfalt? Historische, systematische und digitale Perspektiven auf Meinungsbildung und öffentliche Meinung. Hrsg. Organisation der Mediaagenturen e. V. und ZDF Werbefernsehen GmbH. Berlin. http://www.dwg-online.net/wp-content/uploads/2018/02/Studie_Medienvielfalt_gleich_Meinungsvielfalt_2017_10_21.pdf (letzter Zugriff: 17.05.2021).

Arlt, Hans-Jürgen/Schulz, Jürgen (2019). Die Entscheidung. Lösungen einer unlösbaren Aufgabe. Wiesbaden: Springer.

B Baecker, Dirk (2018). 4.0 oder Die Lücke die der Rechner lässt. Leipzig: Merve.

Bateson, Gregory (1992). Ökologie des Geistes. Anthropologische, psychologische, biologische und epistemologische Perspektiven [1972]. Frankfurt am Main: Suhrkamp.

Baumgarten, Alexander Gottlieb (2007). Ästhetik (2 Bde.) [1750]. Hamburg: Meiner.

Blumenberg, Hans (1979). Schiffbruch mit Zuschauer. Frankfurt a. M.: Suhrkamp.

Blumenberg, Hans (2007). Theorie der Unbegrifflichkeit. Frankfurt a. M.: Suhrkamp.

C Coleridge, Samuel T. (1907). Biographia Literaria [1817]. Gloucestershire: Clarendon Press.

D *Der Spiegel* (2020). „So können Sie jedes europäische Land in nur 14 Tagen in die Knie zwingen". Interview mit Richard Barrons von Konstantin von Hammerstein. In: Spiegel Online, 23.5.2020. https://www.spiegel.de/politik/ausland/ex-general-richard-barrons-ueber-den-krieg-der-zukunft-kampfroboter-bekommen-keine-pension-a-058c61c5-e4c2-4845-9d0e-33f3a7a3e4cc (letzter Zugriff: 17.12.2020).

F Freedman, Lawrence (2006). The Transformation of Strategic Affairs. Abingdon/New York: Routledge.

G Galling-Stiehler, Andreas (2017). Tagtraumhaftes Heldentum. Psychoanalytische Lesarten der Auftragskommunikation. Wiesbaden: Springer.

H Holling, C. S. (1973). Resilience and stability of ecological systems. Annual Review of Ecology and Systematics, 4, S. 1–23.

J Jullien, François (1996). Traité de l'efficacité. Paris Éditions Grasset & Fasquelle.

K Kant, Immanuel (1968). Kritik der reinen Vernunft [1787]. Kants Werke Bd. 3. Berlin: Akademie Textausausgabe.

Kraus, Karl (1913). Die Fackel, Nr. 376–377, 1913, S. 21.

L Landeszentrale für Politische Bildung Baden-Württemberg (2019). Was ist Sicherheit? https://www.lpb-bw.de/was-ist-sicherheit (letzter Zugriff: 17.12.2020).

Luhmann, Niklas (1971). Sinn als Grundbegriff der Soziologie. In: Habermas, Jürgen/Luhmann, Niklas: Theorie der Gesellschaft oder Sozialtechnologie (S. 25–100). Frankfurt am Main: Suhrkamp, S. 43.

Luhmann, Niklas (1984). Soziale Systeme. Grundriß einer allgemeinen Theorie. Frankfurt a. M.: Suhrkamp.

Luhmann, Niklas (1990). Paradigm lost: Über die ethische Reflexion der Moral. Frankfurt a. M.: Suhrkamp.

Luhmann, Niklas (1992). Beobachtungen der Moderne. Opladen: Westdeutscher Verlag.

Luhmann, Niklas (1995). Was ist Kommunikation? In ders.: *Soziologische Aufklärung* 6. Die Soziologie und der Mensch. Wiesbaden: Westdeutscher Verlag, S. 113–124.

M Müller, Robert Caspar (2019). Konsumentenbilder als produktive Fiktionen. Eine theoretische und ethnographische Untersuchung. Wiesbaden: Springer.

S Schmitt, Carl (1932). Der Begriff des Politischen. 6. Aufl., 4. Nachdr. der Ausgabe von 1963. Berlin: Duncker & Humblot, S. 26.

Schulz, Jürgen (2001). Issues Management im Rahmen der Risiko- und Krisenkommunikation – Anspruch und Wirklichkeit in Unternehmen. In: Röttger, Ulrike (Hrsg.) (2001): Issues Management. Opladen: Westdeutscher Verlag, S. 217–234.

Schulz, Jürgen/Galling-Stiehler, Anadreas/Müller, Robert Caspar (2020). Auftragskommunikation – Für Unternehmen und Institutionen sprechen. Wiesbaden: Springer.

Schulz, Jürgen (2020). Feindliche Aufmärsche in der Corona-Krise. bruchstücke Blog für konstruktive Radikalität. https://bruchstuecke.info/2020/09/15/feindliche-aufmaersche-in-der-coronakrise/ (letzter Zugriff: 17.12.2020).

Serrano, Juan Carlos/Medina, Morteza Shahrezaye/Orestis Papakyriakopoulos/Hegelich, Simon (2019). „The Rise of Germany's AfD: A Social Media Analysis." In Proceedings of the 10th International Conference on Social Media and Society, S. 214–223. ACM, 2019. https://dl.acm.org/citation.cfm?id=3328562 (letzter Zugriff: 17.12.2020).

Sidney, Philip (1595). The Defence of Poesie. London: Ponsonby.

Snyder, Timothy (2021). „Trumps Erbe ist die große Lüge". Deutschlandfunk. Timothy Snyder im Gespräch mit Christoph Heinemann. https://www.deutschlandfunk.de/historiker-timothy-snyder-trumps-erbe-ist-die-grosse-luege.694.de.html?dram:article_id=491239 (letzter Zugriff: 22.01.2021).

V Von Bredow, Wilfried (2020). Armee ohne Auftrag: Die Bundeswehr und die deutsche Sicherheitspolitik. Zürich: Orell Füssli.

Von Clausewitz, Carl (1980). Vom Kriege [1832–34]. (Hinterlassenes Werk des Generals Carl von Clausewitz, Bd. 1–3, bei Ferdinand Dümmler, Berlin) Berlin: Ullstein.

Von Foerster, Heinz (1985). Entdecken oder Erfinden. Wie lässt sich Verstehen verstehen? In: Gumin, Heinz, & Mohler, Armin (Hrsg.); Einführung in den Konstruktivismus. München: Oldenbourg, S. 27–68.

Von Senger, Harro (Hrsg.) (1999). Die List. Frankfurt a. M.: Suhrkamp.

W Wellensieck, Sylvia Kéré /Galuska, Joachim (2014). Resilienz. Kompetenz der Zukunft, Weinheim.

Z Zowislo-Günewald, Natascha/Schulz, Jürgen/Buch, Detlef (Hrsg.) (2011). Den Krieg erklären – Sicherheitspolitik als Problem der Kommunikation. Frankfurt: Peter Lang.

Zukunftsinstitut (2020). Die Megatrend-Map https://www.zukunftsinstitut.de/documents/downloads/MegatrendMapZukunftsinstitut_120918.pdf) (letzter Zugriff: 17.01.2021).

Strategisches Kommunikations-management

als Domain der wehrhaften Demokratie

Natascha Zowislo-Grünewald
und Julian Hajduk

03 **Für den Krieg der Zukunft benötige man weder Atomsprengköpfe noch Flugzeugträger, so der britische Ex-General und militärische Vordenker Sir Richard Barrons. Stattdessen genügten eine Kombination aus Präzisionsraketen, Cyberangriffen – und sozialen Medien.[45] Was ist dran an diesem fundamentalen Paradigmenwechsel hin zum Strategischen Kommunikationsmanagement als Domain der wehrhaften Demokratie? Wie zeigen sich die deutsche, europäische und transatlantische Verteidigungspolitik gegenüber diesem gewappnet?**

Eine neue Doktrin?

Soft Power schlägt Hard Power, so könnte man diese Neuorientierung in der Verteidigungspolitik auf den Punkt bringen. Allerdings ist die weiche Macht in diesem Fall weniger auf kulturelle Überlegenheit und internationale Institutionen gegründet, so wie es Joseph S. Nye[46] einst vorgedacht hatte, sondern viel subtilerer Natur und damit zugleich bedrohlicher. Richard Barrons gilt als einer der wichtigsten militärischen Vordenker Großbritanniens und entsprechend militärisch sind seine Äußerungen zu deuten. Schließlich können Kriege weiterhin nur dann gewonnen werden, wenn eine Konfliktpartei die andere besiegt. Findet dieser Konflikt aber gegenwärtig nicht statt, sondern ist nur ein Planspiel, eine Überlegung, eine Projektion, so kommt an dieser Stelle ins Spiel, was in der militärisch-politischen Sphäre mit dem Begriff der Doktrin[47] gefasst wird.

So formulierte die Breschnew-Doktrin ab 1968, dass die Souveränität der einzelnen Sowjetrepubliken dort ende, wo die Interessen der sozialistischen Gemeinschaft bedroht seien. Dies legitimierte den direkten – auch militärischen – Eingriff Moskaus in die politischen Angelegenheiten des de jure autonom strukturierten Staatenverbundes – und faktisch auch in die Staaten des Warschauer Pakts als unmittelbare sowjetrussische Einflusszone. Zugrunde lag dieser Doktrin die These, dass innere und äußere dem Sozialismus feindliche Kräfte Umsturzversuche innerhalb der einzelnen Sowjetrepubliken unternehmen bzw. stets unterstützen würden, sodass NATO-Truppen anschließend in für die UdSSR immer bedrohlicheren geostrategischen Positionen stationiert werden könnten. Die Breschnew-Doktrin diente insofern auch als nachträgliche Legitimation der Militärintervention des Warschauer Pakts in der Tschechoslowakei am 21. August 1968 zur Niederschlagung des sogenannten Prager Frühlings.

Die US-amerikanische Reaktion ließ nicht lange auf sich warten. Beinahe zeitgleich im Jahr 1969 verabschiedeten die Vereinigten Staaten die sogenannte Nixon-Doktrin. Sie forderte hinsichtlich des seit dem unmittelbaren Kriegseintritt der USA 1964 besonders brisant gewordenen Vietnam-

Konflikts zukünftig eine größere militärische wie finanzielle Verantwortung der US-amerikanischen Verbündeten ein. Einerseits war sie also außenpolitische Verpflichtung gegenüber der neuen sowjetrussischen Politik der Breschnew-Doktrin, andererseits versuchte sie, die enormen gesellschafts- und wirtschaftspolitischen Spannungen aufzulösen, welche durch den nicht nur finanziell kostspieligen US-amerikanischen Einsatz entstanden waren.

Die Sowjetunion wie auch die Vereinigten Staaten reagierten und agierten militärstrategisch, indem sie die erwartbaren Erwartungen ihres militärischen Gegenübers in ihre doktrinären Überlegungen ebenso einbezogen wie die in die Zukunft extrapolierten gesellschaftspolitischen Entwicklungen ihrer jeweiligen Einflusssphären. Aus exakt diesen beiden Faktoren entwickelt auch Richard Barrons seine Gedanken, wenn er „Präzisionsraketen, Cyberangriffe […] und soziale […] Medien“[48] als die entscheidenden Instrumente zukünftiger Konflikte benennt:

1. Gesellschaftliche Entwicklungen: Durch die digitale Revolution ist die Zivilbevölkerung auf eine Art und Weise vernetzt, wie dies nie zuvor in der Menschheitsgeschichte der Fall war. Soziale Medien dienen hierbei nicht nur als Akzeleratoren von Informationsflüssen, sondern genießen aufgrund ihrer (wahrgenommenen) Eigenschaft als Many-to-Many- bzw. Word-to-Mouth-Informationskanäle auch eine besonders hohe Authentizität – schließlich werden die Kommunikationen dort mehrheitlich einzelnen Individuen mit ihren privaten Agenden und nicht etwa staatlichen Akteurinnen und Akteuren zugeschrieben. Die daraus erwachsende Möglichkeit von (Des-)Informationskampagnen genau dieser unerkannten Akteurinnen und Akteure, welche sich ohne nennenswerte Zeitverzögerung schneeballartig „von selbst“ verbreiten, wurde bereits mehrfach wissenschaftlich untersucht und validiert.

2. Die erwartbare Erwartung: So wie die Breschnew-Doktrin ihren Schlussfolgerungen Blockdenken und Konkurrenz der Systeme zugrunde legte, auf die die Nixon-Doktrin wiederum reagierte, haben sich nach dem Zusammenbruch der Sowjetunion abseits der Bedrohung durch den internationalen Terrorismus realpolitische Fronten gebildet, deren Extrapolation zu der Erkenntnis führt, dass Kräfte existieren, welche Stabilität, Sicherheit und Frieden der westlichen Welt bzw. der NATO-Mitgliedstaaten gefährden. Das Ende der Blockkonfrontation hat eben nicht zum Ende der Geschichte geführt, sondern eher zum Gegenteil. Der Westen muss daher mit einer tendenziell feindseligen, multipolaren Weltordnung leben lernen.

Richard Barrons Einlassungen sind insofern auch als eine Antwort auf die sogenannte Gerasimov-Doktrin (2013)[49], respektive das offizielle sicherheits- und machtpolitische Vorgehen des Kreml, zu verstehen. In der Gerasimov-Doktrin wird dargelegt, wie asymmetrische Konflikte die althergebrachten Grenzen zwischen Krieg und Frieden auflösen, zirkulierende Botschaften und Informationen Staaten kollabieren lassen können und wie ein geschicktes Agieren in diesem Raum militärische Mittel zur Durchsetzung eigener Interessen sehr effizient ersetzen können:

„In the 21st century we have seen a tendency toward blurring the lines between the states of war and peace. Wars are no longer declared and, having begun, proceed according to an unfamiliar template.

The experience of military conflicts – including those connected with the so-called coloured revolutions in north Africa and the Middle East – confirm that a perfectly thriving state can, in a matter of months and even days, be transformed into an arena of fierce armed conflict, become a victim of foreign intervention, and sink into a web of chaos, humanitarian catastrophe, and civil war. […]

> The very ‚rules of war' have changed. The role of nonmilitary means of achieving political and strategic goals has grown, and, in many cases, they have exceeded the power of force of weapons in their effectiveness. […]
>
> The information space opens wide asymmetrical possibilities for reducing the fighting potential of the enemy. In North Africa, we witnessed the use of technologies for influencing state structures and the population with the help of information networks. It is necessary to perfect activities in the information space, including the defense of our own objects."[50]

Eine derartig gestaltete „Propaganda 2.0" macht sich Russland zur Bewältigung sogenannter „nicht linearer Kriege" bereits jetzt zunutze, auch weil die Strateginnen und Strategen dort in ihrer Extrapolation erwartbarer Erwartungen glauben, sich aufgrund der in der NATO-Osterweiterung angelegten westlichen Expansionspolitik gegen ein weiteres „Einschnüren" durch das westliche Militärbündnis verteidigen zu müssen.

Während Russland im Georgien-Krieg im Jahr 2008 noch recht unbeholfen alte Propagandamuster verwendete, wurde dieser neuartige Ansatz sehr effizient und erfolgreich im Fall der Krim-Annexion im Jahr 2014 durch die Truppen der russischen Föderation exerziert. Der klassische Kampfeinsatz wurde dabei weitgehend durch eine konzertierte Aktion ersetzt, die v. a. darauf setzte, Moral und Einsatzbereitschaft der ukrainischen Bevölkerung zu unterminieren sowie die internationale Staatengemeinschaft hinsichtlich des prorussischen Narrativs in dem Sinne zu beeinflussen, dass Russland nicht die Krim annektieren würde.

So wurde mithilfe der sozialen Medien die ukrainische Regierung vor der eigenen Bevölkerung als korrupt und illegitim beschrieben, während die Geschichte der russisch-westlichen Beziehungen als Vertrauens- und Wortbruch gerahmt wurde, um so einem internationalen Auditorium das Vorgehen des Kreml als Ursache-Wirkung-Zusammenhang zu vermitteln. So

hätte ein NATO-Beitritt der Ukraine zur Folge gehabt, dass die historisch wie militärisch bedeutende russische Schwarzmeerflotte in ihrem Operationsraum nicht nur durch den NATO-Beitritt der Türkei im Jahr 1952 vom Mittelmeer abgeschnitten, sondern sich nun sogar ihr Heimathafen Sewastopol unter der Ägide des nordatlantischen Bündnisses befinden würde.

Die Anknüpfung an das Selbstbestimmungsrecht der Völker sowie das Krim-Referendum taten zuletzt ihr Übriges, um die von Russland ausgehende Aggression als friedliche Revolution zu maskieren – ein Argument, das übrigens auch in der US-amerikanischen respektive westlichen Unterstützung des Arabischen Frühlings eine Rolle in der politischen Bewertung gespielt hat. Es muss an dieser Stelle erwähnt werden, dass deshalb bis heute nicht klar ist, ob Walerij Gerasimov mit seiner Analyse aus russischer Sicht beschrieben hat, was er als realpolitisches „westliches Handeln" zu beobachten glaubte, und der Begriff einer eigenständigen Doktrin daher somit unpassend ist. Nichtsdestotrotz wäre seine Analyse auch dann die militärstrategische Essenz eines emergenten, d. h. aus Faktoren sui generis entstandenen und nicht etwa von langer Hand geplanten Phänomens.

Es gelang Russland zwar nicht, die völkerrechtswidrige Annexion der Krim vor der internationalen Staatengemeinschaft zu legitimieren, allerdings blieb eine gesellschaftliche Ächtung weitestgehend aus: Rund 40 Prozent der Deutschen befürworteten im Jahr 2014 die Eingliederung der Halbinsel in die russische Föderation,[51] und sogar offizielle politische Vertreterinnen und Vertreter wie der damalige brandenburgische Ministerpräsident Matthias Platzeck warben um Verständnis für die russische Haltung und für russisches Handeln.[52]

Die Antwort des Westens?

Kommunikation ist eine Schlüsselgröße der modernen Sicherheits- und Verteidigungspolitik. Der Stratege Richard Barrons hat erkannt, welche Bedeutung Kommunikation als Soft Power besitzt, wenn es darum geht, in den Konflikten einer multipolaren Weltordnung zu bestehen. Russland scheint hierfür gerüstet zu sein. Doch welchen Niederschlag hat dies im deutschen, europäischen und transatlantischen Verständnis von Sicherheitspolitik gefunden?

Wie Elbridge Colby, Direktor des Abwehrprogramms am Center for a New American Security der NATO jüngst formulierte, sollte „Deutschland […] in Europas Verteidigung so etwas wie das Rückgrat sein."[53] Dass es dieses Rückgrat geben muss, sei dabei angesichts der oben skizzierten Bedrohung durch die unter Präsident Wladimir Putin wieder erstarkenden russischen Großmachtbestrebungen unabdingbar, die sich besonders in einer weiteren militärischen wie zivilen Destabilisierung Osteuropas manifestierten. Allerdings, so der US-Amerikaner, darf bezweifelt werden, dass die Bundeswehr aktuell in der Lage sei, „auch nur eine kampfbereite Division zur Verfügung [zu] stellen."[54]

„Deutschland ist die größte Wirtschaftskraft in Europa und liegt dazu noch geografisch günstig, um Streitkräfte zu entsenden"[55], begründet Colby seine Position weiter – und sei im Rahmen eines möglichen NATO-Bündnisfalls an der osteuropäischen Grenze deshalb einzig in der Lage, feindlichen militärischen Akten rasch Einhalt zu gebieten. Hieraus spricht jedoch allein die Logik der Hard Power, die in Anbetracht der chronisch unterfinanzierten militärischen Fähigkeiten der Bundesrepublik, aber auch Europas insgesamt ohne die Vereinigten Staaten als Rückgrat des transatlantischen Bündnisses nicht glaubwürdig aufrechterhalten werden kann.

Erschwerend kommt hinzu: Seit Jahrzehnten mahnen die US-Amerikaner, dass die vor 70 Jahren festgelegte Pauschale für den Verteidigungshaushalt seitens der Bundesrepublik nicht erreicht wird und daraus Konse-

quenzen hinsichtlich des militärpolitischen Engagements der Supermacht erwachsen könnten. Mit der endgültigen Hinwendung der USA zum pazifischen Raum gepaart mit der protektionistischen und nationalistischen Politik Donald Trumps dürfte aber nun der Zeitpunkt gekommen sein, da die Ermahnungen unserer transatlantischen Partner nicht mehr allein kosmetischer Natur sind, sondern tatsächlich die angedrohten Folgen implizieren könnten.

Früher oder später wird Europa damit auf sich allein gestellt sein, wenn es um eine mögliche Erstverteidigung der Außengrenzen geht – so wie es heute aufgrund der lediglich symbolisch zu nennenden Militärpräsenz der US-Amerikaner in Osteuropa übrigens bereits der Fall wäre. Und – folgt man jener der Gerasimov-Doktrin zugrundeliegenden Logik, ist dieser Verteidigungsfall im sogenannten Informationsraum – besser noch: Kommunikations- und Diskursraum – bereits eingetreten.

Der Kommunikations- und Diskursraum: eine neue Domain

Für die Gerasimov-Doktrin wie auch in der Analyse Richard Barrons ist dieser Kommunikationsraum zentral. Hier ist Sicherheit zuallererst keine mathematische Größe, nicht in ein Gleichungssystem aus Divisionen zu fassen – sondern v. a. eine Glaubensfrage: Macht Russland nur das, was der Westen auch tut? Haben wir dringendere Probleme, als zwei Prozent des Staatshaushalts in die Landes- und Bündnisverteidigung zu investieren? Selbstbestimmungsrecht der Völker oder nationalstaatliche Integrität?

Diese fundamentalen Standpunkte, die sich allein aus der Lebenswelt bzw. dem Blickwinkel des Betrachters oder der Betrachterin legitimieren, nennt man innerhalb der Kommunikationswissenschaften Diskurse. Nach Prinzip der Dialektik Theodor W. Adornos konstituieren sich diese Diskurse aus einer Argumentation, ihrem möglichen Antipoden – und allem, was dazwischen liegt. In ihrer Gesamtheit fassen sie den Möglichkeitsraum unserer Wahrnehmung, das, was denkbar ist – und was deshalb gedacht und gesagt wird.

Diskurse verweigern einen objektiven Wahrheitsbegriff innerhalb der sozialen Sphäre, was wiederum nicht bedeutet, dass plötzlich alles möglich ist. Es existieren physikalische, chemische, biologische Gesetzmäßigkeiten, denen sich selbst die Interpretation derselben nicht entziehen kann – darüber hinaus, besonders innerhalb der Verkettung von Wirkzusammenhängen, ist jedoch vieles möglich.

Die Frage nach der Wahrheit, nach dem Ideal Leopold von Rankes, zu beschreiben, „wie es eigentlich gewesen“[56] ist, wird im Rahmen einer diskursiven Beschaffenheit der Welt überflüssig – oder sinnlos. Objektivität wird ersetzt durch die Setzungsmacht dessen, was objektiv ist: durch Deutungshoheit.

Deutungshoheit ist damit genau das, was laut Walerij Gerasimov die Grenzen zwischen Krieg und Frieden dauerhaft verwischen lässt. Denn politische Systeme – nicht nur, aber insbesondere solche, welche die Volkssouveränität zugrunde legen – benötigen politische Unterstützung, um handlungsfähig zu sein. Vereinfacht gesagt: Werden Russland und seine Expansionspolitik nicht als sicherheitspolitisch relevanter Faktor, als Bedrohung, begriffen, so wird eine Partei, welche zur Bekämpfung dieses nunmehr fiktiven Szenarios Steuergelder ausgeben möchte, keine Regierungsverantwortung erlangen.

Erstaunlich scheint, dass diese Erkenntnis seit Beginn des postmodernen respektive nachmetaphysischen Zeitalters nunmehr auf einem theoretisch belastbaren Fundament ruht, gleichzeitig genau darüber aber stets verhandelt wird: Politische Kommunikation scheint überflüssig, da mit dem Zusammenbruch des Ostblocks das „Ende der Geschichte“[57] eingeläutet wurde. Kapitalismus und Demokratie haben gesiegt, weil sie die objektiv besten Systeme darstellen – und somit jeder, der dies anzweifelt, zumindest in der westlichen Welt als Sonderling betrachtet wird.

Dabei gab es Wahlkampf sowie politische Werbung schon immer, selbst totalitäre Systeme legitimieren ihre Positionen in den seltensten Fällen mit einer angeblichen inhärenten Objektivität. Ähnliches gilt für die Kriegsführung: Der Bau des trojanischen Pferdes war wohl der erste Akt psychologischer Kriegsführung. Wie jede Gymnasiastin und jeder Gymnasiast aus dem Geschichtsunterricht weiß, hat Bismarck 1870 die Emser Depesche in der – im Nachgang berechtigten Hoffnung – veröffentlicht, Napoleon III. könnte diesen Affront nicht auf sich beruhen lassen: Preußen wurde in den selbst gewünschten Verteidigungskrieg gezwungen und

schaffte es so, insbesondere die süddeutschen Staaten, die sich ein paar Jahre zuvor noch vehement gegen die Vormachtstellung der Hohenzollern verweigert hatten, hinter sich zu vereinen.

Von einschneidend neuer Qualität sind allerdings die zur Verfügung stehenden Kommunikationsmittel, mit denen der Kampf um Deutungshoheit heutzutage ausgefochten wird: Wie Richard Barrons analysiert, erlauben es die sozialen Medien sowie überhaupt die echtzeitliche Peer-to-Peer- und Group-to-Group-Kommunikation, dass theoretisch jedes Individuum eine Emser Depesche veröffentlichen kann: Die klassischen Gatekeeper (Redaktionen, Herausgeberinnen und Herausgeber, Verlagshäuser) existieren nicht mehr, die Reichweite einer einzelnen Influencerin oder eines einzelnen Influencers übersteigt zeitweise die Einschaltquoten der *Tagesschau*.[58]

Resilienz des Kommunikations- und Diskursraums als Zielgröße

Die Gerasimov-Doktrin macht sich diese Veränderung der Verhältnisse bereits zu eigen. Um nun Verteidigungsfähigkeit in Anbetracht der „kommunikativen Bedrohungslage" zu erreichen, gilt es, Resilienz – also inhaltliche Widerstandskraft – auf diskursivem Gebiet aufzubauen. Für die Verteidigungspolitik in Deutschland bedeutet dies:

1. Ohne eine solide Basis von Soft Power ist keine Hard Power zu erlangen. Entsprechende Faktoren müssen auf diskursiver Ebene aktiviert und gestärkt werden. Dies beinhaltet die Anerkennung einer weltweiten Bedrohungslage auch für Deutschland und die Deutschen. Die freiheitlich-demokratische Werteordnung wird eben doch am Hindukusch verteidigt – nicht nur de jure, sondern auch de facto. Eine globalisierte Welt schafft Feinde, wo früher höchstens Terra incognita existierte. Darüber hinaus ist Russland eben kein potenzieller verlässlicher Partner, sondern betreibt eine ganz auf das national kommunizierte Großmachtstreben zugeschnittene Expansionspolitik, die neben der Ukraine ihr Augenmerk auf das Baltikum – und damit sowohl auf EU-Territorium als auch auf NATO-Partnerinnen und -partner – legt. Diese Entwicklung zeigt sich deutlich anhand der Einflussnahme in der Informationssphäre, die der Kreml tagtäglich auszuüben versucht. Staaten haben eben keine Freunde, wie es Charles de Gaulle einst formulierte, sondern nur Interessen.

2. Auch die Einsatzfähigkeit der Truppe, nicht nur in puncto Ausrüstung, wird durch Soft-Power-Faktoren erhöht. Die gesamtgesellschaftliche Anerkennung der Bundeswehr ist hier zentraler Pfeiler. Soldatinnen und Soldaten sind eben keine Mörder, zumindest dann nicht, wenn sie für einen gerechten Grund Leib und Leben riskieren. Spätestens seit den NATO- und UN-Missionen auf dem Balkan Ende der 1990er-Jahre hat sich die Bundeswehr von ihrer Vergangenheit gelöst. Anerkennung für die Leistungen der Soldatinnen und Soldaten zur Aufrechterhaltung und Durchsetzung einer Weltordnung, die zumindest ein – von uns – empfundenes Höchstmaß an Sicherheit, Stabilität und Wohlstand schafft, sollten eine Selbstverständlichkeit sein. Zu einer gesellschaftlichen Werteordnung, in der wir leben und offensichtlich auch leben wollen, muss man auch bereit sein, sich zu bekennen – nicht objektiv, aber im Sinne einer diskursiven Selbstverständlichkeit. Das Stichwort wehrhafte Demokratie lebt damit sowohl innen- als auch außenpolitisch wieder auf.

Eine Erweiterung des Diskurses zu diesen beiden Polen wirkt sich damit positiv auf Containment (Wehrhaftigkeit) und Deterrence (Abschreckungswirkung) aus, während gleichzeitig die Bereitschaft in der Bevölkerung wächst, die Bedrohungslage anzuerkennen. Außerdem werden so negative Diskursausformungen in ihrem Schadenspotenzial abgemildert: Niemand möchte das Primat der (Verteidigungs-)Politik anzweifeln, aber die Währung der politischen Sphäre in Deutschland sind nun einmal Wählerstimmen. Lautet der gesamtgesellschaftliche Konsens, dass eine Bedrohungslage besteht, der nur mit einer funktionierenden Landesverteidigung begegnet werden kann, so ist es einem Finanzminister schlicht nicht mehr möglich, Haushaltskürzungen wie selbstverständlich zu verlangen.[59]

Dies ist aber nur die eine Seite der Medaille diskursiv-narrativen Denkens. Nimmt man die Gerasimov-Doktrin ernst, stehen die verschiedenen Diskurse in Deutschland im eigentlichen Zentrum der Bedrohung. Neben dem Versuch der aktiven Gestaltung dieser Diskurse ist es daher essen-

ziell, deren Verlauf zu durchdringen und mögliche Wendungen zu antizipieren. Dabei geht es nicht nur darum, die Sphäre dessen, was gesagt werden kann, immer wieder neu zu analysieren. Vielmehr geht es darum, auf die vitalen Diskursebenen wirkende Bedrohungsszenarien frühzeitig zu erkennen und diesen entgegenzuwirken. Schon heute ermöglichen es uns Big Data und die darauf spezialisierten Analysetools, ein relativ gutes Verständnis davon zu erlangen, was die Gesellschaft denkt. Nur so können einerseits innerdeutsche und auch innereuropäische Warnsignale verstanden werden, bevor sie ihre negativen Potenziale voll entfalten. Andererseits schafft man auch Freiheitsgrade gegenüber der aktiven Beeinflussung von außen, wie sie in der Gerasimov-Doktrin als Grundlage nichtlinearer Konflikte festgelegt wurde.

Strategisches Kommunikations- und Diskursmanagement: eine (präventive) Antwort auf narrative Bedrohungen?

Feindliche Narrationen unterminieren die Glaubwürdigkeit von Unternehmen, politischen Organisationen und im Extremfall der Demokratie als Staatsform. Latent oder offensiv, zufällig oder vorsätzlich – die Wirkung ist bei denjenigen, die feindlichen Narrationen nichts entgegenzusetzen haben, die nicht resilient sind, die gleiche. Die Sicherheit der eigenen Überzeugungen bröckelt, möglich scheint alles bis zur Implosion des politischen Systems.

Dass augenscheinlich die Implikationen dieses holistischen Diskursansatzes in der neuen Kalten-Krieg-Führung (noch) keine Berücksichtigung finden und keinesfalls die Bedeutung in der strategischen Planung erlangt haben, die ihnen zukommen müsste, ist mindestens beunruhigend. Der Wertschöpfungsbeitrag der Kommunikation zur Herstellung von Sicherheit wird in aktuellen Planungen nicht kalkuliert und entsprechend nicht dargestellt.

Dabei wäre die Antwort auf die Bedrohung im Diskursraum bzw. eine präventive Stärkung und Abschirmung vor subversiven Diskursen zum einen tatsächlich kostengünstig im Vergleich zu potenziellen Konfliktkosten im weiteren Verlauf und zum anderen unabhängig von der genauen Bestimmung der Quelle der Beeinflussung. Notwendig wäre allerdings, dass man sich den faktischen Auswirkungen der Gerasimov-Doktrin nicht länger verschließt und im deutschen, aber auch im euro-

päischen Sicherheitskontext die notwendigen Fragen, ob und wie wir auf diese neue alte Doktrin reagieren wollen, nicht länger aufschiebt.

1. Diskursanalyse: Zunächst braucht es eine Analyse- und Aufklärungsfähigkeit, die Indikationen für sicherheitsrelevante Diskurse ableitet, im weiteren Sinne ein Frühwarnsystem. Welche Schwellenwerte kommunikationswissenschaftlich gefasst werden können und relevant sind, bei welchen Indikatoren Schwellenwerte auch in Kombination überschritten werden müssen, um von einer fragiler werdenden Sicherheitslage im Kommunikations- und Diskursraum sprechen zu können, ist tatsächlich einer inhaltlichen und politischen Debatte wert, die noch zu führen ist. Was überhaupt sicherheitsrelevante Diskurse sind, wie sich unter Umständen wirtschaftliche, politische und zivilgesellschaftliche Themenbereiche vermischen, gilt es zu durchdringen und im Hinblick auf sicherheitsrelevante Aspekte zu analysieren. Sich aufgrund der Komplexität des Themas dieser Debatte zu entziehen, ist in Anbetracht der oben beschriebenen realen Auswirkungen der bereits ausgeübten Soft Power keine ernsthafte Option.

2. Strategisches Kommunikationsmanagement: Kommunikation findet immer statt, Deutungsrahmen werden immer vergeben. Ohne Auftrag und Zielzuweisung versickert aber die eigene, gut gemeinte Kommunikation ungenutzt, die tatsächlich Resilienz, also einen Wertschöpfungsbeitrag erzeugen könnte. Um der von außen, subtil zersetzend wirkenden Kommunikation und ihren realen Folgen etwas entgegenzusetzen, braucht es eben auch nicht mehr, aber auch nicht weniger als „nur“ Kommunikation, die sich ihrer Wirkmächtigkeit bewusst ist und die sich der Deutungshoheit anderer gezielt entgegenstellt. Dies bedeutet gerade nicht, den Gegner oder die Gegnerin mundtot zu machen oder gar zu vernichten, sondern vielmehr den Auftrag ernst zu

nehmen, für eigene Positionen viel deutlicher zu werben und diese strategisch zu legitimieren, das Ergebnis von Kommunikation nicht dem Zufall bzw. dem oder der wie auch immer beschriebenen Gegner oder Gegnerin zu überlassen. Dies setzt auch voraus, tatsächlich eine glaubwürdige, anschlussfähige eigene Position zu entwickeln, um diese dann auch mit Argumenten versehen nach den Regeln des kommunikativen und diskursiven Raumes zu vertreten.

Das wirksamste Mittel, die Widerstandskraft gegen Propaganda zu stärken, ist und bleibt der Aufbau von Vertrauen. Das argumentative Werben um Akzeptanz, die Anschlussfähigkeit auch an gesamtgesellschaftliche Werte, Überzeugungen und Identitäten ist unumgänglich, um Vertrauen aufzubauen. Ausweis von Vertrauenswürdigkeit ist aber auch das Agieren im Diskursraum selbst, gerade unter der Prämisse einer freiheitlichen, offenen Gesellschaftsordnung. Schließlich ist ein Diskurs nur zu führen, wenn andere hieran auch partizipieren. Dies gilt auch für vitale, im Landesinteresse liegende Diskurse – denn wer nicht selbst kommuniziert und einsteht für das, was er als gut und richtig empfindet, überlässt in einer Welt voller Unwägbarkeiten die Deutungshoheit den Anderen und stellt das entgegengebrachte Vertrauen durch ungeschicktes Agieren im Kommunikations- und Diskursraum infrage.

Eine Problematisierung der Kommunikation als Sicherheits-, Stabilisierung- und Verteidigungsfaktor hat bisher nicht (ausreichend) stattgefunden. Im aufklärerischen und romantischen Sinne darauf zu bauen, dass das Wahre, Gute und Schöne – was ja gerade nicht objektivierbar ist – langfristig siegen wird, weil „wir“ im Gegensatz zu den „Anderen“ die Argumente auf unserer Seite haben, wird den Herausforderungen einer wehrhaften Demokratie im 21. Jahrhundert nicht gerecht und ist allenfalls eines: sehr naiv.

45 „So können Sie jedes europäische Land in nur 14 Tagen in die Knie zwingen“. Interview mit Richard Barrons von Konstantin von Hammerstein. In: *Spiegel Online*, 23.5.2020. https://www.spiegel.de/politik/ausland/ex-general-richard-barrons-ueber-den-krieg-der-zukunft-kampfroboter-bekommen-keine-pension-a-058c61c5-e4c2-4845-9d0e-33f3a7a3e4cc (letzter Zugriff: 17.6.2020).

46 Joseph S. Nye: Soft Power: The Means to Success in World Politics. New York: Public Affairs, 2005.

47 Vgl. zu den verschiedenen Doktrinen der US-amerikanischen Sicherheitspolitik: Heiko Meiertöns: The Doctrines of US Security Policy. An Evaluation under International Law. Cambridge: Cambridge University Press, 2010.

48 Interview mit Richard Barrons, op. cit.

49 Bei der sogenannten Geras Gerasimov-Doktrin handelt es sich um eine von Walerij Gerasimov im Januar 2013 vor der Jahresvollversammlung der Akademie der Militärwissenschaften Russlands gehaltene und als Artikel veröffentliche programmatische Rede über die Notwendigkeit neuer Formen und Methoden, Gefechtsoperationen durchzuführen. Vgl. Charles K. Bartles: Getting Gerasimov Right. In: Military Review, January–February 2016, S. 30–38, hier: S. 30.

50 Die hier zitierte, ins Englische übersetzte Passage aus Gerasimovs Artikel ist dem Blogeintrag von Mark Galeotti entnommen, der diesen Text auch erstmalig als Gerasimov-Doktrin bezeichnete und in westlichen Kreisen bekannt machte. Mark Galeotti: The „Gerasimov Doctrine“ and Russian Non-Linear War, 6.7.2014. https://inmoscowsshadows.wordpress.com/2014/07/06/the-gerasimov-doctrine-and-russian-non-linear-war/ (letzter Zugriff: 17.6.2020).

51 AFP: 39 Prozent für Anerkennung der Krim-Annexion. In: *FAZ.net*, 24.11.2014. https://www.faz.net/aktuell/politik/ausland/europa/39-prozent-der-deutschen-fuer-anerkennung-der-krim-annexion-13282878.html (letzter Zugriff: 20.6.2020).

52 Ebd.

53 Andreas Böhnisch, Sebastian Felser: US-Militärexperte fordert Führungsrolle der Bundeswehr in der NATO. In: *SWR Aktuell* vom 23.2.2020. https://www.swr.de/swraktuell/us-militaeruebung-in-europa-100.html (letzter Zugriff: 17.6.2020).

54 Ebd.

55 Ebd.

56 Leopold v. Ranke: Geschichte der germanischen und romanischen Völker von 1494 bis 1535. Vorrede zur ersten Ausgabe. Leipzig, Berlin: Reimer, 1824, S. VI.

57 Francis Fukuyama: The End of History? In: The National Interest 16/1989, S. 3–18.

58 Die durchschnittliche Reichweite der *Tagesschau* betrug im Jahr 2019 9,8 Millionen Zuschauerinnen und Zuschauer. Quelle: Camille Zubayr, Denise Haddad, Lea Hartmann: Nutzungsgewohnheiten und Reichweiten im Jahr 2019. Tendenzen im Zuschauerverhalten. In: Media Perspektiven 3/2020, S. 110–125, hier: S. 115. Das Video „Die Zerstörung der CDU" des Influencers Rezo wurde von seinem Kanal mehr als 17 Millionen Mal heruntergeladen. Quelle: https://www.youtube.com/watch?v=4Y1lZQsyuSQ (letzter Zugriff: 20.6.2020).

59 Claudia Scholz: Scholz lässt Bekenntnis zum Zwei-Prozent-Ziel der Nato aus Regierungsplänen streichen. In: *Handelsblatt Online*, 7.11.2019. https://www.handelsblatt.com/politik/deutschland/verteidigungsetat-scholz-laesst-bekenntnis-zum-zwei-prozent-ziel-der-nato-aus-regierungsplaenen-streichen-/25202258.html?ticket=ST-4991537-a49vdYbCnvkcddoMRaJ6-ap2 (letzter Zugriff: 17.6.2020).

Sicherheit kommunizieren:

Was die Politische Bildung vom Nachrüstungsstreit der 1980er-Jahre lernen kann

Cedric Bierganns

04

In Deutschland bedarf es eines grundlegenden Bekenntnisses unserer Demokratie zur Wehrhaftigkeit. Wie aber kann kommuniziert werden, was unsere Gesellschaft mit unbequemen Wahrheiten konfrontiert, schnell in eine emotionale Angstdebatte umschlägt und seit jeher politisch inopportun scheint? Antworten hält der NATO-Doppelbeschluss bereit, der vor knapp 40 Jahren in der Bundesrepublik die „schärfste sicherheitspolitische Kontroverse ihrer Geschichte“ entfesselte.[60] Die Kohäsion und Deutungshoheit des westlichen Bündnisses auf breiter gesellschaftlicher Ebene sichergestellt zu haben, war das Ergebnis einer geschickten US-amerikanischen Kultur-, Bildungs- und Informationspolitik. Fünf Erkenntnisse von damals, sind für die Politische Bildung auch heute noch hilfreich.

NATO-Doppelbeschluss 2.0?

„Die Geschichte wiederholt sich nicht, aber sie reimt sich." Mit diesem irrtümlich Mark Twain zugeschriebenem Bonmot sind die 1980er-Jahre heute zurück im Zentrum der Debatte über das nukleare Gleichgewicht in Europa. Damals wie heute bedrohten atomar bestückte Raketensysteme an der Ostflanke der NATO die Sicherheit des Kontinents. Im Jahr 1979 waren es sowjetische Mittelstreckenraketen vom Typ SS-20, die die NATO zu einer Doppelstrategie aus Abschreckung und Dialog bewog. Durch ihre feste, beharrliche und einheitliche Haltung leitete das Bündnis in der Folge das Ende des Kalten Krieges ein.

Heute sind es russische Marschflugkörper vom Typ SSC-8, die von Kaliningrad aus nahezu jeden Punkt in Europa erreichen können. Mit Unterstützung aller NATO-Partner haben die USA deshalb den INF-Vertrag (Intermediate Range Nuclear Forces, dt. nukleare Mittelstreckensysteme) gekündigt. Um Deeskalation bemüht, möchte das Bündnis auf eine landgestützte nukleare Gegenstationierung verzichten. Dennoch behält es sich die Option einer Nachrüstung offen. Hochpräzise Langstreckenraketen mit konventioneller Bewaffnung oder seegestützte, nuklear bestückte Marschflugkörper auf U-Booten in europäischen Gewässern sollen die russischen Mittelstreckensysteme bei Bedarf spiegeln können.

Mit der Rückkehr der 1980er-Jahre steht auch die deutsche Bündnisfähigkeit, insbesondere die der deutschen Öffentlichkeit, zur Debatte. Als „größte außerparlamentarische Massenbewegung in der Geschichte der Bundesrepublik" stellte die Friedensbewegung damals den Zusammenhalt und die Verteidigungsbereitschaft des westlichen Bündnisses offen infrage.[61] Ihre diffusen Untergangsängste und die moralische Grundsatzkritik an der Eigendynamik der nuklearen Abschreckung erschwerten den Dialog von staatlicher Seite maßgeblich.

Auch heute kann und will sich eine Mehrheit der Deutschen nicht eingestehen, dass Diplomatie ohne glaubwürdige Gewaltandrohung nichts als heiße Luft ist. Laut einer repräsentativen Umfrage, die Forsa im August 2020 im Auftrag der Münchner Sicherheitskonferenz durchgeführt hat, sind zwei Drittel (66 Prozent) der Auffassung, dass die Bundesrepublik im Rahmen der nuklearen Teilhabe ganz auf die Abschreckung mit Atomwaffen verzichten sollte.[62] Ebenso ernüchternd fiel die Meinungsumfrage des Pew Research Centers in Washington D. C. von 2015 aus, der zufolge sich 58 Prozent der Deutschen dagegen aussprachen, NATO-Verbündete im Falle eines Konflikts mit Russland militärisch zu unterstützen.[63] Nicht berücksichtigt wird, dass die Glaubwürdigkeit die wichtigste psychologische Ressource der Abschreckung ist. „Die Abschreckung ist dann am stärksten", so erläuterte bereits Sicherheitsberater Henry Kissinger, „wenn die militärische Stärke Hand in Hand mit der Bereitschaft geht, sie auch zu gebrauchen."[64] Nach wie vor ist die Androhung von Gewalt wirksamer als ihre tatsächliche Anwendung.

Während des Nachrüstungsstreits der 1980er-Jahren erodierte der sicherheitspolitische Konsens, der sich in der Bundesrepublik seit der Nachkriegszeit in variierender Festigkeit gehalten hatte. Neue Anforderungen erwuchsen an die Kommunikation von Sicherheit, die weit über die bloße Informationspflicht des Staates hinausgingen. Die Legitimität und Legitimationsbedürftigkeit deutscher Verteidigungspolitik änderte sich nachhaltig, sodass heute regelmäßiger, frühzeitiger und tiefgründiger um politischen Rückhalt geworben werden muss. „Denn politische Handlungsfähigkeit ist auch in der Außen- und Sicherheitspolitik immer enger an innenpolitische Zustimmung geknüpft", erklärte Thomas Bagger, Leiter der außenpolitischen Abteilung im Bundespräsidialamt.[65] Daran anknüpfend identifizieren die im November 2020 von der NATO-Reflexionsgruppe unter Leitung von Thomas de Maiziere vorgelegten Reformvorschläge die proaktive Informationsarbeit und den werbenden Dialog mit der Bevölkerung als entscheidend für ein geschlossenes, lebendigeres und stärkeres Bündnis im Jahr 2030.[66] Fünf Erkenntnisse aus den 80er-Jahren zeigen, wie sich die Notwendigkeit der bewaffneten Verteidigung auch heute zielgruppengerecht vermitteln lässt.

Strategiedebatte fördern und genau zuhören

„Der Unwille zu strategischem Denken ist das Grundübel der deutschen und damit zwangsläufig der europäischen Außenpolitik seit dem Ende des Kalten Krieges."[67] Die ernüchternde Bilanz von Stephan Bierling kann nicht darüber hinwegtäuschen, dass zumindest vonseiten der deutschen Öffentlichkeit in den letzten Jahren ein gesteigertes Interesse an der Außen- und Sicherheitspolitik zu verzeichnen ist. Entgegen dem gern kolportierten Mantra, dass dieses Fachgebiet lediglich wohlwollend zur Kenntnis genommen werde und nicht zu vermitteln sei, interessiert sich laut der Umfrage der Münchner Sicherheitskonferenz eine deutliche Mehrheit von 64 Prozent der Deutschen „stark" oder „sehr stark" für außen- und sicherheitspolitische Themen.[68] Dieses Potenzial sollte am Anfang einer neuen strategischen Debattenkultur in Deutschland stehen, die den Willen und die Fähigkeit zur außen- und sicherheitspolitischen Selbstbehauptung ins Zentrum rückt. Als Demokratie „strategiefähig" zu sein, heißt, im Einklang mit der breiten Öffentlichkeit über die Kunst der Vereinbarkeit von Mitteln und Zielen nachzudenken, und sich dabei auf ein annäherndes Gleichgewicht zwischen diesen zu verständigen. Dabei haben Bürgerinnen und Bürger laut Verteidigungsministerin Annegret Kramp-Karrenbauer ein Recht darauf, auch mit unbequemen Wahrheiten konfrontiert zu werden: „Wer glaubt, das nicht zu können oder nicht zu dürfen, der ist arrogant. Der respektiert die Menschen nicht. Der behandelt sie wie Unmündige."[69] Der Bevölkerung ist also ein neuer Realismus zuzutrauen, der die Welt nüchtern sieht, wie sie ist, und nicht, wie sie sein sollte. „Für Deutschland gibt es keine sicherheitspolitische Nische mehr", konstatiert Ekkehard Brose, Präsident der Bundesakademie für Sicherheitspolitik.[70] Zeiten des rasanten Wandels, in denen alte Gewissheiten brüchig geworden sind, verlangen weniger nach geistiger Selbstverzwergung als vielmehr den mutigen Blick in die Welt hinaus. „Mehr Verantwortung" zu übernehmen heißt, mit kalkuliertem Risiko den Sprung ins Dunkle zu wagen und dabei insbesondere für seine Fehler geradezustehen. Denn niemand übernimmt die „Verantwortung" für

Erfolge. Selbst- und Fremdwahrnehmung der neuen deutschen „Macht in der Mitte“ Europas sollten kontinuierlich abgeglichen und miteinander in Einklang gebracht werden.[71] Dabei ist der Bundestag der natürlichste Ort für eine Strategiedebatte. Was hier von den Parteien erörtert, abgewogen und beschlossen wird, ist für den Rückhalt in der Bevölkerung entscheidend. Deutsche Außen- und Sicherheitspolitik kann mithilfe der Politischen Bildung erklärt und kontextualisiert, nicht aber grundsätzlich in ihrer Attraktivität aufgewertet werden. Heute wie in den 1980er-Jahren gilt: Was keinen Glanz hat, bleibt glanzlos.

Die Strategiedebatte zu fördern ist das eine, genau zuzuhören etwas anderes. Während der Auseinandersetzung um den NATO-Doppelbeschluss kamen Stimmungsbildern, die weit über die bloße Wiedergabe der veröffentlichten Meinung hinausgingen, eine wichtige Schlüsselfunktion zu. Sie lieferten Informationen über abweichende Sichtweisen, Hoffnungen und Ängste der Deutschen und halfen den Vereinigten Staaten ganz wesentlich dabei, ihre Außenpolitik besser an die öffentliche Erwartungshaltung im Bündnis anzupassen. Wer heute genau hinhört, der kann feststellen, unter welchen Bedingungen die Deutschen etwa für den Einsatz der Bundeswehr empfänglich sind. Markus Steinbrecher vom Zentrum für Militärgeschichte und Sozialwissenschaften der Bundeswehr (ZMSBw) belegt mit seinem Framing-Experiment auf Grundlage jährlicher Umfragedaten, dass der Streitkräfteeinsatz in einem Artikel-5-Szenario umso eher akzeptiert wird, je stärker auf die Verpflichtungen des NATO-Vertrages oder die Solidarität der Bündnispartner hingewiesen wird. Dahingegen sinkt die Zustimmungsrate, wenn zunehmende Spannungen als Begründung vorgebracht werden.[72] Auch die NATO-Reflexionsgruppe empfiehlt verstärkte Investitionen in Instrumente der Zuschauer- und Publikumsforschung, inklusive der Möglichkeiten, die sich aus datengesteuerten Analysewerkzeugen für das digitale Nutzerverhalten ergeben.[73] Dem politischen Bildner oder der politischen Bildnerin bieten sich interaktive Umfragetools wie „Slido“ oder „Mentimeter“ an, die in Onlineveranstaltungen oder in Hybridformaten Einsicht in die Meinungen der Teilnehmerinnen und Teilnehmer ermöglichen und die Echtzeitdatenerhebung zu einem spannenden Liveerlebnis machen.

Bedrohungsbewusstsein schärfen und Zusammengehörigkeitsgefühl stärken

Feindbilder sind so alt wie die Menschheit. Auch während der Nachrüstungsdebatte besaßen sie ein starkes mentales Mobilisierungspotenzial, integrierten und solidarisierten den eigenen Gruppenverband und stärkten die westlichen Verteidigungsreflexe. Indem Michail Gorbatschow mit seinem neuen Politikstil ab 1985 alte Feindbilder bewusst verblassen ließ, schwand der für das Bündnis konstitutive Außendruck und stellte die NATO vor die Herausforderung einer nachlassenden gesellschaftlichen Integrationskraft.

Unter all den existenziellen Bedrohungen der Gegenwart – von Pandemien und Cyberangriffen über hochmoderne Waffensysteme und die Krise der Rüstungskontrolle bis hin zur zerfallenden Staatlichkeit in Nordafrika und dem islamistischen Terrorismus – gleicht der internationale Wettbewerb mit aufsteigenden Systemrivalen am ehesten der binären Ordnungslogik des Kalten Krieges. China stellt dem westlichen Modell der offenen Gesellschaft, der Demokratie und des Rechtsstaats eine autoritäre Alternative gegenüber und verlangt nach einer politischen Langzeitstrategie, die das Riesenreich zu Mäßigung und Zurückhaltung bewegt.[74] Laut einer alarmierenden Umfrage der Körber-Stiftung, die im April 2020 unter dem Eindruck der Corona-Pandemie zustande kam, halten 36 Prozent der Deutschen enge Beziehungen zu China mittlerweile für wichtiger als zu den USA.[75] Im November 2019 befürwortete nur eine knappe Mehrheit von 55 Prozent der Bundesbürgerinnen und Bundesbürger die Zugehörigkeit Deutschlands zur westlichen Staaten- und Wertegemeinschaft.[76] Wertrelativismus und Geschichtsvergessenheit machen sich bemerkbar. Vier Jahre Donald Trump und die „Hirntod"-Debatte um die NATO scheinen ihre Spuren im deutschen USA-Bild

hinterlassen zu haben. Hatten vor zehn Jahren noch knapp drei Viertel der Bundesbürgerinnen und Bundesbürger einen positiven Blick auf das Bündnis, sind es heute nur noch 57 Prozent.[77] Nur 27 Prozent der Befragten halten die USA in Fragen der militärischen Verteidigung für den wichtigsten Bündnispartner (Frankreich 48 Prozent).[78] Um das transatlantische Verhältnis wiederzubeleben und die gesellschaftliche Resilienz gegenüber Desinformation zu stärken, kommt der politischen Bildung zukünftig eine Schlüsselaufgabe zu. Norbert Lammert zufolge soll sie „die Zivilgesellschaft gegen ausländische Einflussnahme, die unsere Demokratien unterminieren, imprägnieren."[79]

Auch die 1980er-Jahre wurden vielfach als eine Zeit der transatlantischen Entfremdung empfunden. Besonders in Präsident Ronald Reagan, einem glühenden Antikommunisten, doch zugleich überzeugten Atomwaffengegner, kulminierten die Ängste friedensbewegter deutscher Kritikerinnen und Kritiker. Mit dem viel zitierten Verortungsbegriff der „westlichen Wertegemeinschaft" rückten die Vereinigten Staaten in dieser Zeit das identitätsstiftende Narrativ einer gemeinsamen Vergangenheit ins Zentrum ihrer auswärtigen Kultur-, Bildungs- und Informationspolitik. Eine solche Meistererzählung, „mit [der] Gesellschaften ihre Vergangenheit und Gegenwart verstehen und in deren Licht sie ihre Zukunft antizipieren", hat David Gress in der Formel „From Plato to NATO" gefunden, die die Vorstellung vom Westen auf den kleinsten gemeinsamen Nenner eines fortschrittsorientierten, liberaldemokratischen Antitotalitarismus reduzierte.[80]

In Übereinstimmung mit den Ergebnissen des NATO-Reflexionsprozesses sollte das wertebasierte euroatlantische Situationsverständnis erneuert werden.[81] Für Deutschland bietet sich dazu das „Schicksalsjahr" 2049 als Bezugspunkt an. Dann wird nicht nur das Grundgesetz sein 100-jähriges Jubiläum feiern, sondern auch der Lauf der Geschichte darüber entschieden haben, ob China das durch die Kommunistische Partei selbstgesteckte Ziel, zur führenden politisch-militärischen Weltmacht aufzusteigen, erreicht hat. In diesem internationalen Systemwettbewerb sind „Handlungsfähigkeit", „Selbstbehauptung" und „wehrhafte Demokratie" positiv besetzte Fahnenwörter, die große Suggestivwirkung entfalten.

Sie können dem Themenkontinuum Staatskapitalismus, Überwachungssystem und Umerziehungslager gegenübergestellt werden. Die historische Erfahrung, dass die Menschheit und die Menschlichkeit geschändet werden kann, verstehen die meisten Deutschen jedoch nicht als Verantwortung vor der Geschichte. Laut Umfrage der Münchner Sicherheitskonferenz ist eine knappe Mehrheit der Befragten (56 Prozent) der Auffassung, dass sich aus der deutschen Vergangenheit mehrheitlich keine besondere Verantwortung ergibt, sich für den Frieden in der Welt einzusetzen.[82]

Das Globale im Lokalen veranschaulichen

Durch die Reduktion von Komplexität und das Herunterbrechen auf die Alltagsrealitäten der Durchschnittsbürgerinnen und -bürger gewinnt die transatlantische Sicherheitspolitik an Anschaulichkeit. Beispielsweise nutzten Bonn und Washington im Sommer 1983 das 300. Gedenkjahr der deutschen Einwanderung in die Vereinigten Staaten, um die transatlantische Waffenbrüderschaft im Jahr der Raketenstationierung in einem lokalen Kontext erfahrbar zu machen. Mit der Ansprache von Vizepräsident George H. W. Bush auf dem von Krawallen überschatteten Festakt in der Stadt Krefeld – Entstehungsort des gleichnamigen Protestappells – fand die für den NATO-Doppelbeschluss so charakteristische Verknüpfung des Regionalen mit dem Internationalen ihren Höhepunkt.

Auch heute können globale Zusammenhänge in lokalen Kontexten veranschaulicht werden. Anfang des Jahres 2020 rollte im Rahmen des Großmanövers DEFENDER-Europe 20 schweres Gerät durch Nordrhein-Westfalen. Die umfangreichste Truppenverlegung der USA nach Europa war für die Konrad-Adenauer-Stiftung Anlass, um unter dem Veranstaltungstitel „Drehscheibe NRW" das Transitland als wichtige Nachschublinie zwischen den Tiefwasserhäfen der Nordsee und den multinationalen Kampftruppen in Polen und im Baltikum zu behandeln.[83] Die Folgeübung Steadfast Defender im Jahr 2021 bietet weitere Anknüpfungspunkte, um Sicherheitspolitik für die Bürgerinnen und Bürger vor Ort erfahrbar zu machen.

Indirekte Zugänge wählen und Sachthemen vermenschlichen

„Den stärksten Anlass zum Handeln bekommt der Mensch immer durch Gefühle", war ausgerechnet der nüchtern kalkulierende Militärstratege Carl von Clausewitz überzeugt.[84] Schon während der Debatte um den NATO-Doppelbeschluss argumentierten Nachrüstungsgegnerinnen und -gegner sowie Nachrüstungsbefürworterinnen und -befürworter in disparaten Denksystemen aneinander vorbei, weil sich der in moralisch-existenziellen Kategorien geführte Angstdiskurs der Friedensbewegung einer sachlichen Argumentation entzog. Im Angesicht des vermeintlichen Atomtods verschlossen sich die Gefühle vor der Ratio – ein Befund, der heute auch auf den weltweiten Klimaprotest zutrifft.

Politische Bildung ist mehr als die bloße Anhäufung von Wissen, sondern soll zum emotionalen Lernen anregen und Begeisterung entfachen. In den 1980er-Jahren wählten die sogenannten „Amerikahäuser" bspw. die allgemeinverständliche Sprache der Musik, um in der erhitzten Raketenkontroverse die emotionale Westbindung ihrer Besucherinnen und Besucher zu stärken.

Indem Politik mit Persönlichkeit verknüpft wird, kann komplexen Sachverhalten eine menschliche Dimension gegeben werden. Mit ihrem Podcast „Erststimme", der seit 2020 im Zweiwochenrhythmus auf allen gängigen Plattformen abrufbar ist, stellt die Konrad-Adenauer-Stiftung ganz gezielt die Person hinter dem Thema in den Mittelpunkt. So berichtet bspw. Nariman Hammouti, Muslima, Kind marokkanischer Eltern und Leutnant zur See, über die Bundeswehr als Integrations- und Gleichstellungsmotor. Dr. Peter Tauber, ehem. Parlamentarischer Staatssekretär im Bundesministerium der Verteidigung, verrät, was ihn persönlich antreibt und gewährt Einblicke in sein Leben zwischen Haltung, Verantwortung und Truppe.[85]

Heute wissen wir, dass sich Meinungen nicht durch Informationen aus erster Hand formieren, sondern durch Versatzstücke von dem, „was andere berichtet haben und was wir uns vorstellen können."[86] Abhängig vom persönlichen Lebensumfeld eignen sich Menschen ihre Überzeugungen also eigenwillig und selektiv an. Um den Eindruck zu vermeiden, man vertrete eine Einzelmeinung, sollte die politische Bildnerin oder der politische Bildner keine Maßnahmen ohne unabhängige Kooperationspartnerinnen und -partner planen und durchführen. Die NATO-Reflexionsgruppe empfiehlt, den Kontakt zu internationalen Organisationen, dem Privatsektor, Denkfabriken und der Wissenschaft auszubauen und der zwischenmenschlichen Begegnung auch im Zeitalter der digitalen Kommunikation genügend Raum zu geben.[87]

Junge Zielgruppen erschließen

Der Zukunftsentwurf einer Gesellschaft spiegelt sich v. a. in ihrer Jugend. Ihr sicherheitspolitisches Grundverständnis ist noch nicht ausgeprägt und deshalb formbar. In den 1980er-Jahren schlossen die Vereinigten Staaten neben der Raketenlücke auch eine Generationslücke, indem sie mit dem „Youth Exchange Initiative Act" den Grundstein für einen verstärkten Jugendaustausch mit der Bundesrepublik legten. Das daraus hervorgegangene „Parlamentarische Patenschaftsprogramm" hat den Kalten Krieg bis in die Gegenwart hinein überlebt.

Anders als die sogenannte Nachfolgegeneration, die damals in US-amerikanischen Augen zu Wertrelativismus und geistiger Unentschlossenheit neigte, sind es heute v. a. Angehörige der sogenannten Generation Z (18- bis 30-Jährige), die deutlich häufiger als andere Altersgruppen ein größeres internationales Engagement der Bundesrepublik befürworten.[88] Die jüngste Forsa-Umfrage im Auftrag der Münchner Sicherheitskonferenz verdeutlicht, dass 51 Prozent dieser Alterskohorte der Meinung sind, dass sich Deutschland in Zukunft „stärker als bisher" bei der Lösung von Konflikten in der Welt beteiligen sollte.[89] Als besonders dringlich werden die Themen Klimakrise, Friedenssicherung/Konfliktvermeidung und Terrorismusbekämpfung genannt.[90]

Das gestiegene sicherheitspolitische Interesse junger Menschen greift die Konrad-Adenauer-Stiftung mit einwöchigen Summer Schools auf, die sich mit Fachvorträgen, Workshops und Exkursionen an engagierte Schülerinnen und Schüler eines Abiturjahrganges richten. Um die Entscheidungsträgerinnen und -träger von morgen zu erreichen, wird die Zusammenarbeit mit den Jugendoffizieren der Bundeswehr, dem Bundesverband Sicherheitspolitik an Hochschulen (BSH), der Jungen DGAP (Deutsche Gesellschaft für Auswärtige Politik), der Jungen GSP (Gesellschaft für Sicherheitspolitik), der studentischen Denkfabrik Polis180 oder auch der Initiative junger Transatlantiker empfohlen.

Schlussbemerkung: Sicherheitspolitik und Öffentlichkeit in weltpolitischen Wendezeiten

Demokratische Außen- und Sicherheitspolitik ist nach außen nur so handlungsfähig, wie sie im Inneren von den Bürgerinnen und Bürgern mitgetragen wird. Wie der überwiegende Teil der Menschheitsgeschichte wird auch das nächste Jahrzehnt mit naturgesetzmäßiger Wahrscheinlichkeit von gewaltsamen Konflikten geprägt sein, die „diffuser, vielfältiger und disruptiver" ausgetragen werden.[91] Dieser niederschmetternden Realität historischer Erfahrung kann sich auch die politische Bildnerin und der politische Bildner sowie die deutsche Gesellschaft nicht entziehen. „Wasch mich, aber mach mich nicht nass", könnte ihre außen- und sicherheitspolitische Grundeinstellung lauten. Zwar möchte eine wachsende Mehrheit insbesondere in einem multilateralen Rahmen „mehr Verantwortung" übernehmen, doch vor der Androhung oder Anwendung von Gewalt schrecken die Bürgerinnen und Bürger in unserer wehrhaften Demokratie immer noch reflexartig zurück.[92] Über 75 Friedensjahre hinweg haben sich die Deutschen zu einer „postheroischen Gesellschaft" entwickelt, die ihre Identität aus historisch nachvollziehbaren Gründen aus der Ablehnung von Heldentum und nationalem Opfermut bezieht.[93] Doch heute, 30 Jahre nach der Wiedervereinigung, kann nur ein verantwortungsbereites Deutschland in einem wehrhaften Europa ein attraktiver Partner für seinen engsten Verbündeten sein. „Es geht darum, unsere Einflussmöglichkeiten – oder mit anderen Worten: unsere Macht – realistisch einzuschätzen und klug zu nutzen", wie Bundestagspräsident Wolfgang Schäuble verdeutlicht hat. „Nicht nur das, was wir tun, sondern auch das, was wir nicht tun, wirkt sich anderswo in der Welt aus."[94] Der Auftrag, den uns das Grundgesetz erteilt, ist eindeutig: „Als gleichberechtigtes Glied in einem vereinten Europa dem

Frieden der Welt dienen“. Auf welche Weise wir das tun wollen, darüber muss auf breiter gesellschaftlicher Ebene gesprochen und gestritten werden. 40 Jahre Friedensdemonstration im Bonner Hofgarten werden uns im Oktober 2021 Anlass dazu geben.

60 Rödder, Andreas: Bündnissolidarität und Rüstungskontrollpolitik. Die Regierung Kohl-Genscher, der NATO- Doppelbeschluss und die Innenseite der Außenpolitik. In: Gassert, Philipp/Geiger, Tim/Wentker, Hermann (Hrsg.): Zweiter Kalter Krieg und Friedensbewegung: Der NATO-Doppelbeschluss in deutsch-deutscher und internationaler Perspektive. München: Oldenbourg 2011, S. 124.

61 Das Zitat stammt aus Wirsching, Andreas: Abschied vom Provisorium: Geschichte der Bundesrepublik Deutschland 1982–1990. München: Deutsche Verlags-Anstalt 2006, S. 86.

62 Vgl. Zeitenwende – Wendezeiten: Sonderausgabe des Munich Security Report zur deutschen Außen- und Sicherheitspolitik, Oktober 2020, S.127. https://securityconference.org/assets/01_Bilder_Inhalte/03_Medien/02_Publikationen/MSC_Germany_Report_10-2020_De.pdf (letzter Zugriff: 15.12.2020).

63 Vgl. Pew Research Center: NATO Publics Blame Russia for Ukrainian Crisis, but Reluctant to Provide Military Aid, 10.6.2015. https://www.pewresearch.org/global/2015/06/10/nato-publics-blame-russia-for-ukrainian-crisis-but-reluctant-to-provide-military-aid/ (letzter Zugriff: 15.12.2020).

64 Kissinger, Henry: Kernwaffen und Auswärtige Politik. München: Oldenbourg 1959, S. 112.

65 Bagger, Thomas: Strategiebildungsprozesse. Chancen und Grenzen. In: Jacobi, Daniel/Hellmann, Gunther (Hrsg.): Das Weißbuch 2016 und die Herausforderungen von Strategiebildung: Zwischen Notwendigkeit und Möglichkeit. Wiesbaden: Springer VS 2019, S. 113.

66 Vgl. NATO 2030: United for a New Era. Analysis and Recommendations of the Reflection Group Appointed by the NATO Secretary General, 25. 11.2020, S. 49. https://www.nato.int/nato_static_fl2014/assets/pdf/2020/12/pdf/201201-Reflection-Group-Final-Report-Uni.pdf (letzter Zugriff: 15.12.2020).

67 Bierling, Stephan: „Germany first“: Deutschland fehlt der Wille zum strategischen Denken. *NZZ*, 15.12.2020. https://www.nzz.ch/meinung/germany-first-deutschland-fehlt-der-wille-zum-strategischen-denken-ld.1591983 (letzter Zugriff: 15.12.2020).

68 Vgl. Zeitenwende – Wendezeiten, S. 107.

69 Zweite Grundsatzrede der Verteidigungsministerin an der Helmut-Schmidt-Universität/Universität der Bundeswehr am 17.11.2020 in Hamburg: https://www.bmvg.de/de/aktuelles/zweite-grundsatzrede-verteidigungsministerin-akk-4482110 (letzter Zugriff: 15.12.2020).

70 Brose, Ekkehard: Raus aus der Nische: Sicherheitspolitik braucht mehr Debatten und Rückhalt in der breiten Öffentlichkeit. *Der Tagesspiegel*, 6.10.2020. https://www.tagesspiegel.de/politik/sicherheitspolitik-darf-kein- nischenthema-bleiben-regierung-und-parlament-muessen-fuer-rueckhalt-in-der-gesellschaft-werben/26238736.html (letzter Zugriff: 15.12.2020).

71 Vgl. Münkler, Herfried: Macht in der Mitte. Die neuen Aufgaben Deutschlands in Europa. Hamburg: Edition Körber 2015.

72 Vgl. Steinbrecher, Markus: Cold War Revisited? Germany and the Renaissance of Alliance Defense. Vortrag im Rahmen der Gesis Lecture Series 2017/8 in Mannheim, 6.3.2018. https://www.gesis.org/fileadmin/upload/events/Vortragsreihe/MA_2018306_Steinbrecher_GESIS.pdf (letzter Zugriff: 15.12.2020).

73 Vgl. NATO 2030: United for a New Era, S. 48.

74 Vgl. ebd., S. 12

75 Vgl. Körber-Stiftung: Transatlantische Partnerschaft verliert an Rückhalt, 18.5.2020. https://www.koerber-stiftung.de/transatlantische-partnerschaft-verliert-an-rueckhalt-36-prozent-der-deutschen-finden-enge-beziehungen-zu-china-wichtiger-als-zu-den-usa-2066 (letzter Zugriff: 15.12.2020).

76 Vgl. Körber-Stiftung: Einmischen oder zurückhalten?, 26.11.2019. https://www.koerber-stiftung.de/berliner-forum-aussenpolitik/news-detailseite/deutsche-hinterfragen-westliche-staaten-und-wertegemeinschaft-1927 (letzter Zugriff: 15.12.2020). Gleichwohl ist eine deutliche Mehrheit von 61 Prozent der Auffassung, dass Deutschland bei der Durchsetzung seiner Interessen gegenüber Peking zu zurückhaltend agiere. Unklar bleibt, welche wirtschaftlichen Konsequenzen die Befragten für eine härtere Gangart zu tragen bereit sind. Siehe dazu Zeitenwende – Wendezeiten, S. 120.

77 Vgl. Pew Research Center: NATO Seen Favorably Across Member States, 9.2.2020. https://www.pewresearch.org/global/2020/02/09/nato-seen-favorably-across-member-states/ (letzter Zugriff: 15.12.2020).

78 Vgl. Zeitenwende – Wendezeiten, S. 125.

79 Lammert, Norbert: Das transatlantische Verhältnis nach Trump: Ein Neustart. *Der Spiegel*, 3.1.2021. https://www.spiegel.de/politik/norbert-lammert-ueber-das-transatlantische-verhaeltnis-nach-donald-trump-a-adf2feca-4065-4fcb-8cf9-4522732f6349 (letzter Zugriff: 11.5.2021).

80 Vgl. Gress, David: From Plato to NATO. The Idea of the West and Its Opponents. New York: Free Press 1998, S. 1–48 u. S. 407–462. Zur Meistererzählung Perthes: Volker/Mair, Stefan: Ideen und Macht. Was definiert die relative Gewichtsverteilung in der Welt? In: Internationale Politik, 3 (2011), S. 12.

81 Vgl. NATO 2030: United for a New Era, S. 51.

82 Vgl. Zeitenwende – Wendezeiten, S. 108.

83 Konrad-Adenauer-Stiftung: Drehscheibe NRW. Das Transitland im Zentrum der Weltpolitik, 6.7.2020. https://www.kas.de/de/web/bundesstadt-bonn/veranstaltungen/detail/-/content/drehscheibe-nrw-das-transitland-im-zentrum-der-weltpolitik (letzter Zugriff: 15.12.2020).

84 Clausewitz, Carl von: Vom Kriege. Vollständige Ausgabe, 8. Aufl. Hamburg: Nikol 2016, S. 89. [Erstausgabe Berlin, 1832].

85 Vgl. Konrad-Adenauer-Stiftung: Erststimme. Der Podcast für alles außer Corona. https://podcasts.apple.com/de/podcast/erststimme-der-podcast-für-alles-außer-corona/id1528379178 (letzter Zugriff: 15.12.2020).

86 Lippmann, Walter: Public Opinion. Miami: BN Publishing 2010, S. 63 [Erstausgabe New York, 1922].

87 Vgl. NATO 2030: United for a New Era, S. 49.

88 Vgl. Global Public Policy Institute (GPPI): Neue Erwartungen. Generation Z und der Einstellungswandel zur Außenpolitik, 6.7.2020. https://www.gppi.net/2020/06/06/neue-erwartungen-generation-z-und-der-einstellungswandel-zur-au%C3%9Fenpolitik (letzter Zugriff: 15.12.2020).

89 Vgl. Zeitenwende – Wendezeiten, S. 112.

90 Vgl. ebd.

91 Das Paradox des Fortschritts: Die Welt im Jahr 2035 gesehen von der CIA und dem National Intelligence Council, 2. Aufl., München: C. H. Beck 2018, S. 300.

92 Vgl. Zeitenwende – Wendezeiten, S. 115 f., 128 u. 138. Siehe auch Graf, Timo: Einstellungen zum außen- und sicherheitspolitischen Engagement Deutschlands. In: Ders./Steinbrecher, Markus/Biehl, Heiko (Hrsg.): Sicherheits- und verteidigungspolitisches Meinungsbild in der Bundesrepublik Deutschland: Ergebnisse und Analysen der Bevölkerungsbefragung 2019. Potsdam: ZMSBw 2019, S. 44 u. S. 47–49.

93 Vgl. hierzu Münkler, Herfried, Kriegssplitter. Die Evolution der Gewalt im 20. und 21. Jahrhundert. – Reinbeck bei Hamburg: Rowohlt 2017, S. 169–187.

94 Bundestagspräsident Wolfgang Schäuble: Globale Verantwortung als nationale Herausforderung. Rede beim Festakt zur Verabschiedung von Volker Perthes als Direktor der Stiftung Wissenschaft und Politik in Berlin, 9.9.2020: https://www.swp-berlin.org/fileadmin/contents/products/sonstiges/200909_RedeBundestagspraesident-Schaeuble.pdf (letzter Zugriff: 15.12.2020).

Bildung für Medienkompetenzen zum Resilienzaufbau gegen Informationsbedrohungen

Forschungsstand und Lektionen aus Finnland

Jan Wilhelm Ahmling

05 Zur Begegnung von Informationsbedrohungen und zur gleichzeitigen Stärkung des demokratischen Diskurses setzen Regierungen weltweit auf unterschiedliche politische Maßnahmen. Als politische Maßnahme gegen diese Entwicklung wird die Vermittlung von Medienkompetenz eine besondere Rolle beigemessen. Die vorliegende Analyse zeigt, dass Medienkompetenz – speziell verstanden als Informationskompetenz – einen Beitrag liefern könnte der Wirkung von Informationsbedrohungen entgegenzuwirken. Das behandelte finnische Beispiel verdeutlicht, dass Informationskompetenz als interdisziplinäres Feld nicht allein als Schulfach gedacht werden kann, sondern vielmehr als staatlich-initiiertes und gesellschaftlich getragenes Ökosystem zur Medienkompetenzvermittlung seine Wirkung entfaltet.

Informationsbedrohungen und Medienkompetenz

Frei verfügbare, valide Informationen sind elementar für die Identität von und den politischen Diskurs in liberalen Demokratien, denn auf ihrer Grundlage kann grundsätzlich eine demokratische, kollektive Meinungsbildung im Informationsraum gelingen.[95] Die Integrität des Informationsraumes und die Beeinflussung der kognitiven, psychologischen, ideologischen und moralischen Charakteristika des Zielpublikums sind das Ziel von Influence Operations[96]. Sie sind als wesentliche hybride Sicherheitsbedrohung für die Mitgliedstaaten der EU[97] und der NATO[98] identifiziert.

Das Aufkommen von medial übergreifenden Desinformationskampagnen staatlicher und nicht-staatlicher Akteure nimmt zu. Während 2017 nachweislich 28 Staaten in solchen aktiv waren, ist die Zahl 2018 auf 48 und 2019 auf 78 Staaten gestiegen.[99] Im Rahmen der globalen Covid-19-Pandemie waren ebenfalls unterschiedliche Akteure an Desinformationskampagnen beteiligt.[100] Wenngleich Information Operations kein neuer Trend sind,[101] haben digitale Informationskanäle die Bedeutung und Anwendungsformen verändert. Medial und auch politisch ist in diesem Zusammenhang der Sammelbegriff „Fake News" zur Beschreibung weit verbreitet. Dieser Begriff weist jedoch eine mangelnde inhaltliche Trennschärfe auf.[102] Daher wird im Folgenden allgemein von Informationsbedrohungen[103] für unterschiedliche Phänomene im Informationsraum gesprochen.

Zur Begegnung dieser Bedrohungen und zur gleichzeitigen Stärkung des demokratischen Diskurses setzen Regierungen weltweit auf unterschiedliche politische Maßnahmen. Als politische Maßnahme gegen diese Entwicklung wird die Vermittlung von Medienkompetenz als „most widely agreed-upon recommendation"[104] betrachtet. Dennoch haben bislang nur wenige Regierungen explizit Bildungsmaßnahmen zur Stärkung von Medienkompetenz als Maßnahmen gegen Informationsbedrohungen im Fokus.[105]

Um Informationsbedrohungen als Herausforderung für den demokratischen Diskurs zu entgegnen, stellt diese Arbeit dar, welche Möglichkeit die Vermittlung von Medienkompetenz bietet. Zuerst wird der Begriffskomplex Informationsbedrohungen definiert und die Auswirkungen dargestellt. Danach werden mögliche politische Gegenmaßnahmen unter Differenzierung der systemischen und individuellen Wirkungsweise präsentiert. Ziel ist es, den möglichen Beitrag der Vermittlung von Medienkompetenz gegen Informationsbedrohungen zu analysieren. Dieser wird am Beispiel von Finnland überprüft, welches als herausragendes Beispiel in der Vermittlung von Medienkompetenz gegen Informationsbedrohungen benannt wird.[106] Abschließend werden Fragestellungen für die weitere Forschung und Schlussfolgerungen zusammengefasst.

Bedrohter Informationsraum

Informationsraum meint als Sammelbegriff unterschiedliche Nachrichtenplattformen, auf denen Nachrichten, Medieninhalte und Meinungen geteilt werden. Dazu zählen Medien wie Print, TV, Radio, Webseiten, soziale Medien genauso wie Blogs, Apps, Messengerdienste, E-Mails und das Telefon.[107] Dieser valide Informationsraum wird durch drei wesentliche gesellschaftliche Trends verändert und herausgefordert: die Fragmentierung von gesellschaftlicher Autorität, das Erstarken von Silodenken und eine Sprachverrohung im Sinne einer „persistent ‚trolling' ethic of cynical and aggressive harassment in the name of an amorphous social dissent."[108]

Zusätzlich können soziale Medien die Existenz von Echokammern und Filterblasen – also sich selbst referenziellen Nachrichtenräumen – verstärken.[109] Sie befördern den Trend einer größeren Konsumentendifferenzierung[110] und fördern so die Differenzierung und auch Radikalisierung von Meinungen. Die physische Distanz der Kommunikation und der damit verbundene Prozess von besonderen Gruppendynamiken werden als einer der Gründe für einen unhöflichen und verrohten Diskurs gesehen.[111] Mediennutzende weltweit nehmen daher soziale Medien als Hauptquelle von Informationsbedrohungen wahr.[112] Gleichzeitig lässt sich beobachten, dass die Nutzung von sozialen Medien als Nachrichtenquellen ansteigt.[113]

Im Ergebnis wird die Wahrnehmung vom Wahrheitsgehalt der vorliegenden Informationen zunehmend durch Teile der Bevölkerung infrage gestellt. Dieses Umfeld des Wahrheitsverfalls[114] schafft erste Voraussetzungen für das Wirken von Informationsbedrohungen.

Desinformation, Misinformation & Malinformation

Informationsbedrohungen bezeichnen Instrumente, Taktiken und Strategien, die das fragil gewordene Vertrauen in den Wahrheitsgehalt der Informationen im Informationsraum weiter gefährden. Grundsätzlich lassen sich hier Desinformation, *Misinformation* und *Malinformation* voneinander unterscheiden:[115]

- **Desinformation** bezeichnet dabei falschen oder irreführenden Inhalt, der absichtlich verbreitet wird, um ein ökonomisches oder politisches Ziel zu erreichen oder zu stören. Dabei kann Schaden durch öffentliches Misstrauen entstehen.
- **Misinformation** bezeichnet falschen oder irreführenden Inhalt, der verbreitet wird, ohne einen direkten, gezielten Schaden anrichten zu wollen. Der Schaden, also der Vertrauensverlust, kann dennoch entstehen.
- **Malinformation** schließlich meint die Verbreitung von Inhalten, die zum Teil auf wahren Bestandteilen basieren, mit dem Ziel, Personen, Organisationen oder politische Entscheidungen zu schädigen.

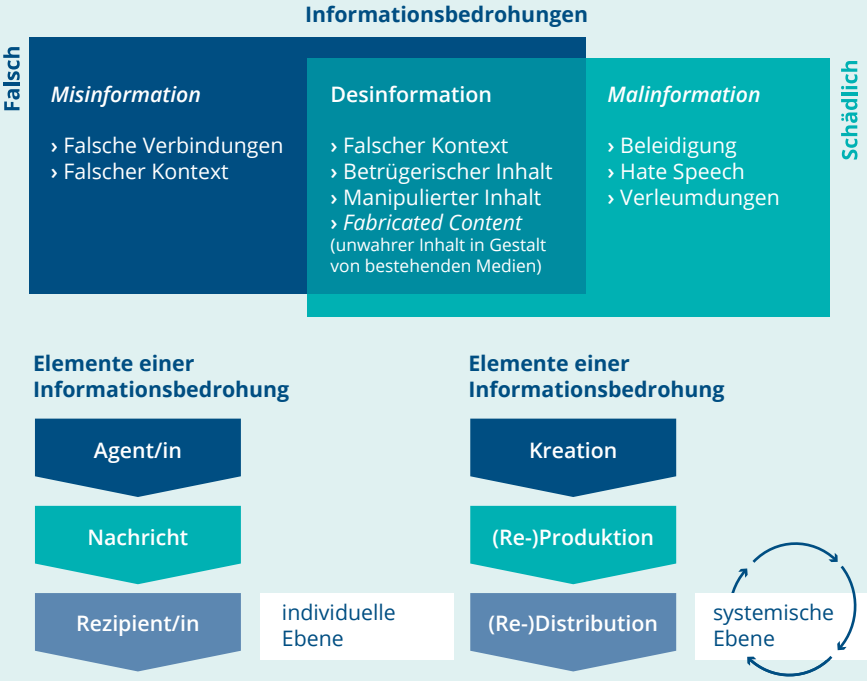
Die unterschiedenen Bedrohungsarten können auch kulminiert in Influence Operations wirken. Diese wiederum machen sich dabei Vorteile von sozialen Medien zunutze. Zum einen ist dies die gesteigerte Effektivität zum Erreichen des Zielpublikums,[116] zum anderen die kostengünstige Produktion der Informationen.[117]

Die Verbreitung von entsprechenden Bedrohungen ist grundsätzlich nicht vermeidbar und ein Bestandteil der Mediengesellschaft.[118] Die genauen gesellschaftlichen Wirkungseffekte und Schäden sind nicht direkt messbar, jedoch gibt es Beispiele für einen Wirkungszusammenhang.[119]

Informationsbedrohungen wirken dabei auf dem Nährboden von gesellschaftlichen Entwicklungen und verstärken die Ungleichheiten und Bruchlinien in der Gesellschaft. Hierzu zählen neben den o. g. Veränderungen die Umstrukturierungen des Medienmarktes und die Dynamiken des digitalen Informationsraumes.[120] Informationsbedrohungen wirken als permanenter schleichender Prozess gesellschaftlicher und diskursiver Veränderung und nicht für sich allein.

Die folgende Grafik fasst die Wirkungsweise von Informationsbedrohungen in Kategorien zusammen:

Abbildung 1: Kategorien von Informationsbedrohungen



Eigene Darstellung, angelehnt an: Wardle/Derakhshan (2017: 20).

Neben den unterschiedlichen Inhalten sind zwei zusätzliche Aspekte für die Verbreitung von Informationsbedrohungen relevant: Die Elemente und Phasen der Verbreitung. Eine Informationsbedrohung besteht immer aus einem Agenten oder einer Agentin, einer Nachricht und einem (gezielt ausgesuchten) Rezipienten oder einer Rezipientin.[121] Die Phasen ihrer Ver-

breitung lassen sich in Kreation, Produktion und Distribution der Nachricht einteilen. Kreation meint den Inhalt der Information, Produktion meint das Medium und die Darstellung der Information. Distribution bezeichnet die Verbreitungskanäle der Information. Mit der Verbreitung der Nachricht kann nun eine sich verstärkende Nachrichtenschleife von Reproduktion und Redistribution beginnen.

Bei der Verbreitung von Informationsbedrohungen lassen sich zwei Wirkungsebenen unterscheiden: die individuelle und die systemische. Während die individuelle Ebene direkt die Wirkung der Nachricht auf den Rezipierenden oder die Rezipierende meint und seine/ihre aus der Nachricht erfolgende Handlung (u. a. die Weiterverbreitung der Nachricht), meint die systemische Wirkungsebene die Rahmenbedingungen, in denen Informationsbedrohungen in Nachrichtenkanälen (re-)produziert und (re-)distribuiert werden. Diese Unterscheidung der Wirkungsebenen ist notwendig, um die Unterschiede von Maßnahmen gegen Informationsbedrohungen zu verstehen.

Politische Maßnahmen zur Begegnung

Die politische Begegnung erstreckt sich auf unterschiedliche Bereiche und beinhaltet u. a. Maßnahmen im Rahmen der strategischen Kommunikation, Ansätze der Plattformregulierung, Förderung der medienpolitischen Bildung und Medienkompetenz, Stärkung und Selbstverpflichtung von Medienunternehmen.[122]

Im internationalen Vergleich ist eine Reihe von Staaten wesentlich durch Plattformregulierung gegen Informationsbedrohungen vorgegangen. Gemäß einer Analyse von Nagasako[123] haben 31 der 53 analysierten Staaten neue Gesetze zur Plattformregulierung gegen Informationsbedrohungen erlassen. Gleichwohl ist hinzuzufügen, dass eine Reihe von Staaten die Gesetze zur Plattformregulierung mit dem alleinigen Fokus auf *Malinformation*en eingeführt haben. Auch das deutsche Netzwerkdurchsetzungsgesetz wirkt im Wesentlichen gegen *Malinformation*en. Elf Staaten haben im Rahmen von Wahlen Kampagnen zur Vermittlung von Medienwissen und Funktionsweise des Informationsraumes initiiert, acht Staaten haben eine nationale Task Force zur Begegnung von Informationsbedrohungen initiiert, acht eine Fact-Checking-Kampagne oder entsprechende Fact-Checking-Website gestartet.

Die Europäische Union setzt hier ebenfalls mit einem gemischten Ansatz an und fokussiert Plattformregulierungen, gezielte strategische Kommunikation durch den Europäischen Auswärtigen Dienst sowie bildungspolitische Maßnahmen. Die Europäische Kommission hat das politische Ziel, gemeinsame Standards zu entwickeln, um Desinformationen zu begegnen.[124] Die direkte Förderung von Medienkompetenz als Maßnahme gegen Informationsbedrohungen wird durch die EU im European Democracy Action Plan forciert.[125]

Diese politischen Ansätze unterscheiden sich dabei grundsätzlich. Regulierungsversuche von Onlineplattformen sowie Selbstverpflichtungen von Medienhäusern setzen in der Phase „Produktion" an. Sie wirken daher systemisch, also ob und wie Informationsbedrohungen auf Plattformen erstellt werden können. In Ergänzung dazu fokussieren Maßnahmen der medialen Bildung oder Fact-Checking-Tools die Stärkung des Rezipierenden und die Chance der Redistribution der jeweiligen Informationsbedrohung (vgl. Grafik 1). Sie wirken damit auf der individuellen Ebene der Rezipientin oder des Rezipienten.

Ein wesentlicher Unterschied ist, dass die systemischen Interventionen auf Plattformen immer aus Sicht der Rezipierenden reaktiv erfolgen können. Im Gegensatz dazu wirken Bildungsmaßnahmen präventiv. Sie fokussieren die Reflexionsfähigkeit und Analysekompetenzen der Rezipierenden und stellen somit einen grundsätzlichen Rahmen für den Umgang mit Informationsbedrohungen bereit.[126]

Zusammenfassend haben nur wenige Regierungen bzw. politische Akteure bisher explizit Bildungsmaßnahmen zur Stärkung von Medienkompetenz und gegen Informationsbedrohungen im Blick.

Medienkompetenz als Informationskompetenz priorisieren

Im Zentrum der bildungspolitischen Maßnahmen gegen Informationsbedrohungen steht die Stärkung von Medienkompetenz. Medienkompetenz ist ein sozialwissenschaftliches Konzept, das Erkenntnisse der Psychologie, Soziologie, Pädagogik und Kommunikationswissenschaft aufnimmt. Gemäß Huther/Schorb (2004) ist Medienkompetenz grundsätzlich eingebettet in soziale Interaktion und unterscheidet sich in Medienwissen, Medienbewertung und Medienhandeln.[127] Eine einheitliche Definition gibt es nicht.

Um dieser Diversität Rechnung zu tragen, sollte Medienkompetenz nicht als festes Konzept, sondern als Denkansatz verstanden werden, der vermittelt, wie Informationen verarbeitet und interpretiert werden.[128] An den Ansatz von Huguet et al. angelehnt, wird Medienkompetenz wie folgt definiert:[129] Medienkompetenz beinhaltet als Antwort auf Informationsbedrohungen die Fähigkeiten:

a. Informationen als Grundlage für Entscheidungen und Verhalten zu identifizieren;

b. Autorinnen und Autoren sowie Quellen kritisch auf Vertrauenswürdigkeit und Glaubwürdigkeit zu überprüfen;

c. den Erstellungsprozess des Medienprodukts nachvollziehen zu können und zu beurteilen;

d. Informationen aus unterschiedlichen Quellen zusammenzuführen und zu verarbeiten;

e. Medienprodukte mit einem Bewusstsein für die Konsequenzen der Verbreitung zu teilen.

Im Verständnis von Hüther/Schorb (2004) werden alle Kompetenzbereiche – Medienwissen (c), Medienbewertung (a,b) und Medienhandeln (d,e) – abgedeckt.[130] Drei dieser Fähigkeiten (a,b,d) sind dabei dem Verständnis der Informationskompetenz zuzuordnen.[131] Dieser Definition folgend wird Medienkompetenz mit einem Schwerpunkt auf Informationskompetenz verstanden, also als „intellectual framework for understanding, finding, evaluating, and using information"[132].

Eine Analyse von Mo Jones-Jang/Mortensen/Liu (2019) zeigt, dass Informationskompetenz aufgrund methodischer und konzeptioneller Gründe geeigneter ist, gegen Informationsbedrohungen zu wirken, als andere Bereiche von Medienkompetenz.[133] Weiterhin konnten Krahé/Busching (2015) zeigen, dass Informationskompetenz auch die Wahrscheinlichkeit für aggressive Kommunikation senkt.[134] Zusammenfassend bietet Medienkompetenz verstanden als Informationskompetenz wirkungsvolle Anknüpfungspunkte gegen Informationsbedrohungen.

Sozialpsychologische Erkenntnisse berücksichtigen

Informationsbedrohungen nutzen in ihrer Struktur die natürliche Trägheit des menschlichen Gehirns aus, wie z. B. das Versagen, systematisch kritisch zu denken und die Gewohnheit, auf Nachrichten zu vertrauen, ohne diese durch externe Quellen zu bestätigen.[135] Dieser „Confirmation Bias" bringt Menschen dazu, Informationen leichter zu akzeptieren, wenn diese bestehende Meinungen oder gelernte Sachverhalte bestätigen. Ergänzend dazu wirkt ein weiteres psychologisches Phänomen, welches die Korrektur von einmal gelernten Sachverhalten – und damit auch der gängigen Methode von Fact-Checking – erschwert. Dies wird mit dem „Continued Influence Effect" beschrieben. Dieser beschreibt den kognitiven Effekt, dass Narrative trotz der Aufdeckung ihres mangelnden Wahrheitsgehalts dennoch bei Personen haften bleiben können.[136] Diese Erkenntnis wird um die Forschung von Nyhan/Reifler (2010) ergänzt.[137] Sie beschreiben unter dem Begriff des „Backfire Effects", dass die Konfrontation mit korrigierten Informationen sehr starke negative Gefühle wecken kann, die trotz der Widerlegung einer falschen Nachricht zu einer Festigung der Auffassung führen. Dies tritt gerade in Korrelation mit dem Vorhandensein von politischen Einstellungen auf. Folglich tendieren Menschen dazu, Informationen zu konsumieren, die ihre bestehende Meinung nicht direkt herausfordert.[138] Dies wird als kognitive Dissonanz beschrieben. Inwieweit dies jedoch als verstärkender Effekt auf den Konsum politisch eingefärbter Nachrichten wirkt, wird kritisch diskutiert.[139]

Grundlegender argumentieren Kognitionswissenschaftlerinnen und -wissenschaftler, die in der menschlichen Informationsverarbeitung keine Suche nach Wahrheit sehen, sondern dies als evolutionären Bestandteil des menschlichen sozialen Wettstreits um eine Position in einer Gesellschaft betrachten. Neue Nachrichten bilden in dieser Logik einen Vorteil

für die Positionierung in einer Gruppe,[140] da sie einen grundsätzlichen Informationsvorsprung verschaffen. Informationsbedrohungen vermitteln häufig den Hinweis auf grundlegend neue Informationen, dies ist auch der Grund, warum sie sich schneller verbreiten als wahre, oftmals weniger spektakuläre Nachrichten.[141]

Diesen Erkenntnissen der Sozialpsychologie Rechnung tragend, sollte Medienkompetenz zusätzlich zu den oben genannten inhaltlichen Punkten grundlegende analytische Kompetenzen und kritisches Denken schulen. Einige Studien weisen darauf hin, dass falsche Informationen schneller von Personen aufgenommen werden, die geringeres analytisches Denken aufweisen.[142] Insofern scheint die Vermittlung von analytischen Fähigkeiten und kritischem Denken zentral für eine Informationskompetenz zu sein, die der Wirkungsweise von Informationsbedrohungen entgegenwirkt.[143] Hüther/Schorb (2004) bezeichnen dies als Medienbewertung.[144] Also sind analytische Fähigkeiten hier als Denkmethode und nicht als (Fach-)Wissen zu verstehen. Denn Studien[145] zeigten, dass Personen, die über Wissen zu einem Thema verfügen, weniger dazu geneigt waren, diese Informationen zu prüfen – dies wird auch als Dunning-Kruger-Effect beschrieben.

Ergänzend unterscheiden Kozyreva/Lewandowsky/Hertwig (2020) auf Grundlage einer ausführlichen Literaturrecherche geeignete Lernmethoden in Technocognition (Verständnis, wie soziale Medien sozio-psychologisches Wissen nutzen), Boosting (Wissensvermittlung zur direkten Informationssuche), Nudging (verhaltensökonomische Interventionen, die Verhalten ändern können) sowie Inoculation (direkte Wissensvermittlung zu Informationsbedrohungen).[146]

Als weiterer erfolgsversprechender Faktor von Programmen zur Vermittlung von Medienkompetenz wurde ein integrierter Ansatz von Medienkompetenz in andere Fächer angesehen bzw. in eine Situation, in der sich die Lernenden sicher fühlen.[147]

Zusammengefasst scheint die Vermittlung von Medienkompetenz im Sinne einer analytisch-kritischen Informationskompetenz ein vielversprechender Ansatz gegen Informationsbedrohungen zu sein. Durch eine Förderung von abstrahiert-kritischem Denken können sozialpsychologische Erkenntnisse über die Wirkung von Informationsbedrohungen in Bildungskonzepte aufgenommen werden.[148] Dieses Lehrkonzept sollte:

1. Kompetenzen zur Identifikation und Prüfung von Informationen,
2. die Bewertung und eigene Produktion von Medieninhalten sowie ein
3. Verständnis von Medien und ihren Konsequenzen vermitteln.

Finnland als Vorreiter?

Als Vorreiter in der Vermittlung von Medienkompetenz gegen Informationsbedrohungen wird Finnland genannt.[149] Die Grundlage des finnischen Erfolgs in der Vermittlung von Medienkompetenz bildet ein ganzheitlicher politischer Ansatz, der durch die Konfrontation mit Desinformationskampagnen weiterentwickelt wurde.

Bereits in den 1950er-Jahren fokussierte die finnische Bildungspolitik Medienkompetenz.[150] 2004 wurde dies als grundlegendes Bildungsziel im Verständnis einer Informationskompetenz[151] für die Gesamtbevölkerung ausgelobt.[152]

Finnland ist seit 2014 zunehmend Ziel von russischen Desinformationskampagnen.[153] 2015 wurde dies als Sicherheitsproblem[154] erkannt und äußert sich auch in der Bedrohungswahrnehmung der Mediennutzenden.[155] Infolge startete Finnland ein Schulungsprogramm für den öffentlichen Dienst[156] und baute bildungspolitische Maßnahmen aus. Finnland führte 2016 in seinem nationalen Curriculum die Maßnahme einer „multi-platform information literacy"[157] ein. Zielsetzung des Programms ist es, kritisches, selbstständiges Denken als festen Bestandteil in allen Fächern und entlang aller Bildungsarten (Kinder, Schul-, Berufs- und Erwachsenenbildung) zu etablieren.[158] Beispiele sind hier aus dem Mathematikunterricht (Veränderungsmöglichkeiten von Statistiken), Kunstunterricht (Veränderung von Bildaussagen), Geschichtsunterricht (Behandlung von Propaganda) oder Sprachunterricht (Möglichkeiten, wie Sprache Inhalte verändern kann) bekannt.[159] Besonders hervorzuheben ist hierbei, dass bereits im Kindergarten[160] angesetzt wird und sich das Vorgehen in die Lehrpläne der weiteren Bildungsbereiche, wie z. B. auch Berufsausbildung, sukzessive einfügt.[161]

Die Zielsetzung des finnischen Bildungssystems ist es, die Lernenden als verantwortliche Kommunikatoren auszubilden. Hierzu gehört die Vermittlung der Kompetenz von Medienkritik, ethischer Werte von Kommunikation und verantwortlicher Interaktion mit Medien.[162]

Weiterhin lässt das finnische Bildungssystem zu, dass die Lehrenden ihre Lehrmethode und die Einbindung von Medienkompetenz in ihren Unterricht frei wählen können.[163] Die Voraussetzung hierfür ist, dass die Ausbildungsstandards von Lehrenden durch die Vermittlung von grundlegendem Wissen und methodischem Verständnis von sozialen Medien ergänzt werden.

Neben der Integration von Informationskompetenz in nahezu alle schulischen Unterrichtsfächer unterstützt eine Reihe von außerschulischen Bildungsorganisationen die Arbeit rund um diesen Bereich. Finnland hat das europaweit größte Netzwerk dieser externen zivilgesellschaftlichen Anbieter zur Begegnung von Informationsbedrohungen.[164]

Finnlands Ansatz deckt sich mit den o. g. Handlungsempfehlungen sowohl hinsichtlich interdisziplinärer Informationskompetenz als auch analytischer Konzepte. Nicht nur wird, wie in der Definition von Huguet et al. (2019) die historische Entwicklung der Medienlandschaft und die Folgen einer ethischen Medienwirkung in den landesweiten Lehrplan aufgenommen, es wird auch die Expertenempfehlung[165] umgesetzt, sodass die Vermittlung von verantwortlicher Kommunikation in andere Fächer integriert wird. Zhang/Zhang/Wang (2020) heben in ihrer vergleichenden Analyse zu der Integration von Medienkompetenz in schulischen Lehrplänen diese Punkte als Besonderheit Finnlands heraus.[166]

Umfassendes Regierungshandeln Finnlands

Obwohl sich Überschneidungen zwischen der finnischen Bildungspolitik und den Empfehlungen zum Einsatz von Medienkompetenz gegen Informationsbedrohungen ergeben, ist die Stärkung von Resilienz gegen Informationsbedrohungen laut finnischem Bildungsministerium kein explizites Ziel. Es betont, Medienkompetenz und seine Vermittlung als breitangelegten Ansatz zu verstehen: Medienkompetenz ist mehr als ein Set von Fähigkeiten. Es ist eng mit persönlichem Wachstum, Kreativität, kritischem Denken und dem Ausdruck, Teil von Gesellschaft und Kultur sein zu können, verbunden.[167] Die Stärkung von Medienkompetenz fügt sich dennoch in einen einheitlichen Ansatz der Regierung. Das für die Bekämpfung von Informationsbedrohungen zuständige finnische Justizministerium verweist ausdrücklich auf die Bedeutung von Medienkompetenz im Kampf gegen Informationsbedrohungen.[168]

Gleichwohl Finnland im Media Literacy Index 2019 als das Land mit dem höchsten Wert in der Kategorie Medienkompetenz genannt wird,[169] bezweifelt das finnische Bildungsministerium die Aussagekraft dieser Analyse.[170] Es sei grundsätzlich problematisch, das Konzept Medienkompetenz aufgrund unterschiedlicher Definitionen in vergleichenden Studien zu messen. Grundsätzlich gesteht selbst das finnische Bildungsministerium ein, dass keine umfassenden Informationen über die Wirkungsweise der umfassenden Reformen zur Ausweitung von Medienkompetenz vorliegen.[171] Die letzten Untersuchungen stammen aus dem Jahr 2014, somit bleibt der „status of media literacy in Finland largely uninvestigated“[172].

Der finnische Ansatz von Medienkompetenz wirkt nicht für sich, sondern ist in ein funktionierendes Bildungssystem, eine breite Trägerschaft, außerschulische Bildungsorganisation sowie ein hohes gesellschaftliches Grundvertrauen in staatliche Institutionen eingebettet. Humprecht/Esser/Van Aelst (2020) untermauern den Ansatz, dass das politische

und gesellschaftliche Umfeld stark die Resilienz gegen Informationsbedrohungen erhöht. Finnland nimmt in ihrem Index den ersten Platz ein.[173] Somit scheint letztendlich die Konsequenz von Regierungshandeln über unterschiedlichste Bereiche hinweg in einem gemeinsamen Ansatz gegen Informationsbedrohungen zu helfen.[174]

Informationskompetenz als integraler Bestandteil kommunikativer Resilienz

Die vorliegende Analyse zeigt, dass Medienkompetenz – speziell verstanden als Informationskompetenz – einen Beitrag liefern könnte, der Wirkung von Informationsbedrohungen entgegenzuwirken,[175] da sie auf der individuellen Wirkungsebene von Informationsbedrohungen ansetzt. Die Vermittlung von Informationskompetenz als interdisziplinärer Ansatz, der verhaltensökonomische Erklärungsansätze gegen die Verbreitung von Informationsbedrohungen mit kognitiv-ansetzenden Bildungsprogrammen verzahnt, wird als wirkungsvoll beschrieben.[176]

Zur genauen Messung der Effektivität von Medienkompetenz gegen Informationsbedrohungen sollten die Forschungsansätze weiterentwickelt werden.[177] Es fehlt aufgrund der unterschiedlichen Rahmenbedingungen der Untersuchungen an einer Vergleichbarkeit der Forschungsergebnisse.[178] Hierbei sollten gesonderte Teilbereiche herausgehoben werden, anstatt allgemeine Konzepte zu vergleichen.[179] Weiterhin ist der Fokus der Maßnahmen umstritten: Sollte die Vermittlung von Informationskompetenz Hintergründe zur Entstehung von Informationsbedrohungen erklären oder helfen, die Falschnachricht als solche zu entlarven? Diese Komplexität des Themas erschwert nicht nur die Vermittlung, sondern auch die Ausbildung von Lehrenden zu diesem Themenkomplex.[180] Im Gegensatz zur Schulbildung scheint die Vermittlung von Informationskompetenz gegen Informationsbedrohungen in der Erwachsenenbildung ein unterentwickeltes Forschungsfeld zu sein. Für die Vermittlung sind hier andere Methoden notwendig.[181]

Weiterhin sind in der Forschung des Themenkomplexes zwei ethische Grundprinzipien nicht außer Acht zu lassen.[182] Zum einen das Recht jedes Menschen auf seine Meinung und seine Weltsicht. Das Vermeiden von der

Verbreitung falscher Informationen sollte keinesfalls dazu führen, dass die Meinungsvielfalt an sich unter den Maßnahmen leidet. Zum anderen sollten Bildungsmaßnahmen stets politisch neutral sein und sich auf die Transparenz des Informationsraumes richten.

Mit Blick auf die deutsche Bildungspolitik lässt sich konstatieren, dass das Unterrichtsthema Informationsbedrohungen im Sinne von „Fake News, Hate Speech und Social Bots“[183] und die Notwendigkeit einer „kritischen Medienkompetenz“[184] bereits in den Beschluss der Kultusministerkonferenz 2018 aufgenommen wurde. Gleichwohl fordern rund 85 Prozent der Jugendlichen in Deutschland, dass das Thema Informationsbedrohungen in den Lehrplan aufgenommen wird.[185] Das finnische Modell kann hier Anknüpfungspunkte für die fächerübergreifende Umsetzung dieses Ziels geben. Bereits heute wird Medienkompetenz als fächerübergreifend definiert.[186]

Nichtsdestotrotz ist die Förderung von Medienkompetenz kein Allheilmittel. Das finnische Beispiel verdeutlicht, dass Informationskompetenz als interdisziplinäres Feld nicht allein als Schulfach gedacht werden kann, sondern vielmehr als staatlich-initiiertes und gesellschaftlich getragenes Ökosystem zur Medienkompetenzvermittlung seine Wirkung entfaltet. Durch die Breite von staatlichen und nichtstaatlichen Akteuren hat der finnische Ansatz eine umfassende Wirkung in die Bevölkerung hinein.

95 Vgl. (Kuklinski, J. H./ Quirk, P. J./ Jerit, J./ Schwieder, D./ Rich, R. F., 2000).

96 Siehe (Larson, E./ Darilek, R./ Gibran, D./ Nichiprouk, B./ Richardson, A./ Schwartz, L./ Thurston, C., 2009, S. 3).

97 Siehe (Europäische Kommission, 2020a, S. 4).

98 Siehe (NATO, 2019, S. 29).

99 Siehe (Bradshaw, S./ Howard, P., 2019, S. 5).

100 Vgl. (Europäische Kommission, 2020b), (European External Action Service, 2020).

101 Vgl. (Rid, T., 2020).

102 Siehe (Wardle, C./ Derakhshan, H., 2017, S. 15 ff.)

103 Vgl. (Wilke, T, 2020).

104 Siehe (Vilmer, J./Escorcia, A./ Guillaume, M./ Herrera, J., 2018, S. 177), vgl. (Mihailidis, P./ Viotty, S., 2017).

105 Siehe (Nagasako, T., 2020, S. 133).

106 Vgl. (Charlton, E., 2019), Siehe (Vilmer, J./Escorcia, A./ Guillaume, M./ Herrera, J., 2018, S. 168).

107 Siehe (Mazarr, M./ Bauer, R./ Casey, A./ Heintz, S./ Matthews, L., 2019, S. 27 ff.).

108 Siehe (Mazarr, M./ Bauer, R./ Casey, A./ Heintz, S./ Matthews, L., 2019, S. 13).

109 Vgl. (Barberá, P./ Jost, J. T./Nagler, J./ Tucker, J./ Bonneau, R., 2015).

110 Siehe (Lewandowsky, S./ Ecker, U. K./Cook, J., 2017, S. 23).

111 Vgl. Ebd.

112 Siehe (Newmann, N./ Fletcher, R./ Schulz, A./ Andi, S./ Nielsen, R., 2020, S. 20).

113 Vgl. Ebd.

114 Vgl. (Kavanagh, J./ Rich, M., 2018).

115 Siehe (Wardle, C./ Derakhshan, H., 2017, S. 20).

116 Siehe (Helmus, T. C., 2020, S. 153).

117 Siehe (Bay, S./ Dek, A./ Dek.,I./ Fredheim, R, 2020, S. 20).

118 Vgl. (Southwell, B./ Thorson, E./ Sheble, L., 2017).

119 Siehe (Colley, T./ Granelli, F./ Althuis, J., 2020, S. 96 ff.).

120 Siehe (Vilmer, J./Escorcia, A./ Guillaume, M./ Herrera, J., 2018, S. 40), Vgl. (Kavanagh, J./ Rich, M., 2018), siehe (Lewandowsky, S./ Ecker, U. K./Cook, J., 2017, S. 23 ff.).

121 Vgl. (Wardle, C./ Derakhshan, H., 2017, S. 20).

122 Vgl. (Wardle, C./ Derakhshan, H., 2017), (Wilke, T, 2020), (Tworek, H., 2018), (Europäische Kommission, 2018), (Europäische Kommission, 2020c).

123 Siehe (Nagasako, T., 2020, S. 133).

124 Siehe (Europäische Kommission, 2019, S. 21).

125 Siehe (Europäische Kommission, 2020c).

126 Vgl. (Jeong, S./ Cho, H./ Huang, Y., 2012), (Kozyreva, A./ Lewandowsky, S./ Hertwig, R., 2020).

127 Siehe (Hüther, J./ Schorb, B., 2004, S. 257 ff.).

128 Siehe (Huguet, A./ Kavanagh, J./ Baker, G./ Blumenthal, M., 2019, S. 41).

129 Siehe Ebd, S. 5 – 6.

130 Siehe (Hüther, J./ Schorb, B., 2004, S. 257 ff.).

131 Siehe (Mo Jones-Jang, S./ Mortensen, T./ Liu, J., 2019, S. 5).

132 Siehe Ebd.

133 Vgl. Ebd.

134 Vgl. (Krahé, B./ Busching, R., 2015).

135 Vgl. (Vilmer, J./Escorcia, A./ Guillaume, M./ Herrera, J., 2018, S. 31), vgl. (Henkel, L. A./ Mattson, M. E., 2011).

136 Vgl. (Lewandowsky, S./ Ecker, U./ Seifert, C./ Schwarz, N./ Cook, J., 2012).

137 Vgl. (Nyhan, B./ Reifler, J., 2010).

138 Vgl. (Donsbach, W., 1991).

139 Vgl. (Metzger, M./ Hartsell, E./ Flanagin, A., 2020).

140 Vgl. (Ng, Y.-L., 2020).

141 Vgl. (Vosoughi, S./ Roy, D./ Aral, S., 2018).

142 Vgl. (Bronstein, M./ Pennycook, G./ Bear, A./ Rand, D./ Cannon, T., 2019), vgl. (Pennycook, G./Rand, D., 2019).

143 Vgl. (McDougall, J./ Zezulkova, M./ van Driel, B./ Sternadel, D., 2018).

144 Vgl. (Hüther, J./ Schorb, B., 2004, S. 257 ff.).

145 Vgl. (Radecki, C. M./Jaccard, J., 1995), (Mahmood, K., 2016).

146 Vgl. (Kozyreva, A./ Lewandowsky, S./ Hertwig, R., 2020, S. 128 ff.).

147 S. (Huguet, A./ Kavanagh, J./ Baker, G./ Blumenthal, M., 2019, S. 22 ff.), vgl. (Walton, G./ Hepworth, M., 2011).

148 Vgl. (Kozyreva, A./ Lewandowsky, S./ Hertwig, R., 2020).

149 Vgl. (Charlton, E., 2019), Siehe (Vilmer, J./Escorcia, A./ Guillaume, M./ Herrera, J., 2018, S. 168).

150 Siehe (Salomaa, S./ Palsa, L., 2019, S. 21).

151 Vgl. (Palsa, L./ Ruokamo, H., 2015).

152 Vgl. (Kupianinen, R., 2019).

153 Vgl. (Nimmo, B., 2017).

154 Vgl. (Szymanski, 2018).

155 Siehe (Newmann, N./ Fletcher, R./ Schulz, A./ Andi, S./ Nielsen, R., 2020, S. 18).

156 Vgl. (Yle.fn, 2016).

157 Siehe (Henley, J., 2020).

158 Siehe (Salomaa, S./ Palsa, L., 2019, S. 34).

159 Vgl. (Henley, J., 2020).

160 Siehe (Mackintosh, E., 2019).

161 Vgl. (Salomaa, S./ Palsa, L., 2019, S. 34 ff.).

162 Vgl. (Zhang, L./ Zhang, L./ Wang, K., 2020).

163 Vgl. (Salomaa, S./ Palsa, L., 2019, S. 34 ff.).

164 Siehe (European Audiovisual Observatory, 2016, S. 38,171).

165 Siehe (Huguet, A./ Kavanagh, J./ Baker, G./ Blumenthal, M., 2019, S. 22–25).

166 Vgl. (Zhang, L./ Zhang, L./ Wang, K., 2020).

167 Siehe (Salomaa, S./ Palsa, L., 2019, S. 5).

168 Siehe Ebd, S. 50.

169 Vgl. (Lessenski, M., 2019).

170 Siehe (Salomaa, S./ Palsa, L., 2019, S. 31).

171 Vgl. Ebd.

172 Siehe Ebd.

173 Siehe (Humprecht, E./ Esser, F./ Van Aelst, P., 2020, S. 505).

174 Vgl. (Standish, R., 2017).

175 Vgl. (Jeong, S./ Cho, H./ Huang, Y., 2012).

176 Vgl. (Lewandowsky, S./ Ecker, U. K./Cook, J., 2017, S. 32), (Kozyreva, A./ Lewandowsky, S./ Hertwig, R., 2020).

177 Siehe (Colley, T./ Granelli, F./ Althuis, J., 2020, S. 100 ff.).

178 Siehe (Bulger, M./ Davidson, P., 2018, S. 1).

179 Siehe (Salomaa, S./ Palsa, L., 2019, S. 32).

180 Vgl. (Schmeichel, M./ Garret, J./ Ranschaert, R./ Thomson, J./ Janis, S./ Clark, C./ Yagata, S./ Bivens, B., 2018).

181 Vgl. (McDougall, J./ Zezulkova, M./ van Driel, B./ Sternadel, D., 2018), siehe (Bulger, M./ Davidson, P., 2018, S. 4).

182 Siehe (Lewandowsky, S./ Ecker, U. K./Cook, J., 2017, S. 37).
183 Siehe (Kultusministerkonferenz (KMK), 2018, S. 3).
184 Siehe ebd.
185 Vgl. (Vodafone Stiftung Deutschland, 2020).
186 Vgl. (Kultusministerkonferenz (KMK), 2012).

Literaturverzeichnis

B Barberá, P./ Jost, J. T./Nagler, J./ Tucker, J./ Bonneau, R. (2015). Tweeting from left to right: Is online political communication more than an echo chamber? In: Psychological Science, Vol. 26, Iss. 10, S. 1531–1542.

Bay, S./ Dek, A./ Dek.,I./ Fredheim, R. (2020). Falling Behind: Social Media Manipulation 2020. How Social Media companies are failing to combat inauthentic behaviour online. NATO Strategic Communication Centre of Excellence. https://www.stratcomcoe.org/how-social-media-companies-are-failing-combat-inauthentic-behaviour-online (letzter Zugriff: 05.01.2021).

Bradshaw, S./ Howard, P. (2019). The Global Desinformation Order. 2019 Global Inventory of organized Social Media Manipulation. https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2019/09/CyberTroop-Report19.pdf (letzter Zugriff: 05.01.2021).

Bronstein, M./ Pennycook, G./ Bear, A./ Rand, D./ Cannon, T. (2019). Belief in Fake News is Associated with Delusionality,Dogmatism, Religious Fundamentalism and Reduced Analytic Thinking. In: Journal of Applied Research in Memory and Cognition, Vol. 8, Iss. 1, S. 108–117.

Bulger, M./ Davidson, P. (2018). The Promises, Challenges and Futures of Media Literacy. In: Journal of Media Literacy Education, Vol. 10, Iss. 1, S. 1–21.

C Charlton, E. (2019). How Finland is fighting fake news – in the classroom. https://www.weforum.org/agenda/2019/05/how-finland-is-fighting-fake-news-in-the-classroom/ (letzter Zugriff: 05.01.2021).

Colley, T./ Granelli, F./ Althuis, J. (2020). Disinformation's societal impact. Britain, Covid, and beyond. In: Defence Strategic Communications, Vol. 8. https://www.stratcomcoe.org/tcolley-fgranelli-and-jalthuis-disinformations-societal-impact-britain-covid-and-beyond (letzter Zugriff: 05.01.2021).

D Donsbach, W. (1991). Exposure to Political Content in Newspapers: The Impact of Cognitive Dissonance on Readers' Selectivity. In: European Journal of Communication, Vol. 6, Iss. 2, S. 155–186.

E Europäische Kommission (2018). A multi-dimensional approach to disinformation. Report of the independent High Level Group on fake news and online disinformation. https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=50271 (letzter Zugriff: 05.01.2021).

Europäische Kommission (2019). Political Guidelines for the next European Commission 2019–2024. https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission_en.pdf (letzter Zugriff: 05.01.2021).

Europäische Kommission (2020a). Communication from the Commission to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Region on the EU Security Union Strategy, No. 605 final. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0605 (letzter Zugriff: 05.01.2021).

Europäische Kommission (2020b). Joint Communication to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, Tackling COVID-19 disinformation – getting the facts right, JOIN (2020) 8. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020JC0008 (letzter Zugriff: 05.01.2021).

European External Action Service (2020). EEAS Special Report Update: Short Assessment of Narratives and Disinformation around the Covid-19 Pandemic. https://euvsdisinfo.eu/eeas-special-report-update-short-assessment-of-narratives-and-disinformation-around-the-covid19-pandemic-updated-23-april-18-may/, (letzter Zugriff: 05.01.2021).

H Helmus, T. C. (2020). Social Media and Influence Operations Technologies Implications for Great Power Competition. In T. F. Lynch, Strategic Assessment 2020. Into a New Era of Great Power Competition (S. 153–168.). Washington DC: Institute for National Strategic Studies, National Defense University.

Henkel, L. A./ Mattson, M. E. (2011). Reading is believing: The truth effect and source credibility. In: Consciousness and Cognition: An International Journal, Vol. 20, Iss. 4, S. 1705–1721.

Henley, J. (2020). How Finland starts its fight against fake news in primary schools. https://www.theguardian.com/world/2020/jan/28/fact-from-fiction-finlands-new-lessons-in-combating-fake-news (letzter Zugriff: 05.01.2021).

Huguet, A./ Kavanagh, J./ Baker, G./ Blumenthal, M. (2019). Exploring Media Literacy education as a tool for mitigating truth decay. https://www.rand.org/pubs/research_reports/RR3050.html (letzter Zugriff: 05.01.2021).

Humprecht, E./ Esser, F./ Van Aelst, P. (2020). Resilience to Online Disinformation. A Framework for Cross-National Comparative Research. In: The International Journal of Press/Politics, Vol. 25, Iss. 3, S. 493–516.

Hüther, J./ Schorb, B. (2004). Grundbegriffe Medienpädagogik. München: kopead.

J Jeong, S./ Cho, H./ Huang, Y. (2012). Media literacy interventions. A Meta-Analytic Review. In: Journal of Communication, Vol. 62, Iss. 3, S. 454–472.

K Kavanagh, J./ Rich, M. (2018). Truth Decay. An Initial Exploration of the Diminishing Role of Facts and Analysis in American Public Life. file:///C:/Users/JWAHML~1/AppData/Local/Temp/RAND_RR2314.pdf (letzter Zugriff: 05.01.2021).

Kozyreva, A./ Lewandowsky, S./ Hertwig, R. (2020). Citizens versus the Internet. Confronting Digital Challenges with cognitive tools. In: Psychological Science in the Public Interest, Vol. 21, Iss. 3, S. 103–156.

Krahé, B./ Busching, R. (2015). Breaking the vicious cycle of media violence use and aggression: A test of intervention effects over 30 months. In: Psychology of Violence, Vol. 5, Iss. 2, S. 217–226.

Kultusministerkonferenz (KMK). (2012). Medienbildung in der Schule, Beschluss der Kultusministerkonferenz vom 8. März 2012. https://www.kmk.org/fileadmin/Dateien/veroeffentlichungen_beschluesse/2012/2012_03_08_Medienbildung.pdf (letzter Zugriff: 05.01.2021).

Kultusministerkonferenz (KMK). (2018). Demokratie als Ziel, Gegenstand und Praxis historisch-politischer Bildung und Erziehung in der Schule, Beschluss der Kultusministerkonferenz vom 06.03.2009 i. d. F. vom 11.10.2018. https://www.kmk.org/fileadmin/Dateien/veroeffentlichungen_beschluesse/2009/2009_03_06-Staerkung_Demokratieerziehung.pdf (letzter Zugriff: 05.01.2021).

Kupianinen, R. (2019). Media Literacy in Finland. In: R. M. Hobbs. International Encyclopedia of Media Literacy (Vol. 2, S. 918–924). Hoboken: Wiley Blackwell.

L Larson, E./ Darilek, R./ Gibran, D./ Nichiprouk, B./ Richardson, A./ Schwartz, L./ Thurston, C. (2009). Foundation of effective Influence Operations. A Framework for Enhancing Army Capabilities. https://www.rand.org/content/dam/rand/pubs/monographs/2009/RAND_MG654.pdf (letzter Zugriff: 05.01.2021).

Lessenski, M. (2019). Just think about it. Findings of the media literacy index 2019. In: Policy Brief No. 55, Open Society Institute Sofia. https://osis.bg/wp-content/uploads/2019/11/MediaLiteracyIndex2019_-ENG.pdf (letzter Zugriff: 05.01.2021).

Lewandowsky, S./ Ecker, U. K./Cook, J. (2017). Beyond Misinformation. Understanding and Coping with the „Post-Truth" Era. In: Journal of Applied Research in Memory and Cognition, Vol. 6, Iss. 4, S. 353–369.

Lewandowsky, S./ Ecker, U./ Seifert, C./ Schwarz, N./ Cook, J. (2012). Misinformation and its correction. Continued Influence und successful debiasing. In: Psychological Science in the Public Interest, Vol. 13, Iss. 3, S. 106–131.

M Mackintosh, E. (2019). Finland is winning the war on fake news. What it's learned may be crucial to Western democracy, CNN Special Report, 2019. https://edition.cnn.com/interactive/2019/05/europe/finland-fake-news-intl/ (letzter Zugriff: 05.01.2021).

Mazarr, M./ Bauer, R./ Casey, A./ Heintz, S./ Matthews, L. (2019). The Emerging Risk of Virtual Societal Warfare. Social Manipulation in a Changing Information Environment. https://www.rand.org/pubs/research_reports/RR2714.html (letzter Zugriff: 05.01.2021).

McDougall, J./ Zezulkova, M./ van Driel, B./ Sternadel, D. (2018). Teaching media literacy in Europe: evidence of effective school practices in primary and secondary education, NESET II report. https://nesetweb.eu/wp-content/uploads/2019/06/AR2_Full_Report_With_identifiers_Teaching-Media-Literacy.pdf (letzter Zugriff: 05.01.2021).

Metzger, M./ Hartsell, E./ Flanagin, A. (2020). Cognitive Dissonance or Credibility? A Comparison of Two Theoretical Explanations for Selective Exposure to Partisan News. In: Communication Research, Vol. 47, Iss. 1, S. 3–28.

Mihailidis, P./ Viotty, S. (2017). Spreadable spectacle in digital culture. Civic expression, fake news, and the role of media literacies in „post-fact" society. In: American Behavioral Scientist, Vol. 61, Iss. 4, S. 441–454.

Mo Jones-Jang, S./ Mortensen, T./ Liu, J. (2019). Does Media Literacy help Identification of Fake News? Information Literacy helps, but other literacies don't. In: American Behaviour Scientist, Vol. 65, Iss. 2, S. 371–388.

N Nagasako, T. (2020). Global disinformation campaigns and legal challenges. In: International Cybersecurity Law Review, Vol. 1, S. 125–136.

NATO. (13.12.2019). The Secretary General's Report 2019. https://www.nato.int/nato_static_fl2014/assets/pdf/2020/3/pdf_publications/sgar19-en.pdf (letzter Zugriff: 05.01.2021).

Newmann, N./ Fletcher, R./ Schulz, A./ Andi, S./ Nielsen, R. (2020). Reuters Institute Digital News Report 2020. https://reutersinstitute.politics.ox.ac.uk/sites/default/files/2020-06/DNR_2020_FINAL.pdf (letzter Zugriff: 05.01.2021).

Ng, Y.-L. (2020). Toward an evolutionary perspective on social media use for cooperation. In: Evolutionary Behavioral Sciences, Vol. 14, Iss. 2, S. 132–146.

Nimmo, B. (2017). Failures and adaptations. Kremlin propaganda in Finland and Sweden. The Foreign Policy Centre, 21.3.2017: https://fpc.org.uk/failures-adaptations-kremlin-propaganda-finland-sweden/ (letzter Zugriff: 05.01.2021).

Nyhan, B./ Reifler, J. (2010). When Corrections Fail: The Persistence of Political Misperceptions. In: Political Behavior, Vol. 32, S. 303–330.

P Palsa, L./ Ruokamo, H. (2015). Behind the concepts of multiliteracies and media literacy in the renewed Finnish core curriculum: A systematic literature review of peer-reviewed research. In: Seminar.net, Vol. 11, Iss. 2, S. 101–119.

Pennycook, G./Rand, D. (2019). Lazy, not biased: Susceptibility to partisan fake news is better explained by lack of reasoning than by motivated reasoning. In: The Cognitive Science of Political Thought, Vol. 188, S. 39–50.

R Rid, T. (2020). Active Measures. The Secret History of Disinformation and political warfare. London: Profile Books Ltd.

S Salomaa, S./ Palsa, L. (2019). Media literacy in Finland. National media education policy. Ministry of Education and Culture, Helsinki: https://medialukutaitosuomessa.fi/mediaeducationpolicy.pdf (letzter Zugriff: 05.01.2021).

Schmeichel, M./ Garret, J./ Ranschaert, R./ Thomson, J./ Janis, S./ Clark, C./ Yagata, S./ Bivens, B. (2018). The Complexity of Learning to Teach News Media in Social Studies Education. In: Journal of Media Literacy Education, Vol. 10, Iss. 2, S. 86–103.

Southwell, B./ Thorson, E./ Sheble, L. (2017). The Persistence and Peril of Misinformation. In: The America Scientist, Vol. 105, Iss. 6, S. 372–375.

Standish, R. (2017). Why Is Finland Able to Fend Off Putin's Information War? https://foreignpolicy.com/2017/03/01/why-is-finland-able-to-fend-off-putins-information-war/ (letzter Zugriff: 05.01.2021).

Szymanski, P. (2018). Finland: the fight against disinformation, Centre for Eastern Studies, Analysis, 2018. https://www.osw.waw.pl/en/publikacje/analyses/2018-10-24/finland-fight-against-disinformation (letzter Zugriff: 05.01.2021).

T Tworek, H. (2018). Responsible Reporting in an Age of Irresponsible Information, Brief No. 009. https://securingdemocracy.gmfus.org/wp-content/uploads/2018/06/Responsible-Reporting_ASD_2_Final.pdf (letzter Zugriff: 05.01.2021).

V Vilmer, J./Escorcia, A./ Guillaume, M./ Herrera, J. (2018). Information Manipulation: A Challenge for Our Democracies, report by the Policy Planning Staff (CAPS) of the Ministry for Europe and Foreign Affairs and the Institute for Strategic Research (IRSEM) of the Ministry for the Armed Forces. https://www.diplomatie.gouv.fr/IMG/pdf/information_manipulation_rvb_cle838736.pdf (letzter Zugriff: 05.01.2021).

Vodafone Stiftung Deutschland. (2020). Die Jugend in der Infodemie, Eine repräsentative Befragung zum Umgang junger Menschen in Deutschland mit Falschnachrichten während der Coronakrise. https://www.vodafone-stiftung.de/wp-content/uploads/2020/12/Studie-Vodafone-Stiftung-Umgang-mit-Falschnachrichten.pdf (letzter Zugriff: 05.01.2021).

Vosoughi, S./ Roy, D./ Aral, S. (2018). The Spread of true and false news online. In: Science, Vol. 359, S. 1146–1151.

W Walton, G./ Hepworth, M. (2011). A longitudinal study of changes in learners' cognitive states during and following an information literacy teaching intervention. In: Journal of Documentation, Vol. 67, Iss. 3, S. 449–479.

Wardle, C./ Derakhshan, H. (2017). Information Disorder. Toward an interdiscplinary framework for research and policy making. In: Council of Europe report, DGI (2017) 09. https://rm.coe.int/information-disorder-toward-an-interdisciplinary-framework-for-research/168076277c (letzter Zugriff: 05.01.2021).

Wilke, T. (2020). Informationsbedrohungen. Herausforderungen für den europäischen Informationsraum. https://www.hss.de/download/publications/AA_77_Infobedrohung_Deutsch.pdf (letzter Zugriff: 05.01.2021).

Y Yle. fn. (2016). US experts gird Finnish officials for information war. https://yle.fi/uutiset/osasto/news/us_experts_gird_finnish_officials_for_information_war/8616336 (letzter Zugriff: 05.01.2021).

Z Zhang, L./ Zhang, L./ Wang, K. (2020). Media Literacy Education and Curriculum Integration. A Literature Review. In: International Journal of Contemporary Education, Vol. 3, Iss. 1, S. 55–64.

Prebunking als Möglichkeit zur Resilienzsteigerung

gegenüber Falsch-informationen in Onlinemedien

Ulrich Schade, Florian Meißner,
Albert Pritzkau und Sonja Verschitz

06

Die Resilienzsteigerung der Bevölkerung gegenüber Falschinformationen in Onlinemedien, also auf Webseiten und in den sozialen Medien, ist ein wesentliches Ziel, wenn es um Erhalt und Stärkung unserer demokratischen Grundordnung geht. Als Ergänzung zu Faktenchecks und zu den Maßnahmen, die auf eine generelle Verbesserung der Informations- und Medienkompetenz abzielen, schlagen wir *Prebunking*, also Warnungen, die Leser und Leserinnen vor dem Konsumieren von Beiträgen auf mögliche Probleme aufmerksam machen, vor. Dazu werden zwei Ansätze vorgestellt, die manuelle Bewertung der Glaubwürdigkeit von Quellen durch NewsGuard und die automatisierte Inhaltsbewertung durch Fraunhofer FKIE.

Einleitung

Die Resilienzsteigerung der Bevölkerung gegenüber Falschinformationen in Onlinemedien, also auf Webseiten und in den sozialen Medien, ist ein wesentliches Ziel, wenn es um Erhalt und Stärkung unserer demokratischen Grundordnung geht. Zwei Ansätze werden häufig diskutiert, um eine solche Steigerung zu erreichen. Dies ist zum einen die generelle Verbesserung der Informations- und Medienkompetenz und zum anderen der Einsatz von Faktenchecks zur Entdeckung von Fake News, auch *Debunking* genannt. Wir wollen uns in diesem Beitrag auf ergänzende Ansätze konzentrieren, mittels derer Leser und Leserinnen von Beiträgen, z. B. solchen in den sozialen Medien, schon vorab darauf aufmerksam gemacht werden, dass ein vorliegender Beitrag möglicherweise Fake News oder manipulative Inhalte enthalten könnte. Ansätze dieser Art werden als *Prebunking* bezeichnet.

Wir werden im Folgenden kurz auf Debunking-Ansätze eingehen und auf die damit verbundenen Probleme hinweisen. Anschließend werden wir zwei Ansätze des *Prebunkings* genauer vorstellen, zunächst die manuelle Bewertung und Markierung der Quelle und dann die automatisierte Bewertung inhaltlicher Faktoren. Im letzteren Fall gehen wir auch auf die Rolle der Emotion ein, wie sie im Beitrag sprachlich kodiert ist, und darauf, wie dies dabei hilft, mögliche problematische Beiträge zu erkennen. Die erläuterten Ansätze entfalten ihre besondere Wirksamkeit dann, wenn sie zusammen und aufeinander abgestimmt genutzt werden. Dies werden wir im abschließenden Abschnitt unseres Beitrags erläutern.

Ulrich Schade, Florian Meißner,
Albert Pritzkau und Sonja Verschitz

Problemstellung: Fake News und Gegenmaßnahmen

Lazer et al. definieren Fake News als „fabricated information that mimics news media content in form but not in organizational process or intent" (2018: 1094). Als zentrale Verbreitungsplattform gelten Social Media (Del Vicario et al. 2016). Der Begriff Fake News ist allerdings umstritten, weil er gerade in den USA häufig politisch instrumentalisiert wird. Alternativ werden die Begriffe *Misinformation* (Falschinformation) und *Disinformation* (Desinformation) verwendet. Dabei wird unterschieden, ob eine falsche Information in dem Glauben verbreitet wird, sie sei wahr, oder ob sie intentional in Umlauf gebracht wird, wobei diese Unterscheidung in der Praxis oft schwierig ist (Wardle/Derakshan 2018).

Seit dem Brexit-Referendum und der US-Präsidentschaftswahl 2016 wird das Thema politisch und gesellschaftlich intensiv diskutiert. In der Folge dieser beiden Voten, die von Debatten rund um den Einfluss gezielter Falsch- und Desinformation geprägt waren, entstanden zahlreiche neue Faktencheckinitiativen (Mantzarlis 2018: 87). Mit Blick auf dieses Ringen um Faktizität in der politischen und medialen Arena sprechen manche von einer Post Truth-Ära (Lewandowsky et al. 2017), in der politische Glaubenssätze oft wichtiger erscheinen als Fakten (Van Bavel/Pereira 2018). Darüber hinaus haben Studien gezeigt, dass sich Lügen in sozialen Netzwerken zuweilen schneller verbreiten als Fakten (Kümpel 2018, Vosoughi et al. 2018). Weniger klar ist hingegen der Einfluss, den Falschinformationen tatsächlich ausüben. So haben einschlägige Webseiten häufig relativ geringe Reichweiten. Zugleich zeigt sich, dass der Content dieser Seiten in sozialen Netzwerken häufig ähnlich viele oder sogar mehr Interaktionen (Likes, Shares, Kommentare) auslöst als Nachrichteninhalte etablierter Medienmarken (Fletcher et al. 2018). Völ-

lig im Unklaren bleibt derweil, wie viele Menschen insgesamt mit Falschinformationen in sozialen Netzwerken konfrontiert sind. Zudem sind geschlossene Gruppen und Messengerdienste für die Wissenschaft weiterhin Black Boxes.

Unstrittig ist, dass sich Krisen immer wieder als Nährboden für Falschinformationen und Verschwörungsmythen erweisen. Dies gilt in besonderer Weise für die Corona-Pandemie (Meißner 2020). Mit Blick auf die zahlreichen medizinischen Falschinformationen sowie Verschwörungsmythen in diesem Zusammenhang sprach die Weltgesundheitsorganisation (WHO 2020) in der Frühphase von einer „Infodemie". Gestützt wird diese Beobachtung etwa von Brennen et al. (2020), deren Untersuchungen zufolge die Zahl der englischsprachigen Faktenchecks zum Coronavirus zwischen Mitte Januar und Ende März 2020 um 900 Prozent zunahm – dennoch blieben viele Social-Media-Posts mit widerlegten Falschinformationen über längere Zeit online.

Ein grundlegendes Problem von Fake News ist, dass unsere kognitiven Verarbeitungsprozesse sie oftmals begünstigen. Ein wichtiger Aspekt ist, dass Nutzerinnen und Nutzer die Qualität von Informationen weniger kritisch betrachten, wenn sie diese nur peripher verarbeiten (Cook/Lewandowsky 2011). Mantzarlis (2018) führt darüber hinaus weitere Aspekte auf: Confirmation Bias (man nimmt v. a. wahr, was die eigene Position zu bestätigen scheint), Motivated Reasoning (Information wird vor allem dann als korrekt eingeschätzt, wenn sie eigenen Positionen entspricht) und Availability Heuristic (Tendenz, diejenigen Informationen als wahr zu erachten, die leicht erinnerlich sind). Den daraus resultierenden Verzerrungen zu begegnen ist nicht trivial. Gerade, wenn dies erst im Nachhinein geschieht, also wenn Falschinformationen bereits rezipiert wurden. Schließlich sind einmal verinnerlichte Informationen nur sehr schwer zu korrigieren („Continued Influence Effect" nach Johnson/Seifert 1994). Natürlich ist es wichtig, dass insbesondere virale Falschinformationen oder populäre Missverständnisse richtiggestellt werden (Debunking), damit Nutzerinnen und Nutzer die Möglichkeit haben, sich korrekt zu informieren. Dies gilt insbesondere bei umstrittenen Fragen oder bei solchen, bei denen ein Zweifel am Wahrheitsgehalt besteht, wie etwa im Zuge der Corona-Pandemie.

Die Bedeutung von professionellen und unabhängigen Faktenchecks steht also außer Frage; sie sind aber nicht die (alleinige) Lösung des Problems. Zum einen wirken die oben angeführten Prozesse, die die Verbreitung von Falschinformationen begünstigen der Wirkung von Faktenchecks entgegen, da diese naturgemäß nachträglich veröffentlicht werden, also erst dann, wenn die Falschinformation sich bereits verbreiten konnte. Zum anderen erreichen Faktenchecks häufig weniger bzw. andere Personen als die ursprüngliche Falschinformation (Sängerlaub/Meier/Rühl 2018). Zum Dritten kann es in manchen Fällen sogar zu einem „Backfire Effect" kommen (Nyhan/Reifler 2010), indem ein Faktencheck als untauglicher Versuch interpretiert wird, unliebsame Wahrheiten zu diskreditieren. In diesem Fall kann ein Faktencheck sogar zu einer Verstärkung des Glaubens an die Falschinformation bzw. an den Verschwörungsmythos führen.

Vor dem Hintergrund der oben beschriebenen Einschränkungen hinsichtlich der Wirksamkeit von Faktenchecks bedarf es gerade in Onlineumfeldern weiterer Ansätze zur Steigerung der Resilienz gegen Falsch- und Desinformation. Ein solcher Ansatz ist das sogenannte *Prebunking*, das darauf setzt, Nutzerinnen und Nutzer bereits *vor* dem Konsum von Nachrichteninhalten auf die (fehlende) Glaubwürdigkeit eines Informationsanbieters hinzuweisen. Ist ein Hinweis vorgeschaltet, dass bei einer Quelle Vorsicht geboten ist, dann besteht eine reelle Chance, dass die (intendierte) Falschnachricht ihre Wirkung verfehlt. In den nachfolgenden Abschnitten werden zwei *Prebunking*-Ansätze vorgestellt.

Lösungsansatz 1: Prebunking durch NewsGuard

NewsGuard[187] ist ein 2018 in den USA gelaunchtes Medien-Start-up. Gegründet wurde es von den Journalisten und Medienunternehmern Steven Brill und Gordon Crovitz. Sie entwickelten ein System zur Bewertung der Glaubwürdigkeit und Transparenz von Nachrichten- und Informationswebseiten, basierend auf neun gewichteten, journalistischen Standards (Tab. 1). Diese Kriterien sind im Journalismus als klassische Gütekriterien anerkannt. Ihre Anwendung wird transparent und neutral gehandhabt; die Bewertungen werden zudem regelmäßig aktualisiert.

Tabelle 1: Die NewsGuard-Kriterien

Glaubwürdigkeit

Kriterium	Erläuterung	Gewichtung (Punkte)
Es werden nicht regelmäßig Falschinformationen veröffentlicht.	In den vergangenen drei Jahren hat die Webseite nicht wiederholt Beiträge veröffentlicht, die NewsGuard-Analysten oder andere Faktenchecker widerlegt haben und die nicht rasch und deutlich richtig gestellt wurden.	22

Kriterium	Erläuterung	Gewichtung (Punkte)
Verantwortungsbewusste Recherche und Aufbereitung von Informationen.	Journalistinnen und Journalisten bemühen sich um akkurate, unabhängige und ausgewogene Recherchen, die auf einer Vielzahl von Quellen beruhen, bevorzugt auf Original- oder auf glaubwürdigen Sekundärquellen. Die Berichterstattung verzerrt Informationen nicht oder stellt diese falsch dar, um den eigenen Standpunkt zu unterstützen.	18
Unterlaufene Fehler werden regelmäßig richtiggestellt.	Die Redaktion hat wirkungsvolle Standards für Klar- und Richtigstellungen sowie Korrekturen etabliert. Auf der Seite ist eindeutig zu erkennen, wie Nutzerinnen und Nutzer redaktionell Verantwortliche kontaktieren können.	12,5
Klare Unterscheidung zwischen Nachricht und Meinung.	Webseiten, die sowohl Nachrichten als auch Kommentare veröffentlichen, unterscheiden diese deutlich voneinander. Die Berichterstattung greift nicht auf eine einseitige Auswahl an Fakten zurück, um einen bestimmten Standpunkt zu unterstützen. Webseiten, die eine bestimmte Sichtweise vertreten, legen diese offen.	12,5
Vermeiden irreführender Überschriften.	Es werden keine Überschriften veröffentlicht, die falsche Informationen enthalten, erheblich sensationalisieren oder übertreiben oder die nicht den tatsächlichen Inhalt des Beitrags wiedergeben.	10

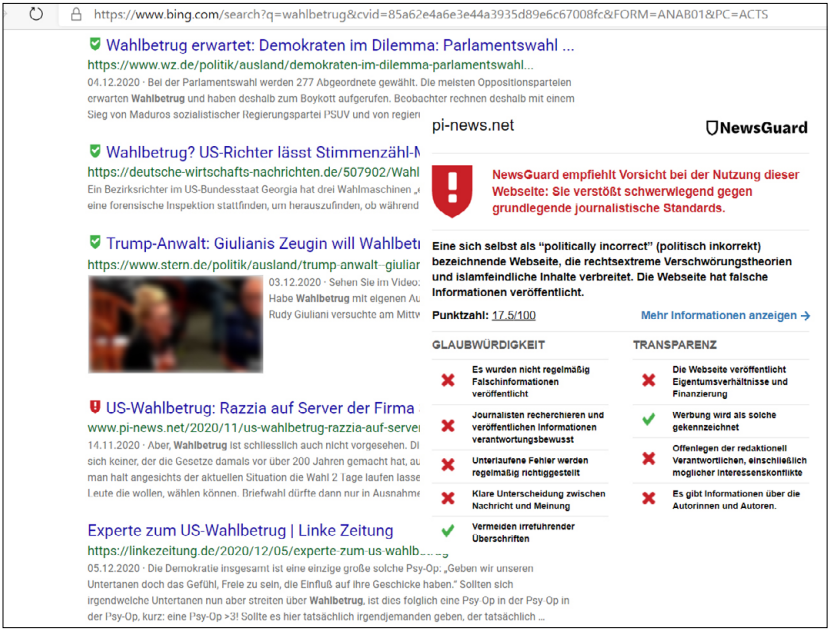
Transparenz

Kriterium	Erläuterung	Gewichtung (Punkte)
Die Webseite veröffentlicht Eigentumsverhältnisse und Finanzierung.	Eigentumsverhältnisse und/oder Finanzierung werden ebenso veröffentlicht wie ideologische Standpunkte/Positionen, die mit den Interessen der Eigentümerinnen und Eigentümer verbunden sind. Dies geschieht in einer nutzerfreundlichen und transparenten Art und Weise.	7,5
Werbung wird als solche gekennzeichnet.	Die Seite zeigt deutlich, welche Inhalte bezahlt sind und welche nicht.	7,5
Offenlegen der redaktionell Verantwortlichen, einschließlich möglicher Interessenskonflikte.	Informationen über Verantwortliche und mögliche Interessenkonflikte sind auf der Webseite zugänglich.	5
Informationen über Journalistinnen und Journalisten	Informationen über Personen, die die Inhalte des Mediums erstellen, sind auf der Webseite zugänglich.	5

Jede Prüfung einer Webseite durchläuft einen mehrstufigen redaktionellen Prozess, an dem immer mindestens fünf NewsGuard-Journalistinnen und Journalisten beteiligt sind. Dabei wird jedes Kriterium eingehend geprüft. Erreicht eine Webseite einen Gesamtscore von mindestens

60 Punkten, erhält sie eine grüne NewsGuard-Bewertung. Für weniger als 60 Punkte gibt es eine rote Bewertung (vgl. Abb. 1). Das jeweilige Ergebnis wird Nutzerinnen und Nutzern per Browsererweiterung in Form eines grünen oder roten NewsGuard-Icons angezeigt. Das Icon erscheint dann neben verlinkten Nachrichtenbeiträgen in Social-Media-Feeds, Suchmaschinentreffern, aber auch beim direkten Ansteuern einer Webseite. Per Mouseover werden die Bewertungsergebnisse in allen neun Kriterien angezeigt. Mit einem weiteren Klick lässt sich zudem ein ausführlicher Mediensteckbrief aufrufen, der zahlreiche Hintergründe zur jeweiligen Webseite sowie ausführliche Begründungen und Belege sowie sämtliche Quellen enthält. Die Erweiterung ist für alle gängigen Browser verfügbar und in dem Microsoft-Edge-Browser bereits als Opt-in-Feature implementiert. Für mobile Geräte ist zudem eine App verfügbar.

Abbildung 1: Die NewsGuard-Bewertung in der Nutzung



Aktuell, also mit dem Jahresende 2020, werden weltweit bereits mehr als 6.000 Webseiten von NewsGuard bewertet. Der Schwerpunkt liegt in den USA, aber seit Frühjahr 2019 sind auch jeweils Hunderte von Bewertungen französischer, italienischer und deutscher Medien verfügbar. Die Abdeckung liegt jeweils bei rund 95 Prozent der Onlineinteraktionen mit News-Content in sozialen Netzwerken. Zielgruppe sind Privatnutzerinnen und -nutzer, aber auch Bildungseinrichtungen. Auch in der Forschung werden die NewsGuard-Bewertungen eingesetzt, bspw. durch die University of Michigan, das Institute for Strategic Dialogue[188] oder, wie unten beschrieben, am Fraunhofer FKIE. Die Intention der NewsGuard-Bewertungen ist es, dass diese wie Nutrition Labels, also Nährwertangaben, funktionieren: Für Verbraucherinnen und Verbraucher soll auf den ersten Blick erkennbar sein, wie (un-)gesund der Inhalt ist, damit Nachrichten entsprechend bewusst und mit kritischem Blick für die Qualität der Inhalte konsumiert werden.

Ulrich Schade, Florian Meißner,
Albert Pritzkau und Sonja Verschitz

Lösungsansatz 2: Ein Tool zur inhaltlichen Bewertung

Prebunking ist nicht nur durch die Bewertung der Quelle, sondern auch durch eine automatisierte Beurteilung inhaltlicher Faktoren möglich. Dies soll hier auf der Grundlage eines existierenden Systems zur Warnung vor Fake News aufgezeigt werden (Pritzkau/Schade 2021). Das System schätzt automatisiert Beiträge in den sozialen Medien dahingehend ein, ob sie Fake News bzw. Beeinflussung enthalten könnten. Im Sinne des *Prebunkings* werden diese dann markiert. Das System ist im Kern ein mit Mitteln des Maschinellen Lernens entwickelter Klassifikator. Dieser nutzt für seine Klassifikation sowohl sprachliche Merkmale als auch Merkmale, die sich aus Metadaten ergeben. Wir werden im Weiteren nicht auf die technische Realisierung und damit auf die eingesetzten Algorithmen des maschinellen Lernens eingehen, sondern einen Detailblick auf die genutzten Merkmale werfen. Unser Fokus bei den sprachlichen Merkmalen liegt auf denen, die zu einer Emotionalisierung der Beiträge führen. Weitere sprachliche Merkmale ergeben sich aus dem Anwendungskontext. Wird etwa eine Beeinflussung durch den staatlichen Akteur Z angenommen, so dienen als weitere Merkmale typische Fehlermuster, die auf einen Verfasser oder eine Verfasserin mit der Muttersprache von Z hindeuten, welcher bzw. welche in Deutsch schreibt. Neben sprachlichen Merkmalen überprüft das System auch Metamerkmale, insbesondere solche, die annehmen lassen, dass die zu klassifizierende Nachricht über ein Bot im Netz verbreitet wird. Darauf werden wir im Detail eingehen, nachdem wir die sprachlichen Merkmale der Emotionalisierung betrachtet haben.

Emotion in der Sprache als Klassifikationsmerkmal

Bevor dargestellt wird, welche Rolle die Emotion in der Sprache als Kriterium zur Erkennung von Fake News spielt, muss für ein besseres Verständnis der Bedeutung dieses Kriteriums kurz auf die unterschiedlichen Funktionen von Sprache eingegangen werden. Sprache ist nicht nur ein dem Menschen eigenes Mittel, um Informationen über Dinge, Ereignisse und Sachverhalte auszutauschen und diese darzustellen. Darüber hinaus können wir mit ihr sowohl innere Zustände wie Einstellung, Wahrnehmung und Emotion(en) als auch individuelle Weltsichten zum Ausdruck bringen und für unser Gegenüber erfahrbar machen. Wir können aber auch durch ihren Einsatz selbst Handlungen durchführen (aufrufen, mobilisieren, abwerten, loben etc.) sowie das Gegenüber (die Rezipientin bzw. den Rezipienten) zur Durchführung einer Handlung bewegen (Grinth 2015: 1). Agierende können also durch den Einsatz sprachlicher Mittel Handlungen auslösen, die ihren Interessen und Intentionen entsprechen. Soll ein Beitrag aber affektiv, intuitiv und schnell verbreitet werden, werden die Emotionen des Gegenübers angesprochen. Artikel werden dann so aufgebaut, dass die enthaltende und zu transportierende Botschaft emotionalisiert vermittelt wird. Emotionalität bewirkt, dass eine Vielzahl anderer Nutzer und Nutzerinnen die Beiträge konsumieren, zitieren, kommentieren und weiterverbreiten.

Emotion lässt sich durch zahlreiche sprachliche Mittel evozieren, bspw. durch den Gebrauch eines Ideologievokabulars, das allerdings vom Nutzungskontext abhängt. Zum Ideologievokabular sind positiv konnotierte Begriffe (Affirmationswörter) und negativ konnotierte Begriffe (Stigmawörter) zu zählen. Zu den Affirmationswörtern zählen Fahnenwörter, welche den eigenen Standpunkt unterstreichen. Ein Beispiel dafür ist aus unserer westlichen Sicht das Wort „Demokratie“. Fahnenwörter werden „geprägt und verwendet, damit sich daran die Geister scheiden“ (Niehr, 2014, 73): Die eigene Anhängerschaft wird angesprochen und der Gegner wird provoziert. Noch emotionalisierender wirken Stigmawörter. Beispiele dafür aus dem Kontext der deutschen Innenpolitik reichen je nach eigener Position von „Linksmade“ bis zu „Nazi“. Mit Stigmawörtern wird der Gegner direkt angegriffen und verunglimpft.

Weniger offensichtlich, aber vielfältiger nutzbar ist der Einbezug des Gegenübers („wir“) oder der Einsatz von Adverbien, Adjektiven und des Konjunktivs, um Aussagen zu emotionalisieren („Wäre es nicht außerordentlich fahrlässig, wenn wir nicht …“). Als weiteres Beispiel soll hier die Aussage „X ist in der Tat eine demokratische Partei“ dienen. Der Ausdruck „in der Tat“ wird hier synonym für Adverbien wie „tatsächlich“, „wirklich“, „wahrhaftig“, „gewiss“ und „durchaus“ genutzt und dient der Betonung der Wahrhaftigkeit der Aussage und zur Beteuerung bzw. Unterstreichung der Position des Produzenten bzw. der Produzentin. Eine emotionale Nähe des Produzenten bzw. der Produzentin zu der Partei X kann damit abgeleitet werden. Dies erzeugt beim Gegenüber eine entsprechende emotionale Gegenreaktion, sei dies nun Zustimmung oder Ablehnung. Ziel ist die resultierende Weiterverbreitung.

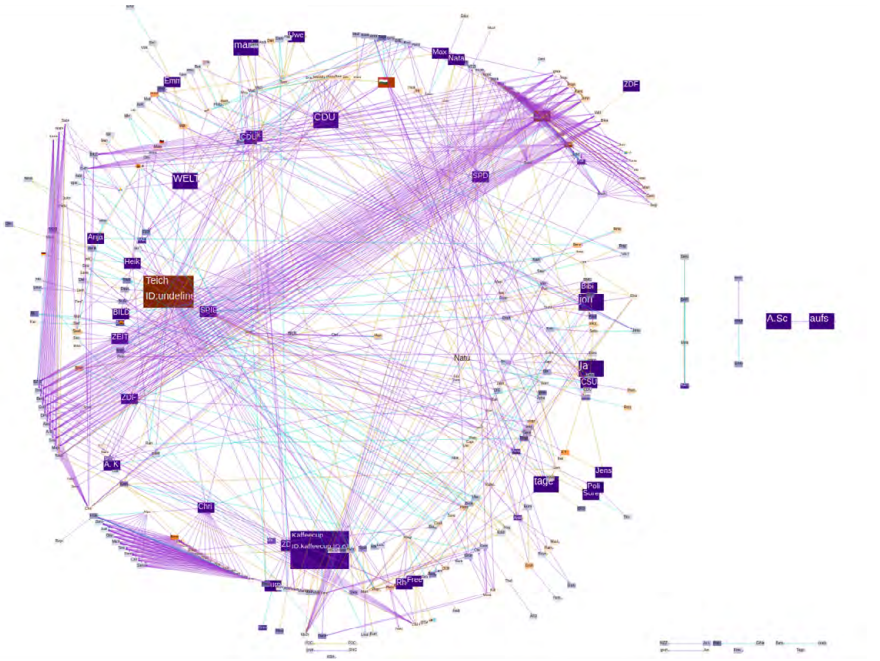
Insgesamt zeigt sich, dass bestimmte sprachliche Ausdrücke, etwa Wörter, die in einem bestimmten Kontext als Fahnenwörter oder als Stigmawörter wirken, oder Ausdrücke, die verstärken oder die die Einstellung der oder des Produzierenden zu einem Sachverhalt darlegen, emotionalisierend wirken. Das Auftreten solcher Ausdrücke entspricht nicht dem sachlichen Duktus einer Nachricht, dient aber deren Verbreitung im Netz und ist damit ein Merkmal, das auf das Ziel einer möglichst umfassenden Weiterverbreitung zu Lasten einer der (auch sprachlichen) Neutralität verpflichteten Publizierung von Nachrichten und somit auf Fake News bzw. manipulative Inhalte hinweist.

Metadaten als Klassifikationsmerkmal

Im Bereich der sozialen Medien lässt sich die Tendenz zur Verbreitung von Fake News und Desinformation häufig aus den für solche Accounts direkt verfügbaren Metadaten sowie aus den Daten zum Verhalten eines entsprechenden Accounts ableiten. Direkte Metadaten sind etwa die Anzahl der Follower, die Anzahl der „Friends“, das Alter des Accounts, der Accountname und weitere Angaben, die mit dem Account verknüpft sind (Shu/Wang/Liu 2018). Daten zum Verhalten ergeben sich daraus, wann ein

Account einen Beitrag postet, wem er als Follower beitritt, wen und was er zitiert usw. Da menschliche Nutzerinnen und Nutzer weniger regelgeleitet agieren als geskriptete Bots, sind insbesondere offensichtliche Regelmäßigkeiten im Verhalten ein Hinweis auf Bots, was wiederum daraufhin deutet, dass die geposteten Inhalte eines solchen Accounts problematisch sein könnten.

Abbildung 2: Visualisierung synthetischer Strukturen aus dem Referenzverhalten auf Twitter



Fraunhofer FKIE. Eigene Darstellung.

Um (statistische) Regelmäßigkeiten im Kommunikations- und Interaktionsverhalten von Accounts zu finden, nutzen wir Methoden der Netzwerkanalyse. Analyseaufgaben messen dabei Beziehungen auf der Mikroebene, also solche, die von einzelnen Accounts ausgehen, und verwenden Verfahren, um das Vorhandensein von Strukturen auf der Makroebene abzuleiten. Auf der Mikroebene erfolgen verschiedene Zentralitätsanalysen (Grad, Nähe und Eigenvektorzentralität), um damit zunächst einzelne Knoten (Accounts) in einem Netzwerk zu charakterisieren. Die kritischen Rollen spiegeln sich als Brücken, Senken oder Quellen im Netzwerk wider. Die Muster auf der Mikroebene erlauben dann den Rückschluss auf Makrostrukturen (z. B. auf Cliquen). In Abb. 2 wird das Referenzverhalten bei Twitter visualisiert. Im unteren linken Bereich der Abbildung lassen sich synthetische Strukturen erkennen, die sich durch eine außerordentlich hohe Verknüpfung auszeichnen. Entsprechende Strukturen sind Indikatoren für Bots (Chu et al. 2013, Gröndahl et al. 2018, Hall/Terveen/Halfaker 2018). Die Erfassung der Werte der angesprochenen Metamerkmale kann weitgehend automatisiert erfolgen, setzt aber voraus, dass entsprechende Daten über einen Zeitraum hinweg erfasst werden.

Das Zusammenspiel der Lösungsansätze

In den vorangehenden Abschnitten haben wir zwei Ansätze des *Prebunkings* vorgestellt, deren Anwendung nach unserer Ansicht die Resilienz gegen Beeinflussung durch Falsch- und Desinformation erhöhen können. In diesem Abschnitt werden wir darauf eingehen, wie diese Ansätze zusammenspielen können, um einen weiteren Mehrwert zu entfalten.

Studien haben gezeigt: *Prebunking* wirkt, indem es die wahrgenommene Glaubwürdigkeit von Beiträgen z. B. in sozialen Netzwerken senkt (Amazeen et al. 2018, Clayton et al. 2019). Warnhinweise werden wahrgenommen und führen zu einer kritischeren Rezeption des entsprechenden Inhalts. Durch die Bewertung von Nachrichten- und Informationswebseiten auf der Grundlage von journalistischen Glaubwürdigkeits- und Transparenzkriterien, wie dies durch NewsGuard erfolgt, kann also die Resilienz gegen Desinformation und Fake News gestärkt werden. Eine entsprechende Bewertung ist jedoch für die meisten Onlineplattformen und damit für die Accounts, die Beiträge in den sozialen Medien verbreiten, allein aufgrund der Anzahl solcher Quellen nicht manuell realisierbar. Die automatisierte Auswertung von Metadaten und Accountverhalten bietet hier also eine Ergänzung, über die auch solche Quellen bewertet werden können. Die automatisierte inhaltliche Kategorisierung von Beiträgen liefert darüberhinausgehend weitere Indizien für die Verbreitung von Fake News und Beeinflussungskampagnen. Da sich diese Analyse auf Einzelbeiträge und nicht auf Quellen bezieht, kann die Kombination der beiden Lösungsansätze auch für die frühzeitige Erkennung von Beeinflussungskampagnen genutzt werden. Bei gleichzeitigem Auftreten von Warnungen – verdächtiger Inhalt aus verdächtiger Quelle – kann der Inhalt dafür mit Stichproben überprüft werden.

Abschließend sei erwähnt, dass die Bewertungen durch NewsGuard auch eine Evaluation derjenigen sprachlichen Merkmale erlaubt, mit der die inhaltliche Bewertung erfolgt. Hat man für ein Thema eine größere Anzahl von Texten und Beiträgen aus nach NewsGuard vertrauenswürdigen und nicht vertrauenswürdigen Quellen, so lässt sich untersuchen, welche sprachlichen Mittel nichtvertrauenswürdige Quellen nutzen, die vertrauenswürdige Quellen nicht oder jedenfalls deutlich weniger anwenden. Ein einfaches Beispiel eines sprachlichen Ausdrucks dieser Art ist das Adverb „absolutely", das dem oben analysierten „in der Tat" gleicht. Bei einer Untersuchung von Beiträgen, die sich auf die Stimmabgabe per Brief bei der US-Wahl 2020 bezogen, fand sich das Adverb „absolutely" sehr häufig in Beiträgen aus nach NewsGuard weniger glaubwürdigen Quellen, aber nur selten in den Beiträgen vertrauenswürdiger Quellen.

187 https://www.newsguardtech.com/de/ – Einer der Autoren dieses Beitrags, Florian Meißner, ist Advisor Germany bei NewsGuard.

188 https://csmr.umich.edu/projects/iffy-quotient/ (letzter Zugriff 03.12.2020).

Literaturverzeichnis

A Amazeen, M. A./Thorson, E./Muddiman, A./Graves, L. (2018). Correcting political and consumer misperceptions: The effectiveness and effects of rating scale versus contextual correction formats. In: Journalism & Mass Communication Quarterly, 95(1), 28–48. https://doi.org/10.1177/1077699016678186 (letzter Zugriff: 10.12.2020).

B Brennen, S./Simon, F./Howard, P. N./Nielsen, R. K. (2020). *T*ypes, sources, and claims of COVID-19 misinformation. https://reutersinstitute.politics.ox.ac.uk/types-sources-and-claims-covid-19-misinformation (letzter Zugriff: 10.12.2020).

C Chu, Z./Gianvecchio, S./Koehl, A./Wang, H./Jajodia S. (2013). Blog or block: Detecting blog bots through behavioral biometrics. In: Comput Networks, 57(3), S. 634–646. http://dx.doi.org/10.1016/j.comnet.2012.10.005 (letzter Zugriff: 10.12.2020).

Clayton, K./Blair, S./Busam, J. A./ Forstner, S./Glance, J./Green, G./ Nyhan, B. (2019). Real solutions for fake news? Measuring the effectiveness of general warnings and fact-check tags in reducing belief in false stories on social media. In: Political Behavior, 38(2), 173. https://doi.org/10.1007/s11109-019-09533-0 (letzter Zugriff: 10.12.2020).

Cook, J./Lewandowsky, S. (2011). The debunking handbook (Version 2). St. Lucia, Australia: University of Queensland.

D Del Vicario, M./Bessi, A./Zollo, F./Petroni, F./Scala, A./Caldarelli, G. et al. (2016). The spreading of misinformation online. In: Proceedings of the National Academy of Sciences of the United States of America, 113(3), S. 554–559. https://doi.org/10.1073/pnas.1517441113 (letzter Zugriff: 10.12.2020).

F Fletcher, R./Cornia, A./Graves, L./Nielsen, R. K. (2018). Measuring the reach of „fake news" and online disinformation in Europe, Reuters Institute for the Study of Journalism. https://reutersinstitute.politics.ox.ac.uk/sites/default/files/2018-02/Measuring%20the%20reach%20of%20fake%20news%20and%20online%20distribution%20in%20Europe%20CORRECT%20FLAG.pdf (letzter Zugriff: 10.12.2020).

G Girnth, H. (2015). Sprache und Sprachverwendung in der Politik. Eine Einführung in die linguistische Analyse öffentlich-politischer Kommunikation. Germanistische Arbeitshefte, 39. 2. überarbeitete und erweiterte Auflage. Berlin: de Gruyter.

Gröndahl, T./Pajola, L./Juuti, M./Conti, M./Asokan, N. (2018). All you need is „love": Evading hate speech detection. In: *Pro*ceedings of the ACM Conference on Computer and Communications Security. Association for Computing Machinery (S. 2–12). https://doi.org/10.1145/3270101.3270103 (letzter Zugriff: 10.12.2020).

H Hall, A. K./Terveen, L. G./Halfaker, A. (2018). Bot detection in Wikidata using behavioral and other informal cues. In: Proceedings of the ACM on Human-Computer Interaction, 2 (CSCW), Art. No. 64. https://doi.org/10.1145/3274333 (letzter Zugriff: 10.12.2020).

J Johnson, H. M./Seifert, C. M. (1994). Sources of the continued influence effect: When misinformation in memory affects later inferences. In: Journal of Experimental Psychology: Learning, Memory, and Cognition, 20(6), S. 1420–1436. https://doi.org/10.1037/0278-7393.20.6.1420 (letzter Zugriff 10.12.2020).

K Kümpel, A. S. (2019). Nachrichtenrezeption auf Facebook. Vom beiläufigen Kontakt zur Auseinandersetzung. Wiesbaden: Springer Fachmedien. https://doi.org/10.1007/978-3-658-24229-9 (letzter Zugriff: 10.12.2020).

L Lazer, D. M.J./Baum, M. A./Benkler, Y./Berinsky, A. J./Greenhill, K. M./Menczer, F. et al. (2018). The science of fake news. Science (New York, N. Y.), 359(6380), S. 1094–1096. https://doi.org/10.1126/science.aao2998 (letzter Zugriff: 10.12.2020)

Lewandowsky, S./Ecker, U. K.H./Cook, J. (2017). Beyond Misinformation: Understanding and Coping with the „Post-Truth" Era. In: Journal of Applied Research in Memory and Cognition, 6(4), S. 353–369. https://doi.org/10.1016/j.jarmac.2017.07.008 (letzter Zugriff: 10.12.2020)

M Mantzarlis, A. (2018). Fact-checking 101. In: C. Ireton/J. Posetti (Eds.). Journalism, „fake news" & disinformation. Handbook for journalism education and training (UNESCO series on journalism education, S. 85–100). Paris: United Nations Educational Scientific and Cultural Organization.

Meißner, F. (2020). Mediale Krisenkommunikation 24/7, Auf: European Journalism Observatory. https://de.ejo-online.eu/qualitaet-ethik/mediale-krisenkommunikation-24-7-der-journalismus-und-das-coronavirus (letzter Zugriff: 10.12.2020).

N Niehr, T. (2014). Einführung in die linguistische Diskursanalyse. Darmstadt: Wissenschaftliche Buchgesellschaft.

Nyhan, B./Reifler, J. (2010). When Corrections Fail: The Persistence of Political Misperceptions. In: Political Behavior, 32(2), S. 303–330. https://doi.org/10.1007/s11109-010-9112-2 (letzter Zugriff: 10.12.2020).

P Pritzkau, A./Schade, U. (2021). Vorsicht: mögliche „Fake News" – ein technischer Ansatz zur frühen Erkennung. In Klimczak, P./Zoglauer, T. (Hrsg.). Wahrheit und Fake im postfaktisch-digitalen Zeitalter. Distinktionen in den Geistes- und IT-Wissenschaften. Wiesbaden: Springer-Vieweg.

S Sängerlaub, A./Meier, M./Rühl, W.-D. (2018). Fakten statt Fakes. Verursacher, Verbreitungswege und Wirkungen von Fake News im Bundestagswahlkampf 2017, Stiftung Neue Verantwortung. https://www.stiftung-nv.de/sites/default/files/snv_fakten_statt_fakes.pdf (letzter Zugriff: 10.12.2020).

Shu, K./Wang, S./Liu, H.(2018). Understanding User Profiles on Social Media for Fake News Detection. In: Proceedings of the IEEE 1st Conference on Multimedia Information Processing and Retrieval, S. 430–435. https://ieeexplore.ieee.org/abstract/document/8397048/ (letzter Zugriff: 10.12.2020)

V Van Bavel, J. J./Pereira, A. (2018). The Partisan Brain: An Identity-Based Model of Political Belief. In: Trends in Cognitive Sciences, 22(3), S. 213–224. https://doi.org/10.1016/j.tics.2018.01.004 (letzter Zugriff: 10.12.2020)

Vosoughi, S./Roy, D./Aral, S. (2018). The spread of true and false news online. In: Science (New York, N. Y.), 359(6380), S. 1146–1151. https://doi.org/10.1126/science.aap9559 (letzter Zugriff: 10.12.2020).

W Wardle, C./Derakhshan, H. (2018). Thinking about „Information Disorder“: Formats of Misinformation, Disinformation, and Mal-Information. In: C. Ireton/J. Posetti (Eds.). Journalism, „fake news“ & disinformation. Handbook for journalism education and training (UNESCO series on journalism education, S. 44–56). Paris: United Nations Educational Scientific and Cultural Organization.

WHO (2020, 2. Februar). Novel Coronavirus(2019-nCoV). Situation Report – 13, WHO. https://www.who.int/docs/default-source/coronaviruse/situation-reports/20200202-sitrep-13-ncov-v3.pdf (letzter Zugriff: 10.12.2020).

Fake News und Propagandaarten

als Herausforderung für Bundeswehreinsätze im Ausland

Amelie Stelzner und Jakob Landwehr-Matlé

07

Während der Begriff Fake News im Zusammenhang mit öffentlichen Informationskampagnen in den vergangenen Jahren an Bedeutung gewonnen hat und in den Fokus von Wissenschaft und Politik gerückt ist, eignet er sich nicht für die Untersuchung der Bundeswehr. Stattdessen bietet sich in diesem Kontext der Begriff Propaganda an. Im Zuge der Auseinandersetzung mit den Definitionen und Konzepten von Fake News zeigen wir in diesem Beitrag jedoch, dass Desinformationen sich sowohl als Propagandaart als auch als Kernelement vieler Ansätze von Fake News wiederfinden. Wir plädieren dafür, Desinformationen in den Mittelpunkt wissenschaftlicher Untersuchungen im Kontext der Bundeswehr zu rücken. Am Fallbeispiel des Einsatzes Enhanced Forward Presence (eFP) in Litauen zeigen wir auf, dass die Bundeswehr strategisch ausgerichteten Desinformationskampagnen ausgesetzt ist. Um diesen zu begegnen, werden unterschiedliche Fähigkeiten benötigt, da sich jeder Angriff unterscheidet und unterschiedliche Herausforderungen birgt. Daraus folgt, dass es keinen Automatismus gibt, um solche Gefahren im Cyber- und Informationsraum zu bekämpfen, sondern situativ entschieden werden muss.

Bundeswehr und Fake News im akademischen Kontext

Wie kann die Bundeswehr Propaganda gegen sich erkennen und begegnen? Welche Strukturen gibt es diesbezüglich in der Bundeswehr? Diesen übergeordneten Fragen geht der vorliegende explorative Beitrag nach, der sich zunächst dem Begriff Fake News und seiner Verwendung widmet und damit eine Grundlage für die mögliche Einordnung im Kontext der Bundeswehr schafft.

Der Begriff Fake News hat in den vergangenen Jahren an Aufmerksamkeit gewonnen und wird seither vermehrt in der wissenschaftlichen Literatur und in politischen Debatten berücksichtigt (Wagner/Boczkowski 2019, 872). In diesem politischen Kontext wird üblicherweise auf die Präsidentenwahl in den USA 2016 und die Beeinflussung der Brexit-Kampagne im selben Jahr in Großbritannien verwiesen (Bradshaw/Howard 2018, 3; (Molina/Sundar/Le/Lee 2019, 184). Tatsächlich wurde der Begriff erst 2017 offiziell in das Oxford Wörterbuch übernommen und gewann im selben Jahr die „Collins Dictionary Word of the Year"-Auszeichnung (Sample/Justice/Darraj 2019, 1; Vamanu 2019, 197). Die oft mit finanziellen oder ideologischen Motiven verbreiteten Desinformationen gehen als Form der Propaganda geschichtlich viel weiter zurück (Hindman/Barash 2018, 9). Fake News haben sich jedoch im Zeitalter der internetbasierten Medien zu einem bedeutenden Phänomen entwickelt und sind in den Fokus von wissenschaftlichen Auseinandersetzungen und der öffentlichen Debatte gerückt (Molina/Sundar/Le/Lee 2019, 180). Daraus wird allerdings auch ersichtlich, wie aufgeladen der Begriff inzwischen ist und dass eine sachliche Einordnung dadurch erschwert wird.

Fake News können eine starke Politisierung und Misstrauen gegenüber öffentlichen Einrichtungen bewirken und so schwerwiegende Konsequenzen für Demokratien haben (Allen/Howland/Mobius/Rothschild/Watts 2020, 1). Prinzipiell wird zwischen zwei Arten von Fake News unterschieden: „Genre" und „Label" (Egelhofer/Lecheler 2019, 97). Während sich das Genre auf die Delegitimierung von Medien bezieht, wird unter dem „Label" eine Verbreitung von falschen Informationen verstanden, der eine Absicht zu Grunde liegt. Diese Form von Fake News hat vermehrt die Aufmerksamkeit der Forschung auf sich gezogen (Habgood-Coote 2018, 1033; Egelhofer/Lecheler 2019, 97). In diesem Zusammenhang nähert sich die Wissenschaft dem Phänomen aus verschiedenen disziplinären Zugängen; dabei wird der Fokus auf eine Kombination unterschiedlicher Ansätze und Methoden gelegt (Sample/Justice/Darraj 2019, 1). Eine große Anzahl der Beiträge beschäftigt sich mit der Definition von Fake News und versucht diese von ähnlichen Begriffen abzugrenzen, als „Oberbegriff" zu etablieren oder anhand von Kriterien eine Einordnung und Abgrenzung zu ermöglichen (siehe beispielsweise Allcott/Gentzkow 2017; Wardle/Derakhshan 2017; Tandoc Jr./Lim/Ling 2018; Asanov 2019; Molina/Sundar/Le/Lee2019). Darüber hinaus fokussiert sich die Forschung auf die Wahrnehmung und damit verbunden die Messung der Glaubwürdigkeit von Fake News sowie deren Verbreitung (Hajduk/Zowislo-Grünewald 2020). Das Aufspüren von Fake News durch entwickelte Modelle (siehe beispielsweise Zhou/Jain/Phoha/Zafarani 2019) führt zu verschiedenen Lösungsansätzen, um dieser Form von Nachrichten reaktiv zu begegnen und sie proaktiv zu verhindern.[189]

Fake News werden im militärischen Kontext häufig mit Propaganda in Verbindung gebracht. Dabei werden die Aktivitäten einzelner Staaten wie beispielsweise Russland (Guadagno/Guttieri 2019) oder der Informationskrieg in einzelnen Ländern wie der Ukraine (Sarmina 2020) oder in der Golfkrise (Jones 2019) gezielt untersucht. In Verbindung mit der Bundeswehr werden Fake News in der Wissenschaft hingegen bislang kaum behandelt. Es mangelt an Untersuchungen, welche die Bundeswehr heute und im Hinblick auf die Entwicklungen in den vergangenen Jahren betrachten. In einem der wenigen vorhandenen Beiträge untersucht Drews (2006) die psychologische Verteidigung und Kampfführung der Bundeswehr vor

dem Hintergrund der Ost-West-Konfrontation zwischen 1957 und 1990. In einem von Möllers und Jacobs (2019) herausgegebenen Sammelband geht es um die Medienwirkung der Bundeswehr und die mediale Rolle, die die Bundeswehr in Deutschland spielt. Der Fokus liegt jedoch auf der medialen Berichterstattung über die Bundeswehr und deren Auswirkungen. Busch und Düe (2017) beschreiben und bewerten zumindest die Aufstellung des Kommandos Cyber- und Informationsraum (CIR) als Antwort auf neue Herausforderungen im Informationsraum. Daher betrachten wir in diesem Beitrag eine Problematik, die in den vergangenen Jahren an Bedeutung gewonnen hat.

Zunächst wird dafür die methodische Vorgehensweise kurz beschrieben. Im nächsten Abschnitt widmen wir uns bisherigen Versuchen Fake News zu definieren, und ordnen die Bundeswehr und ihren Umgang mit diesem Begriff ein. Ziel ist es, aufzuzeigen, dass Fake News in allen Definitionsversuchen zwar Elemente abdecken, die auch für die Bundeswehr Relevanz haben, der Begriff selbst aber für eine wissenschaftliche Auseinandersetzung im Zusammenhang mit der Bundeswehr unpassend ist. Damit ist der Rahmen geschaffen, um die Maßnahmen, Instrumente und Kompetenzen der Bundeswehr zu betrachten und anhand eines Fallbeispiels – der anerkannten Mission 2017 in Litauen[190] – zu veranschaulichen. Der Beitrag soll eine erste Übersicht der Herausforderungen durch Fake News für Auslandsmissionen der Bundeswehr liefern und die deutschen Streitkräfte im Rahmen der akademischen Debatte über Fake News als Akteur einzuordnen.

Methodik

Um die aufgeworfenen Forschungsfragen zu beantworten und dem explorativen Charakter der Studie gerecht zu werden, greifen wir auf Experteninterviews zurück. Wir nutzten gezielte explorative Experteninterviews, um allgemeine Informationen zu sammeln und Forschungslücken zu schließen (Kaiser 2014, 35). Die interviewten Experten[191] setzen sich aus Angehörigen der Streitkräfte sowie dem Bereich des Bundesverteidigungsministeriums (BMVg) zusammen. Die Interviews wurden semistrukturiert mithilfe eines Leitfadens geführt, der bei Bedarf verändert und an die Gesprächssituation angepasst worden ist. Zudem wurden gegebenenfalls Informationen aus vorherigen Interviews mit eingebaut (siehe für mehr Informationen Gläser/Laudel 2010, 149).[192] Für die virtuell oder per Telefon geführten Interviews wurden Gedächtnisprotokolle während und direkt nach den Interviews und in Absprache mit den interviewten Personen angefertigt. Insgesamt wurden vier Einzelinterviews und ein Gruppeninterview geführt. Wir griffen zudem auf die „kommunikative Validierung" oder auch *member check* (Bogner/Littig/Menz 2014, 95) zurück und überprüften die Ergebnisse unserer Arbeit mithilfe der interviewten Experten. Als Gütekriterium diente in diesem Zusammenhang der Umstand, ob unserer Interpretation und Herausarbeitung der relevanten Informationen in den Gedächtnisprotokollen von Seiten der Experten zugestimmt wurde, oder, ob Informationen ergänzt werden mussten.[193] Bei der Auswahl des Fallbeispiels folgen wir dem *typical case* nach Seawright und Gerring (2008) und Gerring (2006). Im Folgenden gilt es zunächst zu untersuchen, wie sich die wissenschaftliche Auseinandersetzung und der Versuch einer Definition mit der Verwendung des Begriffes Fake News durch die Bundeswehr decken.

Fake News als unpassender Begriff bei der Bundeswehr

Obwohl der Begriff Fake News mittlerweile Teil des Alltagswortschatzes ist, erweist sich eine genaue Begriffsbestimmung als schwierig. Handelt es sich hierbei um einen Oberbegriff für die vielen verschiedenen Formen, der die Definitionen von falschen Informationen bündelt, wie beispielsweise von Molina/Sundar/Le/Lee (2019, 5) vorgeschlagen? Und: wie lässt sich der Begriff zu anderen Definitionen von falschen Informationen abgrenzen?

Zunächst lassen sich einige Elemente von einem Oberbegriff trennen. Dazu gehören Satire, die so gehalten ist, dass sie nicht missverstanden werden kann, oder Fehler in Nachrichten, die nicht beabsichtigt sind. Verschwörungstheorien, die deren Begründer meist für wahr halten, sind ebenfalls abzugrenzen (Allcott/Gentzkow 2017, 5). Schwieriger wird es bei der Berücksichtigung von einer Intention bei der Verbreitung von falschen Informationen (Allcott/Gentzkow 2017, 213; Jack 2017, 15). Zimmermann und Kohring (2020, 24–25) argumentieren, dass Intention und die Formatierung als vermeintlich authentische Informationen die einzigen zwei allgemein anerkannten Elemente einer Definition von Fake News sind. Jedoch herrscht Uneinigkeit darüber, ob die Informationen immer empirisch falsch sein müssen, nur online-basierte Informationen einbezogen werden oder eine tatsächliche Täuschung erfolgt sein muss, um von Fake News sprechen zu können. Grundlegend kann festgestellt werden, dass für die Güte der Definition der damit verbundene Fokus entscheidend ist (Zimmermann/Kohring 2020, 24). Hierbei bietet sich eine Differenzierung zwischen drei Arten von Informationen, die sich bei den Dimensionen Schaden und Intention unterscheiden, an: Desinformationen, Fehlinformationen und *Malinformationen* (Wardle/Derakhshan 2017, 20). Desinformationen sind absichtlich falsch formulierte Informationen, die

einem ausgewählten Ziel Schaden zufügen sollen und beide Dimensionen damit kombinieren. Fehlinformationen hingegen sind inkorrekt, aber haben nicht das Ziel, Schaden zu verursachen. *Malinformationen* wiederum sollen Schaden anrichten, aber basieren nicht auf Falschinformationen (Wardle/Derakhshan 2017, 20). Desinformationen reichen vom bewussten manipulativen Entwurf der Information über die Verbreitung bis hin zur Manipulation eines bestimmten Publikums (Gelfert 2018, 84). Nemr/Gangware (2019, 4) weisen darauf hin, dass bei Desinformation durchaus authentisches Material verwendet werden kann, welches nur durch den Kontext verzerrt wird, wodurch sie eine falsche Verbindung beim Empfänger des Materials erzeugen. Dazu gehören beispielsweise Bilder mit einer falschen Beschreibung oder Bildausschnitte, die entscheidende Informationen zum Kontext der Aufnahme vermissen lassen.

Wardle und Derakhshan (2017) kombinieren alle drei Begriffe in ihrer Definition von Fake News. Turcilo und Obrenovic (2020, 12) kommen bei demselben Anliegen nicht auf den Begriff Fake News, sondern Informationsunordnung. Hindman (2018, 13) bezieht sich auf den Inhalt von Nachrichten, die nicht den üblichen Prozess der Verifizierung durchlaufen haben, und Egelhofer und Lecheler (2019, 6) definieren Fake News als Desinformationen in einem journalistischen Format. Nemr und Gangware (2019, 5) fassen zusammen: „However, the literature on the topic overwhelmingly uses the terms misinformation, disinformation, and even fake news and propaganda interchangeably." Tatsächlich ist der Begriff Propaganda der Einzige der angesprochenen Begriffe, der im Weißbuch 2016 zur Sicherheitspolitik und zur Zukunft der Bundeswehr verwendet wird: „Alle Bereiche gesellschaftlichen Lebens können zum Ziel hybrider Angriffe werden: Durch Cyberangriffe und Informationsoperationen (zum Beispiel Propaganda), wirtschaftlichen und finanziellen Druck sowie Versuche zur politischen Destabilisierung" (Die Bundesregierung 2016, 39). Dies gibt einen Einblick in die Verwendung der Begrifflichkeit Propaganda.

Propaganda hat im Zuge der durch Fake News manipulierten politischen Prozesse, wie den Wahlen in den USA oder in der Brexit-Kampagne, in den letzten Jahren ein vermehrtes Interesse hervorgerufen. Tandoc Jr., Lim und Ling (2018, 10) verweisen in diesem Zusammenhang auf das Verständnis von Propaganda als „news stories which are created by a political entity to influence public perceptions. The overt purpose is to benefit a public figure, organization or government." Generell kann zwischen weißer, grauer und schwarzer Propaganda unterschieden werden. Während weiße Propaganda wahre Informationsquellen nutzt, ist schwarze Propaganda darauf ausgerichtet, Quellen bewusst fehlzuinterpretieren und unzutreffende Quellen zu nutzen. Graue Propaganda stellt eine Zwischenform dar (Jowett/O'Donnell 2012, 17–19). Im militärischen Kontext lässt sich unserer Meinung nach jedoch eher ein Bezug zur Attribuierbarkeit herstellen: Der Verfasser, die Verfasserin ist bei weißer Propaganda ersichtlich, bei grauer nicht bekannt und im Fall von schwarzer Propaganda gibt der Verfasser, die Verfasserin vor, jemand anderes zu sein. Dies zeigt deutlich, dass auch Propaganda definitorische Elemente von Fake News enthält. Dadurch wird aber umso deutlicher, dass eine Definition seitens des Akteurs[194] erfolgen muss, da weder eine einheitliche vorhanden ist, noch die Begrifflichkeiten gut voneinander trennbar sind. Bisher sind keine Definitionen bezüglich Fake News von Seiten des BMVg veröffentlicht worden. Im Jahr 2020 wurden zumindest intern im Kontext der Fähigkeitsentwicklung folgende Arbeitsbegriffe entwickelt.

Tabelle 1: Übersicht relevanter Arbeitsbegriffe vom BMVg (2020):

Desinformation	Propagandaart, bei der durch den Absender unwahre Informationen mit Schädigungswillen verbreitet werden.
Irreführende Information	Propagandaart, bei der objektiv „wahre" Sachverhalte durch falsche bzw. äußerst begrenzte Kontexte, starke Vereinfachung oder andere Bezüge verzerrt und mit Schädigungswillen verbreitet werden.
Misinformation	Umfasst die Verbreitung von unwahren Informationen ohne Schädigungswillen. Sie kann durch gegnerische Akteure propagandistisch aufgegriffen werden, indem die organische Verbreitung systematisch durch anorganische Netzwerke unterstützt und gefördert wird.
Malinformation	Wahre, allerdings geschützte Information, die von Unbefugten mit Schädigungswillen verbreitet wird und häufig durch kriminelles Handeln (Hacking, Verrat etc.) erworben wurde.
Propaganda	Systematische Verbreitung von politischen, weltanschaulichen, o. ä. Botschaften mit Wirkungs- und/oder Schädigungspotenzial, die einem Akteur zugeordnet werden. Ziel der Propaganda ist es, den Diskurs zu stören und/oder die Wahrnehmung, Einstellung und das Verhalten eines Rezipienten oder einer Rezipientengruppe im Sinne des Akteurs zu beeinflussen.

(basierend auf Bereitstellung und der Formulierungen eines Dokuments im Anschluss an das Gruppeninterview)

Zwei Merkmale werden aus diesen Arbeitsbegriffen ersichtlich: Erstens ähnelt die Unterscheidung sehr der des wissenschaftlichen Diskurses über Malinformationen, Desinformationen und Mis- bzw. Fehlinformationen. Zweitens erfolgt keine Definition von Fake News. Da der Begriff Fake News unter anderem keinen werturteilsfreien Gebrauch zulasse, sprechen sich Experten des BMVg und der Bundeswehr gegen seine Verwendung aus und verwenden stattdessen den Begriff Desinformation als eine Form von Propaganda.

Auffallend ist, dass alle oben genannten Informationsformen als Unterkategorie von Propaganda erfasst werden können. Insbesondere die Subkategorie Desinformation scheint für eine Betrachtung der Bundeswehr interessant, weswegen wir diese im Folgenden analysieren werden.

Überblick: Bedeutung von Desinformation und Strukturen in der Bundeswehr

Im Weißbuch der Bundesregierung von 2016 wird Cyber-Abwehr als notwendige Bedingung für die nationale Sicherheit und als eine von zehn zentralen Herausforderungen für die deutsche Sicherheitspolitik genannt. Innere und äußere Sicherheit sind hierbei eng miteinander verwoben, die Gewährleistung von Cybersicherheit sei eine gesamtstaatliche Aufgabe (Die Bundesregierung 2016, 37 f.). Das Bundesministerium des Innern, für Bau und Heimat (BMI) ist für die Cybersicherheit und den Schutz der zivilen Infrastruktur zuständig und entwickelt federführend die deutsche Cybersicherheitsstrategie. Das Auswärtige Amt (AA) gestaltet die internationale Cybersicherheitspolitik, während das Bundesverteidigungsministerium (BMVg) für die Cyberabwehr zuständig ist (Die Bundesregierung 2016, 38).

Für die Bundeswehr hat Generalleutnant Leinhos (2017), erster Inspekteur des Cyber- und Informationsraums und Leiter des entsprechenden Aufbaustabes, die neue Aufgabe wie folgt zusammengefasst: „Wir verteidigen Deutschland im Cyber- und Informationsraum“ (news aktuell GmbH 2020). Dafür wurden neue Strukturen geschaffen und Personal eingestellt: Im Jahr 2017 wurde der Cyber- und Informationsraum als eigenständiger militärischer Organisationsbereich aufgestellt. Dessen oberste Dienststelle und gleichzeitig Stab des Inspekteurs ist das Kommando Cyber- und Informationsraum, ihm unterstehen verschiedene Dienststellen wie das Kommando Strategische Aufklärung direkt (BMVg o. D. b). Die Aufgaben des CIR sind vielfältig und reichen vom Schutz und Betrieb der IT-Systeme der Bundeswehr bis hin zur Stärkung und Weiterentwicklung der Fähigkeiten bei Aufklärung und Wirkung im Cyber- und Informationsraum (BMVg o. D. b; BMVg o. D. f). Auch im Rahmen der North Atlantic Treaty Organization (NATO) und der Europäi-

schen Union (EU) wurden verschiedene Zentren geschaffen, um hybriden Bedrohungen und Desinformation zu begegnen. Zwei davon werden im Laufe des Beitrags näher beschrieben.

Inland: Zurückgenommene Rolle der Bundeswehr

In Bezug auf Desinformation gilt es zunächst, Bedrohungslagen zu erkennen, diesen zu begegnen und im Idealfall das Eintreten von Risiken und Schäden zu verhindern. In Zeiten zunehmender hybrider Bedrohungsszenarien können sich Aktionen im CIR unter anderem auf militärische Einsätze vor Ort auswirken. Dies gilt sowohl für das jeweilige Einsatzgebiet der Bundeswehr als auch für die Stabilität kritischer Infrastrukturen sowie der politischen Stabilität Deutschlands (Interview 4; Interview 5; BMVg o. D. c).

Festzuhalten ist zunächst, dass in Deutschland keine systematische Überwachung gesellschaftlicher Meinungsbildungsprozesse seitens der Bundeswehr stattfindet und auch in Zukunft nicht stattfinden wird (Interview 4). Die Bundeswehr konzentriert sich auf den Schutz ihrer eigenen Soldatinnen und Soldaten sowie zivilen Mitarbeitenden (Interview 2).

Allerdings lässt sich hervorheben, dass neben den neuen, veränderten Strukturen und dem Personalaufbau die Bundeswehr zum Erkennen von Desinformation vermehrt mit der Wissenschaft kooperiert (Institut für Politische Wissenschaft o. D.; Interview 2). Zusammen mit der Universität der Bundeswehr München und der Rheinisch-Westfälischen Technischen Hochschule Aachen werden derzeit Instrumente und Strategien entwickelt, um Desinformation erkennen zu können. So soll mittels eines möglichst breit gedachten Ansatzes mit Unterstützung aus dem akademischen Bereich dieser neuartigen Bedrohung entgegentreten und Synergieeffekte genutzt werden (Institut für Politische Wissenschaft o. D.; Interview 2; Lieberenz 2019). Im Gespräch mit Interviewpartner 2 wurden die hohe Relevanz der Zusammenarbeit sowie ihr Nutzen bestätigt. Hier ist insbesondere das seit 2018 laufende Projekt zur Fähigkeitsentwicklung „Propaganda Awareness“ zu nennen, dessen Erkenntnisse ab Anfang 2022 operativ

umgesetzt werden sollen (Interview 2; Redaktion der Bundeswehr 2021). Das Projekt ist thematisch und in der Durchführung das erste seiner Art bei der Bundeswehr: Untersucht wird die Wirkung von Propaganda gegen die Bundeswehr grundsätzlich. Ebenso gilt es, Fähigkeiten der Analyse und der Prognose von Bedrohungssituationen aufzubauen; hierfür werden entsprechende Werkzeuge entwickelt. Mensch und Maschine sollen frühzeitig gegen die Bundeswehr gerichtete und gestreute Desinformation erkennen, um zielgerichtet Abwehrmaßnahmen durchzuführen und eine entsprechende Widerstandsfähigkeit im kognitiven Bereich (Resilienz) aufzubauen. So soll die Bundeswehr in die Lage versetzt werden, belastbar zu erkennen, wie und in welchem Ausmaß Soldatinnen und Soldaten (potentiell) durch Propaganda, sowohl im Einsatz als auch zu Hause, beeinflusst werden (Interview 2).

Insgesamt begegnet die Bundeswehr Desinformation im Inland dementsprechend nicht aktiv, sondern reaktiv. Auch gibt es keine festgelegten Strukturen oder Antwortschemata, das heißt keinen definierten Handlungsablauf. Ob und welche Reaktion von welchem Akteur zu welchem Zeitpunkt erfolgt, wird daher situativ entschieden (Interview 4).

Wie im Interview 4 bestätigt, können eine breite und leicht zugängliche Informationsbasis und Aufklärungsarbeit Desinformation die Schlagkraft nehmen. Dementsprechend berichtet das BMVg über aktuelle Geschehnisse sowie die Streitkräfte im Rahmen ihrer Presse- und Öffentlichkeitsarbeit, der sogenannten Informationsarbeit (BMVg o. D. f). Ziel ist es, die Bundesbürgerinnen und -bürger sowie die Politikerinnen und Politiker transparent und umfassend über die Bundeswehr zu informieren (BMVg o. D. d). Die kontinuierliche Informationsbereitstellung dient auch dem Aufbau von Resilienz gegenüber Propaganda und Desinformation der Bevölkerung (Interview 4). Eine besondere Rolle spielt dabei die Berichterstattung über die Einsätze im Ausland. Diese prägt in der deutschen Bevölkerung die Wahrnehmung der Bundeswehr in besonderem Maße, weswegen der Informationsbedarf darüber von besonderer Relevanz ist (BMVg o. D. d). Gerade in Bezug auf die Auslandseinsätze lässt sich jedoch festhalten, dass eine Mehrheit der Bürgerinnen und Bürger diese zwar befürwortet, das

Informationsniveau jedoch gering ist und die Mehrheit sich zudem nicht ausreichend über die Auslandseinsätze informiert sieht (Steinbrecher/Graf/Biehl/Irrgang 2021, 11). Dadurch bietet sich eine Angriffsfläche für Desinformation.

Um diese Angriffsfläche zu mindern, ist der Aufbau von systemischer und individueller Resilienz notwendig. Dafür ist sowohl ein Diskurs in der Gesellschaft als auch in der Wissenschaft notwendig, wo die Eindämmung von Desinformation langfristig politisch anzusiedeln ist und welche Rolle die Bundeswehr bei der systemischen Resilienzbildung spielt. Aufbau der systemischen Resilienz liegt zwar im Interesse der Bundeswehr und der Bundeswehrangehörigen, aber die Verantwortung dafür ist zunächst bei Politik und Gesellschaft verortet (Janke 2021, 13).

Auslandseinsätze: Desinformation erkennen, begegnen und verhindern

Die Akteure, die Desinformationen in Auslandseinsätzen bekämpfen, sind vielfältig. Seitens der Bundeswehr sind es schwerpunktmäßig das Einsatzführungskommando (Stabsreferentin, -referent vor Ort und Presse- und Informationszentrum (PIZ) in Deutschland), das Kommando CIR und das Zentrum Operative Kommunikation der Bundeswehr (ZOpKomBw) als dem Kommando CIR nachgeordnete Dienststelle. Darüber hinaus ist – je nach Relevanz – das BMVg involviert. (Interview 3; Interview 5). Neben Pressestabsoffizieren vor Ort, die direkt Informationen nach Deutschland weiterleiten, werden mithilfe des sogenannten *reach-back*-Verfahrens auch Aufgaben, die nicht zwingend im Einsatzland durchgeführt werden müssen, in Deutschland erledigt. Beispiele hierfür sind die Auswertung von Aufklärungsergebnissen oder die Erstellung von Kartenmaterial (BMVg o. D. c; Interview 5). Hinzukommen, je nach Prozess und Zuständigkeitsketten sowie der Verbreitungswirkung, andere Bundesministerien und Akteure in Deutschland (aber auch Verteidigungsausschuss im Bundestag) und Partner Deutschlands (NATO, EU) (Interview 1; Interview 4; Interview 5; BMVg 2020).

In Auslandseinsätzen gilt es, das Informationsumfeld vor Ort zu erfassen und zu analysieren. Das Informationsumfeld ist der Anteil des CIR, in den Informationen zur Meinungsbildung aufgenommen, verarbeitet und weitergegeben werden. In Interview 5 wurde ausgeführt, wie je nach Einsatz zudem unterschiedliche Ziele verfolgt und dementsprechend unterschiedliche Fähigkeiten erforderlich sein. So können u. a. die Fähigkeiten des Zentrums operative Kommunikation der Bundeswehr benötigt werden. Beispiele für diese Aufgaben sind: Informationsbereitstellung für die Bevölkerung im Einsatzgebiet, beispielsweise durch Medienprodukte (stromunabhängige Radios) oder geplante und zielgerichtete Gespräche mit der Bevölkerung vor Ort (BMVg o. D. c; BMVg o. D. f; Interview 2; Interview 4; Interview 5).

Alle Auslandseinsätze finden im Rahmen von multinationalen Einsätzen der EU, NATO oder der Vereinten Nationen statt. Bei der Begegnung mit Desinformationen gibt es multinationale Ansätze. So beispielsweise von NATO-Staaten, wie die Errichtung des NATO-akkreditierten Kompetenzzentrums Strategic Communications Centre of Excellence (NATO StratCom CoE) mit Sitz in Riga. Im NATO StratCom CoE forschen und entwickeln die Mitgliedsstaaten gemeinsame Kommunikationsansätze. Eines der Ziele ist die Aufklärung und Information der Bevölkerung (EU- und NATO-Mitgliedsstaaten), um Desinformationen die jeweiligen Fakten entgegenzusetzen (Interview 1).

Es wurde aufgezeigt, dass bei der Bekämpfung von Desinformationen unterschiedliche Fähigkeiten benötigt werden. Daraus folgt, dass es keinen Automatismus gibt, wie die Bekämpfung bei Desinformation vonstattengeht. Es wird situativ entschieden (Interview 4; Interview 5). Um dies zu verdeutlichen, untersuchen wir im Folgenden anhand der anerkannten Mission der Bundeswehr in Litauen, wie Desinformation konkret aussehen und wie reagiert werden kann.

Fallbeispiel: Die NATO-Mission in Litauen

Bei der anerkannten Mission in Litauen gab es bisher verschiedene Fälle von Desinformation. So lässt sich in Bezug auf deren Auftreten zunächst festhalten, dass die litauische Regierung ein vitales Interesse daran hat, Desinformation über die eFP in ihrem Land effektiv zu bekämpfen. Sie ist entsprechend sensibilisiert und entschlossen, schnell gegen diese vorzugehen. Dementsprechend gibt es in Fällen von Desinformation eine enge Zusammenarbeit zwischen Deutschland und Litauen, jedoch konnten und kann deren Verbreitung nicht vollkommen verhindert werden (Interview 3; Interview 4; Interview 5).

Desinformation in Bezug auf die Bundeswehr traten insbesondere zu Beginn der Mission auf (Interview 3). Das NATO StratCom CoE stuft Litauen als „mittelschweres Ziel" für Desinformation ein. Als Urheber werden in der Regel Kreml- und kremlnahe Akteure vermutet (Rodríguez 2020, 139 ff.; 150). Aus russischer Perspektive erhöhen die multinationalen *Battlegroups* im Baltikum und in Polen die Spannungen aufgrund der Nähe zur russischen Exklave Kaliningrad sowie zu Belarus, einem verbündeten Staat Russlands; die Stationierung der Truppen wird daher als Aggression wahrgenommen (Rodríguez 2020, 150 f.). Inhaltlich zielt die Desinformation darauf ab, die deutschen Streitkräfte als Rahmennation und die NATO-Verbündeten negativ darzustellen und die eFP zu unterminieren. So soll sowohl in der litauischen (im größeren Rahmen ebenso baltischen) Bevölkerung, der russischsprachigen Minderheit in den baltischen Staaten, als auch in der deutschen Bevölkerung Zweifel an der Legitimität der Truppenpräsenz gestreut werden (Althuis/Haiden 2018, 50 f.). Aus europäischer Sicht bedient sich der Kreml Desinformation, um zu verwirren und zu spalten (Althuis/Haiden 2018, 50 f.; Rodríguez 2020, 139).

In der folgenden Tabelle werden zwei Fälle von Desinformation im Rahmen der eFP dargestellt. Sie stehen exemplarisch für die Herausforderungen resultierend aus Desinformation, denen die Bundeswehr im Ausland ausgesetzt ist.

Tabelle 2: Übersicht Fallbeispiele Desinformationen in Litauen

	Deutsche Soldaten vergewaltigen minderjährige Litauerin vor Kinderheim in Jonova.	**Deutsche Soldaten schänden jüdischen Friedhof in Kaunas mit deutschem Panzer.**
Datum	14.02.2017	25.09.2019
Art	E-Mail an litauischen Parlamentspräsidenten und Medien	Artikel inklusive Fotomontage
Ablauf	Kleinere litauische Medien griffen Fall auf, auch in Deutschland wurde darüber berichtet	Gepostet auf litauischem Blog, Starten von Petitionen (Englisch & Litauisch), dadurch schnelle Verbreitung
Herkunft	Nicht identifizierbar	Nicht identifizierbar
Wahrheitsgehalt	wirkt glaubhaft aufgrund detaillierter Beschreibung Ort des Geschehens, liegt in der Nähe des Stationierungsorts der deutschen Soldaten, ein Kinderheim gibt es dort nicht.	Battle-Group-Panzer ist an dem Tag durch die Ortschaft gefahren, aber grüne Blätter auf Bild obwohl Ende September und keine Reifenspuren vorhanden.

Eigene Darstellung

Am 14. Februar 2017 wurden E-Mails an den litauischen Parlamentspräsidenten, weitere Abgeordnete und die lokale Polizei geschickt, in denen behauptet wurde, deutsche Soldaten hätten eine minderjährige Litauerin vor einem Kinderheim vergewaltigt (Bundesregierung 2017, 3). Kleinere, vorwiegend lokale litauische Medien verbreiteten die Nachricht (Gebauer 2017). Die Bundeswehr wurde am 15. Februar 2017 informiert (Bundesregierung 2017, 3).

Die litauischen Behörden ermittelten und identifizierten diese Meldung schnell als Desinformation, da zum einen das Kinderheim nicht existierte und zum anderen deutsche Soldaten am genannten Tag nicht in der Ortschaft waren (Gebauer 2017). Schnell veröffentlichte die litauische Regierung diese Fakten, wodurch die weitere Verbreitung bzw. Glaubhaftigkeit der Desinformation unterbunden wurde (Interview 5). In Deutschland wurde der Vorfall von vielen großen Medien aufgegriffen, unter anderem von der *Frankfurter Allgemeinen Zeitung*, dem *Focus*, der *Süddeutschen Zeitung*, dem *Stern* und der *Welt*. *Der Spiegel* veröffentlichte den „Versuch" der Desinformation als erstes großes, deutsches Nachrichtenportal und behauptete, dass die NATO Russland als Urheber verantwortlich mache. Dies musste später revidiert werden, da es ein Verdacht blieb (Gebauer 2017). Seitens der Bundesregierung ist dieser Fall von Desinformation als eine „professionell konzertierte Aktion" bewertet worden (Bundesregierung 2017, 2). Ziel sei die Diffamierung deutscher Soldaten und der eFP (Bundesregierung 2017, 2). Diese Meldung wurde in Deutschland folglich zwar weit verbreitet, aber zugleich als (fehlgeschlagener) Versuch von Desinformation eingeordnet, weswegen sie ihr Ziel weder in Litauen noch in Deutschland erreichte.

Im September 2019 veröffentlichte der litauische Blog lzbltkauno.wordpress.com einen Artikel über die Schändung eines jüdischen Friedhofs in der litauischen Stadt Kaunas durch einen deutschen Panzer (Rodríguez 2020, 150 f.). Der Artikel enthielt eine Fotomontage eines Panzers mit einer deutschen Flagge, der über den Friedhof fuhr. Verantwortlich hierfür wurden die unweit von Kaunas stationierten deutschen Streitkräfte gemacht (Rodríguez 2020, 150 f.). Sechs Medien verbreiteten diese Information in

litauischer, englischer und russischer Sprache. Auf der weltweit größten Kampagnenplattform chance.org erschien sogar eine Petition, welche jedoch später wieder gelöscht wurde (Rodríguez 2020, 150 f.). Das litauische Militär bezeichnete das Vorgehen als eine Desinformationskampagne, die gezielt und koordiniert erfolgte (Hoffmann/Welscher 2019). Primärer Adressat der Desinformation scheint somit die litauische Bevölkerung zu sein, um die stationierten NATO-Truppen in diesem Personenkreis zu delegitimieren (Rodríguez 2020, 150 f.). Die Zustimmung zur NATO-Mitgliedschaft des eigenen Landes ist in Litauen mit 77 Prozent hoch und wird als elementar für die eigene Sicherheit betrachtet (Kolb/Matthias, 2020). Dass die Desinformation in sechs unterschiedlichen, wenn auch eher kleinen litauischen Medien als „wahre Meldung" verbreitet wurde, verweist auf ihre vorhandenen Erfolgschancen.

Insgesamt lässt sich eine große Resilienz gegenüber Desinformation über die eFP seitens der Bevölkerung in Litauen feststellen, die sich auch durch die hohen Zustimmungswerte zur NATO-Mitgliedschaft erklären lässt. Ebenso reagierte die Regierung schnell und deutlich. Dies führte auch dazu, dass die Desinformationen entweder nicht in Deutschland ankamen oder bereits bei der diesbezüglichen Berichterstattung die korrekten Fakten vorlagen. Lediglich einige der Bundeswehr nahestehende Medien wie der Reservistenverband griffen dieses „Ereignis" auf (Hoffmann/Welscher 2019).

Schlussfolgerungen

Dieser Beitrag verfolgt zwei Zielsetzungen. Zunächst sollten Implikationen aus der diffusen Begriffsdebatte zu Fake News für die Bundeswehr abgeleitet werden. Dazu legte der Beitrag einen Grundstein für weitere Untersuchungen und zeigte dabei auf, dass der Begriff Fake News für die Verwendung im Kontext der Bundeswehr wenig hilfreich ist. Stattdessen stehen im sicherheitspolitischen Diskurs Propaganda und Propagandaarten mit speziellem Fokus auf Desinformation im Vordergrund. Bei der Erkennung, Begegnung und Bekämpfung von Desinformation durch das BMVg und die Bundeswehr werden je nach Art und Intensität unterschiedliche Fähigkeiten benötigt; dementsprechend sind unterschiedliche Bereiche und Dienststellen involviert. Daraus folgt, dass es keinen festen Automatismus und definierten Prozess gibt. Es wird situativ gehandelt und entschieden, die Zuständigkeiten und Ablaufketten variieren. Auch gibt es bei der konkreten Bekämpfung von Desinformation in Einzelfällen kein dafür spezifisch zuständiges Personal.

Am Beispiel der anerkannten Mission in Litauen, bei der die Bundeswehr von Desinformation betroffen ist, wurde beispielhaft gezeigt, welche Arten von Desinformation auftreten können. Die Anzahl von Nachrichten, die in Deutschland öffentlich wahrgenommen und diskutiert werden, sind bisher gering. Bislang konnten Desinformationen durch eine gute Überprüfung schnell belastbar widerlegt werden. Es bleibt abzuwarten, ob Ausmaß und Intensität versuchter Desinformation zunehmen, beispielsweise durch (weitere) Professionalisierung der Urheber, und wie die neu geschaffenen Strukturen und Maßnahmen sich auswirken.

Zusätzlich empfiehlt es sich, weitere – vorzugsweise andere westliche – Armeen zu betrachten, um einen Vergleich der Begriffsdefinitionen zu ziehen und Mechanismen für den Umgang mit Propagandaarten zu untersuchen. Ein besonderes Interesse gilt dabei den Strukturen der

NATO und der Kooperation mit den Mitgliedsstaaten des Bündnisses, insbesondere da die Bekämpfung von Propagandaarten in den NATO-Partnerländern variiert und mit dem NATO StratCom CoE bereits erfolgt.

189 Einen sehr guten Überblick über den aktuellen Forschungsstand zu Fake News, einen theoretischen Rahmen und damit verbunden eine Forschungsagenda, zeigen Egelhofer und Lecheler (2019) auf.

190 2016 beschlossen die Staats- und Regierungschefs der NATO-Staaten bei dem Gipfeltreffen in Warschau die Stationierung vier multinationaler Gefechtsverbände (*Battlegroups*) in den drei baltischen Staaten und Polen als Beistandsinitiative. Auslöser dafür war die völkerrechtswidrige russische Annexion der Krim und die anhaltende Destabilisierung der Ukraine von Seiten Russlands (BMVg o. D. a). Die Operation stellt daher einen Ausdruck der Stärke und Bündnissolidarität mit den östlichen NATO-Staaten dar und gilt der Sicherung der Ostflanke der Allianz. (BMVg o.D.a; BMVg o. D. e). Ab 2017 wurden in Polen und den baltischen Staaten jeweils eine multinationale *Battlegroup* stationiert. Deutschland führt als Rahmennation die *Battlegroup* in Litauen. Für die Bundeswehr stellt die eFP eine sogenannte anerkannte Mission dar, d. h. es ist kein Einsatz bewaffneter Streitkräfte, sondern eine Auslandsverwendung unter einsatzähnlichen Rahmenbedingungen. Folglich muss der Bundestag die Stationierung deutscher Soldaten in Litauen nicht mandatieren. (BMVg o. D. a; BMVg o. D. e). Für weitere Details zur Vorbereitung, Durchführung und Auswertung von Experteninterviews verweisen wir auf Kaiser (2014) oder Gläser und Laudel (2010).

191 Bei unseren Interviewpartnern handelte es sich ausschließlich um Männer; daher verzichten wir an dieser Stelle auf das Gendern.

192 Für weitere Details zur Vorbereitung, Durchführung und Auswertung von Experteninterviews verweisen wir auf Kaiser (2014) oder Gläser und Laudel (2010).

193 Neben den ethischen Aspekten zum Experteninterview (siehe beispielsweise Kaiser 2014, 49) wurden die Personen aufgrund des Themas und auf ihren Wunsch hin anonymisiert. Eine Liste wurde aber während des Publikationsverfahrens mit vollständigen Namen eingereicht.

194 Unter dem Begriff Akteur fassen wir Personen und Institutionen zusammen

Literaturverzeichnis

A Allcott, Hunt & Gentzkow, Matthew. (2017). Social Media and Fake News in the 2016 Election. *Journal of Economic Perspectives, 31(2),* Pages 211–236.

Allen, Jennifer & Howland, Baird, Mobius, Marine, Rothschild, David & Watts, Duncan. (2020). Evaluating the fake news problem at the scale of the information ecosystem. *Science Advances, 6*, 1–6.

Althuis, Jente & Haiden, Leonie. (2018). Fake News: A Roadmap. King's Centre for Strategic Communications & NATO Strategic Communications Centre of Excellence.

Asanov, Temir. (2019, 17. März). Fake News in Modern News Media: Disinformation, Misinformation and Malinformation, https://medium.com/@tasanoff/fake-news-in-modern-news-media-disinformation-misinformation-and-malinformation-e4fdfa2ab571 (letzter Zugriff: 13.02.2021).

B Bogner, Alexander, Littig, Beate & Menz, Wolfgang. (2009). Introduction: Expert Interviews – An Introduction to a New Methodological Debate, in: Bogner, Alexander, Littig, Beate & Menz, Wolfgang (Hrsg.). *Interviewing Experts* (1. Auflage, 1–13). London: Palgrave Macmillan.

Bogner, Alexander, Littig, Beate & Menz, Wolfgang. (2014). Interviews mit Experten. Eine praxisorientierte Einführung (1. Auflage). Wiesbaden: Springer VS.

Bradshaw, Samantha & Howard, Philip N. (2018). Challenging Truth and Trust: A Global Inventory of Organized Social Media Manipulation, https://comprop.oii.ox.ac.uk/wp-content/uploads/sites/93/2018/07/ct2018.pdf (letzter Zugriff: 13.02.2021).

Bundesministerium der Verteidigung. (o. D. a) Anerkannte Missionen der Bundeswehr, https://www.bundeswehr.de/de/einsaetze-bundeswehr/anerkannte-missionen (letzter Zugriff: 13.02.2021).

Bundesministerium der Verteidigung. (o. D. b) Auftrag des Organisationsbereichs CIR, https://www.bundeswehr.de/de/organisation/cyber-und-informationsraum/auftrag (letzter Zugriff: 13.02.2021).

Bundesministerium der Verteidigung. (o. D. c). Der Organisationsbereich Cyber- und Informationsraum im Einsatz, https://www.bundeswehr.de/de/organisation/cyber-und-informationsraum/cir-im-einsatz (letzter Zugriff: 13.02.2021).

Bundesministerium der Verteidigung. (o. D. d). Informationsarbeit / Pressearbeit Bundeswehr, https://www.bundeswehr.de/de/organisation/streitkraeftebasis/auftrag/pressearbeit-in-der-bundeswehr (letzter Zugriff: 13.02.2021).

Bundesministerium der Verteidigung. (o. D. e). Litauen – Enhanced Forward Presence, https://www.bundeswehr.de/de/einsaetze-bundeswehr/anerkannte-missionen/efp-enhanced-forward-presence (letzter Zugriff: 13.02.2021).

Bundesministerium der Verteidigung. (o. D. f). Organisation des Organisationsbereichs CIR, https://www.bundeswehr.de/de/organisation/cyber-und-informationsraum/kommando-und-organisation-cir (letzter Zugriff: 13.02.2021).

Bundesministerium der Verteidigung. (o. D. g). Social Media-Guidelines, https://www.bundeswehr.de/resource/blob/153030/7713bef2cf60a5198b74abfe0b8b0444/20191122-download-social-media-guidelines-data.pdf (letzter Zugriff: 13.02.2021).

Bundesministerium der Verteidigung. (o. D. f) Zentrum Informationsarbeit Bundeswehr, https://www.bundeswehr.de/de/organisation/streitkraeftebasis/organisation/streitkraefteamt/zentrum-informationsarbeit-bundeswehr (letzter Zugriff: 13.02.2021).

Bundesministerium der Verteidigung. (2020, 09. Dezember). BMVg startet „Kompetenzzentrum Krisenfrüherkennung", https://www.bmvg.de/de/presse/bmvg-startet-kompetenzzentrum-krisenfrueherkennung-4916304 (letzter Zugriff: 13.02.2021).

Busch, Carolin & Düe, Nadine. (2017). Informationskriege: Eine Herausforderung für die Bundeswehr, Arbeitspapier Sicherheitspolitik, Nr. 24/2017 Bundesakademie für Sicherheitspolitik, https://www.baks.bund.de/de/arbeitspapiere/2017/informationskriege-eine-herausforderung-fuer-die-bundeswehr (letzter Zugriff: 13.02.2021).

D Die Bundesregierung. (2016). Weißbuch zur Sicherheitspolitik und zur Zukunft der Bundeswehr. https://www.bundesregierung.de/resource/blob/975292/736102/64781348c12e4a80948ab1bdf25cf057/weissbuch-zur-sicherheitspolitik-2016-download-data.pdf (letzter Zugriff: 13.02.2021).

Deutscher Bundestag. (2017). Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Andrej Hunko, Sevim Dağdelen, Annette Groth, weiterer Abgeordneter und der Fraktion DIE LINKE. – Drucksache 18/11678 –, http://dipbt.bundestag.de/doc/btd/18/119/1811987.pdf (letzter Zugriff: 13.02.2021).

Deutscher Bundestag. (2018). Antwort der Bundesregierung auf die Kleine Anfrage des Abgeordneten Dr. Anton Friesen und der Fraktion der AfD.

Drucksache 19/4796 –, http://dipbt.bundestag.de/dip21/btd/19/047/1904796.pdf (letzter Zugriff: 13.02.2021).

Drews, Dirk. (2006). Die Psychologische Kampfführung/Psychologische Verteidigung der Bundeswehr – eine erziehungswissenschaftliche und publizistikwissenschaftliche Untersuchung, https://www.fachportal-paedagogik.de/literatur/vollanzeige.html?FId=847716#vollanzeige (letzter Zugriff: 13.02.2021).

E Egelhofer, Jana Laura & Lecheler, Sophie. (2019). Fake news as a two-dimensional phenomenon: a framework and research agenda. *Annals of the International Communication Association, 43(2)*, 97–116.

G Gebauer, Matthias. (2017, 16. Februar). Nato vermutet Russland hinter Fake-News-Kampagne gegen Bundeswehr, in: Spiegel, https://www.spiegel.de/politik/ausland/bundeswehr-fake-news-attacke-gegen-deutsche-soldaten-in-litauen-a-1134925.html (letzter Zugriff: 13.02.2021).

Gelfert, Axel. (2018). Fake News: A Definition. *Informal Logic, 38(1)*, 84–117.

Gerring, John. (2006). Case Study Research Principles and Practices. Cambridge: Cambridge University Press.

Gläser, Jochen & Laudel, Grit. (2010). Experteninterviews und qualitative Inhaltsanalyse (4. Auflage). Wiesbaden: VS Verlag.

Guadagno, Rosanna E. & Guttieri, Karen. (2019). Fake News and Information Warfare: An Examination of the Political and Psychological Processes From the Digital Sphere to the Real World, in: Chiluwa, Innocent E. & Samoilenko, Sergei A. (Hrsg.) *Handbook of Research on Deception, Fake News, and Misinformation Online* (1. Auflage, 167–191). Hershey Pennsylvania: IGI Global: International Academic Publisher.

H Habgood-Coote, Joshua. (2018). Stop talking about fake news!. *Inquiry, 62(9–10),* 1033–1065.

Hajduk, Julian & Zowislo-Grünewald, Natascha. (2020). „Fake News“: neue Bedrohung oder alter Hut? – Grundlagen für ein Strategisches Diskursmanagement, in: Hohlfeld, Ralf, Harnischmacher, Michael, Heinke Elfi, Lehner Lea Sophia, Sengl, Michael (Hrsg.). *Fake News und Desinformation. Herausforderungen für die vernetzte Gesellschaft und die empirische Forschung* (1. Auflage, 297–311). Baden-Baden: Nomos.

Hemicker, Lorenz. (2017, 16. Februar). Attacke auf die Bundeswehr in Litauen, in: Frankfurter Allgemeine Zeitung, https://www.faz.net/aktuell/politik/sicherheitskonferenz/bundeswehr-in-litauen-wird-opfer-von-fake-news-attacke-14882067.html (letzter Zugriff: 13.02.2021).

Hindman, Matthew & Barash, Vlad. (2018). Disinformation, ‘Fake News’ and Influence Campaigns on Twitter, Knight Foundation, https://kf-site-production.s3.amazonaws.com/media_elements/files/000/000/238/original/KF-DisinformationReport-final2.pdf (letzter Zugriff: 13.02.2021).

Hoffmann, Carsten & Welscher, Alexander. (2019, 10. Oktober). Schlachtfeld Internet: Bundeswehr wehrt in Litauen Desinformation ab, in: Deutscher BundeswehrVerband, https://www.dbwv.de/aktuelle-themen/newsbeitrag/schlachtfeld-internet-bundeswehr-wehrt-in-litauen-desinformation-ab (letzter Zugriff: 13.02.2021).

Institut für Politische Wissenschaft, Rheinisch-Westfälischen Technischen Hochschule (RWTH) Aachen. (o. D.). Propaganda Awareness. http://www.ipw.rwth-aachen.de/wp/propaganda-awareness/ (letzter Zugriff: 13.02.2021).

Interview 1. (2020, 18. Dezember). Gruppeninterview, Bundesministerium der Verteidigung.

Interview 2. (2020, 4. Dezember). Einzelinterview, Kommando Cyber- und Informationsraum.

Interview 3. (2020, 18. November). Einzelinterview, Zentrum Operative Kommunikation der Bundeswehr.

Interview 4. (2020, 2. Dezember). Einzelinterview, Cyber- und Informationsraum.

Interview 5. (2020, 3. Dezember). Einzelinterview, Einsatzführungskommando, Presse- und Informationszentrum der Bundeswehr.

J Jack, Caroline. (2017). Lexicon of Lies: Terms for Problematic Information. Data & Society Research Institute, https://datasociety.net/library/lexicon-of-lies/ (letzter Zugriff: 13.02.2021).

Janke, Reinhold. (2021). Einsatzfähig durch Widerstandskraft. Resilienz als materielle und immaterielle Ressource. *Zeitschrift für Innere Führung*, 2(21), 8–13.

Jones, Marc Owen. (2019). Propaganda, Fake News, and Fake Trends: The Weaponization of Twitter Bots in the Gulf Crisis. *International Journal of Communication, 13(2019),* 1389–1415.

Jowett, Garth S. & O'Donnell, Victoria. (2012). Propaganda and persuasion (5. Ausgabe). Thousand Oaks: SAGE Publications.

K Kaiser, Robert. (2014). Qualitative Experteninterviews. Konzeptionelle Grundlagen und praktische Durchführung. Wiesbaden: Springer VS.

Kolb, Matthias. (2020, 10. Februar). Umfrage: Die USA sollen es für die NATO richten, https://www.sueddeutsche.de/politik/nato-pew-umfrage-usa-russland-1.4790618 (letzter Zugriff: 13.02.2021).

L Leinhos, Ludwig. (2020). Cyber Defence in Germany: Challenges and the Way Forward for the Bundeswehr. *The Quarterly Journal, 19(1),* 9–19.

Lieberenz, Constanze. (2019, 11. November). Kommando CIR goes Wissenschaft, https://www.unibw.de/home/news/kommando-cir-goes-wissenschaft (letzter Zugriff: 13.02.2021).

M Möllers, Heiner & Jacobs, Jörg. (2019). Bundeswehr und Medien. Ereignisse – Handlungsmuster – Mechanismen in jüngster Geschichte und heute. Baden-Baden: Nomos.

Molina, Maria D., Sundar, S. Shyam, Le, Thai & Lee, Dongwon. (2019). „Fake News" Is Not Simply False Information: A Concept Explication and Taxonomy of Online Content. *American Behavioral Scientist, 65(2)*, 180–212.

N Nemr, Christina & Gangware, William. (2019). Weapons of Mass Distraction: Foreign State-Sponsored Disinformation in the Digital Age. Park Advisors, https://www.state.gov/wp-content/uploads/2019/05/Weapons-of-Mass-Distraction-Foreign-State-Sponsored-Disinformation-in-the-Digital-Age.pdf (letzter Zugriff: 13.02.2021).

news aktuell GmbH. (2020, 25. September). Führungswechsel beim Cyber- und Informationsraum der Bundeswehr, https://www.presseportal.de/pm/129406/4717496 (letzter Zugriff: 13.02.2021).

R Redaktion der Bundeswehr (2021, 27. Februar). Hybride Bedrohung: Fake News und Desinformation, https://www.bmvg.de/de/aktuelles/fake-news-und-desinformation-186254 (letzter Zugriff: 28.02.2021).

Rodríguez, Belén Carrasco. (2020). Information Laundering in the Nordic Baltic Region. NATO Strategic Communications Centre of Excellence.

S Sample, Char, Justice, Connie & Darraj, Emily. (2019). A Model for Evaluating Fake News, https://scholarworks.iupui.edu/bitstream/handle/1805/24572/Sample2019AModel.pdf?sequence=1&isAllowed=y (letzter Zugriff: 13.02.2021).

Sarmina, Anna. (2020). Die Macht der Propaganda im Ukrainekonflikt in: Hohlfeld, Ralf, Harnischmacher, Michael, Heinke Elfi, Lehner Lea Sophia, Sengl, Michael (Hrsg.). *Fake News und Desinformation. Herausforderungen für die vernetzte Gesellschaft und die empirische Forschung* (1. Auflage, 117–134). Baden-Baden: Nomos.

Seawright Jason & Gerring John. (2008). Case Selection Techniques in Case Study Research: A Menu of Qualitative and Quantitative Options. *Political Research Quarterly, 61(2),* 294–308.

Steinbrecher, Markus, Graf, Timo, Biehl, Heiko & Irrgang, Christina. (2021). Sicherheits- und verteidigungspolitisches Meinungsbild in der Bundesrepublik Deutschland, Zentrum für Militärgeschichte und Sozialwissenschaften der Bundeswehr, https://www.bundeswehr.de/resource/blob/5036360/dd413dbbd10610484755c6f4fbfbaa93/download-fober-128-data.pdf (letzter Zugriff: 13.02.2021).

T Tandoc Jr. Edson C., Lim, Zheng Wei & Ling, Richard. (2017). Defining „Fake News". *Digital Journalism, 6(2)*, 137–153.

Turcilo, Lejla & Obrenovic, Mladen. (2020). Fehlinformationen, Desinformationen, Malinformationen: Ursachen, Entwicklungen und ihr Einfluss auf die Demokratie. Heinrich-Böll-Stiftung, https://www.boell.de/sites/default/files/2020-08/200825_E-Paper3_DE.pdf (letzter Zugriff: 13.02.2021).

V Vamanu, Iulian. (2019). Fake News and Propaganda: A Critical Discourse Research Perspective. *Open Information Science*, 3, 197–208.

W Wagner, María Celeste & Boczkowski, Pablo J. (2019). The Reception of Fake News: The Interpretations and Practices That Shape the Consumption of Perceived Misinformation. *Digital Journalism, 7(7)*, 870–885.

Wardle, Claire & Derakhshan, Hossein. (2017). Information Disorder: Toward an interdisciplinary framework for research and policy making, Council of Europe, https://rm.coe.int/information-disorder-toward-an-interdisciplinary-framework-for-researc/168076277c (letzter Zugriff: 13.02.2021).

Wiegold, Thomas. (2019). Zwei Jahre (deutsch geführte) NATO-Battlegroup in Litauen. Auch auf Facebook. Blog Augengeradeaus. https://augengeradeaus.net/2019/02/zwei-jahre-deutsch-gefuehrte-nato-battlegroup-in-litauen-auch-auf-facebook/ (letzter Zugriff: 13.02.2021).

Z Zhou, Xinyi, Jain, Atishay, Phoha, Vir V. & Zafarani, Reza. (2020). Fake News Early Detection: A Theory-driven Model. *Digital Threats: Research and Practice, 1(2),* 1–25.

Zimmermann, Fabian & Kohring, Matthias. Aktuelle Desinformation – Definition und Einordnung einer gesellschaftlichen Herausforderung in: Hohlfeld, Ralf, Harnischmacher, Michael, Heinke Elfi, Lehner Lea Sophia, Sengl, Michael (Hrsg.). *Fake News und Desinformation. Herausforderungen für die vernetzte Gesellschaft und die empirische Forschung* (1. Auflage, 21–42). Baden-Baden: Nomos.

Counter Influence Campaigns

as Integral Part of Policy Planning for Resilience

Holger Knappenschneider und Johannes Feige

08 Der Einsatz von Online-Fähigkeiten durch feindliche Akteurinnen und Akteure, um Narrative zu kontrollieren und die Entscheidungsfindung sowie das Verhalten anderer zu beeinflussen, ist zu einer großen Bedrohung für liberale Demokratien geworden. Die Verteidigung gegen diese Angriffshandlungen ist das Ziel von strategischen Kommunikationskampagnen (Counter-Influence-Kampagnen). Sie ist entscheidend für die dauerhafte Stärke des politischen Systems in Deutschland und in Europa. Die Frage, ob diese Art von Angriffen bekämpft werden kann, steht nicht zur Diskussion, sondern nur das Wie.

Einleitung

Der Einsatz einer ganzen Reihe von Onlinefähigkeiten durch feindliche Akteure, um Narrative zu kontrollieren und die Entscheidungsfindung und das Verhalten anderer Akteure zu beeinflussen, ist zu einer großen Bedrohung für liberale Demokratien geworden. Die Bedrohung wird vervielfacht durch die Verbreitung von Technologien, die zunehmende Nutzung sozialer Medien und des Internets als Instrumente der Desinformation sowie die sich ändernden Gewohnheiten der Menschen bei der Beschaffung und Nutzung dieser Informationen. Da Cyberkriminelle und Verbreiter von Falschinformationen immer geschicktere Strategien entwickeln und ihre Methoden und Ausrüstung professionalisieren, sind die westlichen Demokratien nicht mehr in der Lage, diese Bedrohungen zu erfassen und ihnen wirksam zu begegnen.

Aufgrund der relativen Leichtigkeit, Effektivität und Anonymität dieser feindlichen Beeinflussungsoperationen hat ihr Einsatz in den letzten Jahren dramatisch zugenommen und ist zu einer neuen Form der Informationskriegsführung geworden.[195] Während ihr Einsatz oft einem kinetischen Konflikt vorausgeht, ist die Informationskriegsführung auch ein Selbstzweck, wenn ihr primäres Ziel darin besteht, den öffentlichen Informationsraum eines Ziels zu dominieren. Dies hat schwerwiegende Folgen für das Funktionieren und die Stabilität demokratischer Systeme, denn deren Qualität und Legitimität erwachsen aus der Fähigkeit der Wählerinnen und Wähler, informierte Entscheidungen zu treffen, die wiederum auf sachlich korrekten Überzeugungen über die politischen Verhältnisse und das politische System selbst beruhen.[196]

Deutschland ist nicht immun gegen diese zersetzenden Effekte und wurde von feindlichen Akteuren für Angriffe im Onlinebereich ausgewählt. Angesichts der bevorstehenden Bundestagswahl 2021 muss Deutschland seine Abwehrmaßnahmen gegen gezielte Desinformationskampagnen verstärken. Die Definition der Bedrohung, die Identifizierung bösartiger Narrative und die Umsetzung einer effektiven Gegenbeeinflussungskampagne, die kritisches Denken und die Nutzung von faktengeprüften

Informationen fördern soll, sind dringende Prioritäten. Nur dadurch kann verhindert werden, dass das gesellschaftspolitische Umfeld Deutschlands von innen heraus untergraben wird.

Die Anatomie der Desinformation

Die feindlichen Beeinflussungsoperationen, die hinter Desinformation stehen – Onlineveröffentlichungen von absichtlich falschen Aussagen, die zu strategischen Zwecken produziert und zur sozialen Beeinflussung verbreitet werden[197] – beziehen ihre Wirksamkeit aus den Narrativen, die sie in Diskurse einbringen. Diese bilden die Linse, durch die Einzelne die Informationen interpretieren und damit interagieren, und bestimmen die Art der moralischen Lehren und Schlussfolgerungen, die daraus gezogen werden. Feindliche Beeinflussungsoperationen zielen darauf ab, die „Herzen und Köpfe" des Zielpublikums zu gewinnen, es zur Matrix des Aggressors zu bekehren und mit dieser manipulierten Wahrnehmung die Welt und die Ereignisse, die sich in ihr abspielen, zu beurteilen.

Der Kern dieser Operationen ist die Ausnutzung von Emotionen. Indem man emotionale – im Gegensatz zu rationalen – Reaktionen hervorruft, werden Fakten zunehmend aus den Diskursen entfernt. Narrative, die darauf abzielen, zu übertreiben, Vorurteile zu schüren und vorgefertigte Ideen zu bestätigen, untergraben daher nicht nur die Fähigkeit der Zivilgesellschaft zu einer nüchternen Debatte, sondern höhlen gleichzeitig „die Normen und Institutionen aus, die interne Konflikte friedlich lösen"[198] können. Mit dem dauerhaft veränderten Interpretationsrahmen hat der Staat die Deutungshoheit teilweise an den Feind verloren und wird es immer schwerer haben, die für seine eigene Sicherheit relevanten manipulierten Diskurse einzudämmen.

Da Desinformationskampagnen weniger Ressourcen benötigen, um effektiv zu sein, als der Einsatz von militärischer Hardware, haben sie eine übergroße Wirkung im Verhältnis zu den eigentlichen Kosten aber auch bezüglich der zivilgesellschaftlichen Störungen, die sie zu produzieren in der Lage sind. Denn sie verwischen die Grenze zwischen zivilen und militärischen Zielen unter Zuhilfenahme des Internets und hier ins-

besondere der sozialen Medien. Letztere sind der wichtigste Kanal, um Desinformation einem breiten Publikum zugänglich zu machen. Nachdem sie mehrere Ebenen der Desinformationsverbreitung durchlaufen haben – von geschlossenen und halbgeschlossenen Räumen (Chat-Apps wie Telegram und Messaging-Boards wie 4chan) hin zu voreingenommenen offenen Räumen (Verschwörungscommunities, Facebook-Gruppen und YouTube-Kanäle) – finden wir sie schließlich in weithin zugänglichen Mainstreamräumen der sozialen Medien wie Twitter, Facebook-Seiten und anderen sozialen Plattformen wieder.

Der Erfolg dieser Art Kampagnen liegt darin, dass das Publikum selbst zum aktiven Teilnehmer oder zur aktiven Teilnehmerin in der (Des-) Informationsverarbeitung wird, anstatt nur passiver Empfänger oder Empfängerin zu bleiben. Ein Publikum, dass sich mit diesen (Des-)Informationen durch Teilen, Liken und Posten beschäftigt und in das eigene persönliche Netzwerk als relevante Information einbringt. Durch die gezielte Ansprache bestimmter Personen und Gruppen mit maßgeschneiderten Inhalten kann ein Angreifer sowohl die Zuschauerzahl als auch das Engagement maximieren. Ein Nebeneffekt dieser Dynamik ist, dass ein erheblicher Teil der Wertschöpfungskette der Desinformation effektiv an die Zielgruppe ausgelagert wird, was zu deren schnellen Verbreitung in der Gesellschaft beiträgt.[199]

Soziale Medien, als Nebenerscheinung der heutigen hochgradig digitalisierten und globalisierten Welt, haben neue Abhängigkeiten und Schwachstellen für unsere Gesellschaften geschaffen. Sie haben Plattformen, Domänen und Staaten so miteinander verflochten, dass ein Angriff auf das Computernetzwerk eines Akteurs bspw. kaskadenartige Auswirkungen auf die physischen, digitalen und telekommunikativen Sphären nicht nur der eigenen, sondern auch externer staatlicher Domänen haben kann. Cyberkriminelle finden auch Wege, Desinformationen in hybriden Angriffen zu nutzen, die physische Folgen für die Bürgerinnen und Bürger sowie die Gesellschaft, in der sie leben, haben können.

Deutschlands Schwachstellen

Mit den kommenden Bundes- und Landtagswahlen 2021 in Deutschland gewinnt das Problem der Bekämpfung bösartiger Informationskampagnen eine neue Dringlichkeit.[200] Die aktuelle Corona-Krise, das wohl akuteste Beispiel für narrative Manipulation, verschärft die Spannungen und macht Deutschland für gezielte Kampagnen angreifbar wie nie zuvor.

Das Bundesamt für Verfassungsschutz (BfV) hat bereits eine Zunahme der Propagandaaktivitäten über die gesundheitliche Situation in Deutschland festgestellt, insbesondere aus Russland und seinen deutschsprachigen Medienangeboten.[201] Der gleichzeitige Aufstieg von prominenten Verschwörungstheoretikerinnen und -theoretikern wie Attila Hildmann und seiner gleichnamigen Bewegung sowie der Plattform Querdenken711 verdeutlicht die Potenz der Desinformation als mobilisierende Kraft gegen das politische System.[202] Darüber hinaus werden die Wege der Verbreitung über offene und geschlossene soziale Netzwerke bis hin zu Demonstrationen und Massenprotesten aufgezeigt.

Seiner Natur als multidirektionale Bedrohung folgend, ist auch Deutschland mit gezielten Einflusskampagnen aus China konfrontiert worden. Im April 2020 warnte die Europäische Kommission, dass sich Pekings Einflusskampagnen darauf konzentrierten, das globale Image Chinas im Zuge der Pandemie zu verbessern.[203] Berlin bestätigte kurz darauf, dass chinesische Diplomaten aktiv auf deutsche Beamte zugehen und positive öffentliche Stellungnahmen zum Coronavirus-Management der Volksrepublik China fordern.[204]

Schließlich schafft Deutschlands politisches Spenden- und Wahlkampffinanzierungsgesetz einen weiteren nicht zu vernachlässigenden Weg der ausländischen Einflussnahme. Da es einfache Umgehungsmöglichkeiten gibt, wie z. B. Zahlungssplitting oder die Nutzung inländischer Dritter, können missliebige und/oder ausländische Akteure die Aufmerksamkeit von Politikerinnen und Politikern auf bestimmte Themen richten und deren öffentliche Kommunikation dazu beeinflussen.

Rückgewinnung der Deutungshoheit: ein zweigleisiger Ansatz

Die Verteidigung gegen diese Angriffshandlungen ist das Ziel strategischer Kommunikationskampagnen (Counter-Influence-Kampagnen). Sie sind ein Mittel für den verteidigenden Staat, ein besseres Verständnis für die Bedrohung zu entwickeln, indem er feindliche Akteure, Kanäle und Techniken identifiziert. In dieser Eigenschaft fungieren sie als aktive Verteidigungslinie gegen den zersetzenden Einfluss von Narrativen, die darauf abzielen, die Gesellschaft und letztlich auch den Staat selbst zu destabilisieren.

Die Geschwindigkeit der modernen Kommunikation macht es ineffektiv, sich bei der Vermittlung von Fakten auf die traditionellen (Rundfunk-)Medien zu verlassen. Was stattdessen benötigt wird, ist ein proaktiver Ansatz, der ein intimes Verständnis der Informationsflüsse mit der Fähigkeit kombiniert, feindliche Narrative zu erkennen, sobald sie sich entwickeln. Mit anderen Worten: ein Frühwarnsystem, das als erste Verteidigungslinie der Zivilgesellschaft gegen Versuche dient, den Informationsraum zu erobern.

Hierbei ist es notwendig, dass erstens feindliche Narrative frühzeitig aufgedeckt und zweitens ein strategisches Management von Gegennarrativen entwickelt wird, um die Sensibilität der Bevölkerung gegenüber irreführenden Informationen zu erhöhen. Die technischen Werkzeuge sind bekannt. Open Source Intelligence (OSINT) und klassische Monitoringexpertise, gepaart mit umfangreichen strategischen Kommunikationsfähigkeiten, sind in Deutschland und Europa vorhanden. Die Herausforderung besteht darin, schnell auf sich ändernde oder aufkommende Narrative zu reagieren und das strategische Messaging in kurzer Zeit entsprechend anzupassen. Die Fähigkeiten sollen gerade nicht für die aktive

Verbreitung einer staatlich sanktionierten oder parteipolitisch motivierten Meinung dienen. Der Einsatz dieser reaktiven Fähigkeiten zielt darauf ab, ein feindliches Narrativ daran zu hindern, seine maximale Wirksamkeit zu entfalten und ist daher entscheidend für die Wiedererlangung der Deutungshoheit in der Onlinesphäre – die wiederum Voraussetzung für die Stärkung der demokratischen Resilienz ist.

Narrative und Vektoren der Verbreitung identifizieren

Grundvoraussetzung für die Bekämpfung von Desinformation ist es, zu verstehen, wie sich durch Desinformationskampagnen geschaffene Narrative verbreiten. Nur so können sie identifiziert und ihnen glaubwürdig entgegengetreten werden. Wie bereits erwähnt, durchläuft die Desinformation mehrere Verbreitungsebenen, die jeweils durch den Grad der Anonymität definiert sind, bevor sie die sozialen Netzwerke und sogar die Rundfunkmedien (den sogenannten Mainstream) erreicht. Diese Ebenen können mithilfe von Cyber Intelligence (CYBINT)[205] und – noch wichtiger – Open-Source Intelligence (OSINT)[206] effektiv beobachtet werden, um dadurch feindliche Aktivitäten in diesen Bereichen zu identifizieren, zu überwachen, zu kartieren und zu entlarven.

Der erste Schritt ist die Überwachung von halbgeschlossenen Räumen. Der Zugang hierzu muss vorrangiges Ziel sein, erfordert jedoch spezielles technisches Know-how. Aber auch hierfür wurden bereits eine Reihe von maßgeschneiderten OSINT-Tools und -Techniken entwickelt, um legalen Zugang zu diesen Räumen zu erhalten und Daten über die darin ausgetauschten Informationen zu gewinnen. Dadurch ist es möglich, die einflussreichsten Nutzerinnen und Nutzer sowie die Muster des Informationsaustauschs mit anderen Gruppen zu untersuchen und ein umfassendes Verständnis für das Verhalten einer Gruppe zu entwickeln. Diese Techniken werden bspw. bereits verwendet, um die Dynamik zu analysieren, die der Anti-5G-Bewegung in mehreren europäischen Ländern zugrunde liegt. Dabei zeigte sich, dass geschlossene Gruppen auf Telegram, ByoBlu, Facebook und in geringerem Maße auch Discord pri-

märe Inkubatoren für feindselige Narrative waren, die schließlich in den öffentlichen Raum mäandern, um letztendlich über Twitter, Facebook und YouTube geteilt zu werden.

Desinformation wird typischerweise von einigen wenigen aktiven Accounts innerhalb einer Gruppe vorangetrieben, die dem Zweck dienen, Narrative zu waschen – indem sie immer wieder dieselben Desinformationen verbreiten, bis diese ständige Verbreitung die Wahrnehmung eines Themas dauerhaft verändert, was als „Wahrheitseffekt"[207] beschrieben wird. Je häufiger bestimmte singuläre Begriffe wiederholt werden, desto wahrscheinlicher ist es, dass sie Teil eines Desinformationsnarrativs sind, das zu einem späteren Zeitpunkt von nichtsahnenden Nutzerinnen und Nutzern verbreitet werden wird.

Obwohl es praktisch unmöglich ist, die Entwicklung eines Narrativs direkt vorherzusagen, ist es möglich, Signale zu verfolgen – z. B. das Auftauchen neuer Schlüsselbegriffe, häufig geteilte Artikel oder Videos – die auf eine sich verändernde Zielgruppe hinweisen. Sie fungieren als Signal, dessen Bedeutung darin liegt, dass es neue Zielgruppen anspricht und dadurch bisher unverbundene Gruppen miteinander verbindet.[208, 209]

Die Analyse der Anti-5G-Narrative veranschaulicht diesen Punkt über sich verschiebende und erweiternde Zielgruppen: Anti-5G-Stimmungen waren ursprünglich auf kleine Gruppen von Esoterikerinnen und Esoterikern beschränkt, die in relativer Isolation in speziellen Chatgruppen und Onlineforen agierten. Das änderte sich schlagartig, als neue Mitglieder hinzukamen, die neue Sichtweisen einbrachten, die sich auf populäre globale Verschwörungstheorien um George Soros, Covid-19 oder QAnon bezogen. Dies führte zu einer Verflechtung der Anti-5G- und globalen Verschwörungsnarrative, was zu einer raschen Ausweitung des Publikums von einer kleinen Randgruppe zu einer populären Gemeinschaft führte, gepaart mit einer aggressiveren Einstellung zur Politik.

Die Echokammern durchbrechen

Sobald ein sicherheitsrelevanter Diskurs identifiziert ist, besteht der nächste Schritt in der Entwicklung einer geeigneten Counter-Influence-Kampagne durch einen vielschichtigen Prozess der Veröffentlichung und Verbreitung von faktengeprüften Botschaften in Form von schriftlichem und grafischem Material. Das Ziel ist nicht, eine feindliche Beeinflussungskampagne gänzlich zu unterdrücken, sondern ihre Effektivität zu schwächen, indem man gegensätzliche Narrative schafft, die die Verwendung von unabhängig verifizierten Informationen fördern. Langfristig trägt dies dazu bei, das Bewusstsein der Bürgerinnen und Bürger für ein bestimmtes Thema zu schärfen, und hilft ihnen, Desinformation und Fake News zu erkennen.

Bislang haben sich die westlichen Regierungen schwergetan, kohärent auf die Verbreitung von Desinformation zu reagieren. Obwohl es mehrere Initiativen gibt, um das Bewusstsein für die Bedrohung und ihre Auswirkungen auf die öffentliche Meinung zu schärfen, konzentrieren sich diese in erster Linie darauf, falsche und irreführende Informationen, die bereits im Umlauf sind, zu korrigieren, anstatt ihre Verbreitung frühzeitig einzudämmen.[210] Die Begrenzung der Auswirkungen von Desinformation ist aufgrund ihrer hochdynamischen Natur eine gewaltige Herausforderung, die es erforderlich macht, dass sich Gegenerzählungen ebenso stark an wechselnde Inhalte, Zielgruppen und Kontexte anpassen.

Das Material, das der Counter-Influence-Kampagne zugrunde liegt, muss sich von dem der feindlichen Desinformationskampagnen dadurch unterscheiden, dass es korrekt, transparent und frei von rhetorischen Mitteln ist, die darauf abzielen, Emotionen hervorzurufen. Deutsche Regierungsinstitutionen verfügen offline bereits über eine Fülle solcher Informationen, was sie für die breite Öffentlichkeit jedoch praktisch unsichtbar macht und sie für den Aufbau einer glaubwürdigen Verteidigungslinie im Onlinebereich dadurch unbrauchbar macht. Die Herausforderung besteht darin, diese Fülle an Material online zu bewegen und es damit im öffentlichen Diskurs auf eine stetige, koordinierte Art und Weise zu verbreiten; und zwar im Kontext von Themen, bei denen es am wirkungsvollsten sein kann.

Obwohl das Vertrauen der deutschen Bevölkerung in die Regierung über die Jahre hinweg bemerkenswert hoch geblieben ist,[211, 212] gibt es keine Garantie, dass dies für die Zukunft so bleiben wird. Die wachsende Bedeutung von Graswurzelinfluencerinnen und -influencern wie KenFM, Attila Hildmann und Bewegungen wie Querdenken 711 im Gefolge der Covid-19-Pandemie zeigt, dass ein größerer Teil der Bevölkerung skeptischer gegenüber öffentlichen Institutionen und der Verbreitung von Informationen von oben nach unten wird. Das macht es wahrscheinlicher, dass diese Menschen Informationen, die von offiziellen staatlichen Social-Media-Accounts und Webseiten stammen, ablehnen. Zweitens fällt es deutschen Politikerinnen und Politikern schwer, mit der Wählerschaft über soziale Medien auf sinnvolle und konsistente Weise in Kontakt zu treten,[213] um nützliche Informationen in die Öffentlichkeit zu bringen.

Um dieses Dilemma zu überwinden, bedarf es einer neutraleren Vermittlung zwischen der Regierung und der breiten Bevölkerung unter Aufsicht unabhängiger staatlicher Stellen. Dies bedeutet, dass ein breites Spektrum an schriftlichem und visuellem Material zur Verteidigung der deutschen Grundwerte über soziale und Printmedien sowie Videoplattformen ohne explizites Regierungsbranding veröffentlicht werden sollte. Da OSINT-Monitoring Wissen aus erster Hand darüber liefert, wer die gefährdeten Zielgruppen sind und was gesagt wird, kann die Gegenerzählung genau auf diese Gruppen zugeschnitten und so verpackt werden, dass sie spezifische Narrative der Desinformation anspricht und entlarvt.

So kann zum Beispiel der stetige Fluss von Gegennachrichten in sozialen Netzwerken wie Twitter, Facebook und YouTube fein abgestimmt werden, um sicherzustellen, dass sie den Trendthemen folgen und von einflussreichen Accounts aufgegriffen werden. Um jedoch wirklich von der sozialen Dynamik zu profitieren – und den Eindruck eines Informationsflusses von oben nach unten zu vermeiden – muss eine erfolgreiche Counter-Influence-Kampagne auf einer tieferen Ebene mit der Zivilgesellschaft in Verbindung treten, und zwar über Basisorganisationen, Crowdsourcing-Thinktanks und unabhängige Fact-Checking-Dienste als zusätzliche Vektoren zur Erhöhung der Reichweite und der Bekanntheit von unten nach oben.

Ein Hauptziel des Auswerfens eines breiten Netzes von Vektoren ist es, Social-Media-Nutzerinnen und -nutzer zur Interaktion mit den Counter-Influence-Inhalten zu verleiten. In der Tat nutzt die Counter-Influence-Kampagne dieselbe Dynamik, die die Desinformation ermöglicht: Als aktive statt passive Konsumentinnen und Konsumenten von Informationen hilft das Teilen, Liken und Kommentieren von Nutzerinnen und Nutzern jetzt aber, die Sichtbarkeit von Fakten in Nachrichten und Trending Feeds aufrecht zu erhalten.

Der Unterschied besteht darin, dass die anhaltende Konfrontation mit einem Standpunkt, der einer etablierten Perspektive widerspricht, die Bestätigungsvoreingenommenheit der Menschen herausfordert. Am wichtigsten ist, dass die Informationen, die durch die Counter-Influence-Kampagne verbreitet werden, aus einer neutralen Richtung kommen, so dass die Nutzerinnen und Nutzer geneigter sind, sie als alternative Informationsquelle zu verarbeiten und zu verbreiten. Mit anderen Worten: Während Desinformationskampagnen und Algorithmen einem Publikum den Raum nehmen können, eigene Überzeugungen zu hinterfragen,[214] bietet eine gezielte Counter-Influence-Kampagne den sicheren Raum, um das kritische Denken zu entwickeln, das notwendig ist, um sich von diesen manipulierten Überzeugungen und dem damit verbundenen Echokammereffekt zu lösen.

Containment erreichen

Das derzeitige System macht die gutwilligen, besorgten und nichtsahnenden Verbreiter der (Des-)Informationen verantwortlich, nicht aber die eigentlichen böswilligen Urheber der Desinformation. Deutschland verfolgt eine Politik, die den Medien eine freiwillige Selbstkontrolle auferlegt, auch wenn die Effektivität eines solchen Ansatzes im Zusammenhang mit sozialen Netzwerken infrage gestellt wurde.[215] Während die Identifizierung der genauen Quelle von Desinformation mit zahlreichen technischen Schwierigkeiten behaftet ist, ist es möglich, die breiteren Desinformationsnetzwerke, die in Deutschland operieren, abzubilden –

seien es Webseiten oder Konten auf Facebook und Twitter – und sie zu entlarven und dadurch die Möglichkeit zu eröffnen, ihre Operationen zu stören.

Wenige Hauptakteure spielen bei der Verbreitung von militanten Antiimpfkampagnen und Anti-Corona-Kampagnen in mehreren europäischen Ländern – darunter auch Deutschland – mithilfe eines umfangreichen Netzes von verknüpften Website-Domains eine maßgebliche Rolle. Diese werden von Servern aus betrieben, die einer einzigen Einheit gehören. Es war bekannt, dass die auf diesen Websites veröffentlichten Themen die Debatten auf Telegram und Facebook beeinflusst hatten. Aber erst die Erkenntnis, dass es einer einzigen Entität gelungen war, einen ganzen Bereich des deutschsprachigen Internets zu Antiimpfthemen und verwandten Themen effektiv zu monopolisieren, lieferte den konkreten Beweis, dass eine koordinierte Desinformationskampagne im Gange ist, mit dem Ziel, die öffentliche Meinung negativ zu beeinflussen.

Damit einhergehende Recherchen, die sich infolge auf soziale Medien konzentrierten, enthüllten, wie wenige hochaktive Accounts – gefälscht und echt – dieselben Informationen über mehrere Facebook-Gruppen in Deutschland und anderen Ländern austauschen. Die Zuführung und Verbreitung der gleichen gefälschten oder irreführenden Quellen in einer Reihe von parallellaufenden Debatten führte infolge zur Schaffung eines einzigen, weitgehend kohärenten Narrativs, das von Antiimpfaktivistinnen und -aktivisten in der gesamten EU sowohl online als auch im weiteren Verlauf offline – in Form von Demonstrationen – verbreitet wurde.

Das Wissen um die spezifischen Plattformen und Netzwerke, die die Säulen der feindlichen Narrativbildung sind, macht die Anpassung von Gegennarrativen effektiver, und in Kombination mit dem Identifizieren dieser Netzwerke hat ein Staat ein schlagkräftiges Werkzeug, um Desinformation bereits beim Entstehen einzudämmen.

Resilienz als Sicherheitsfaktor

Die Sensibilisierung von Internetnutzerinnen und -nutzern für Desinformationsquellen ist jedoch nur eine Facette einer größeren nationalen Strategie zur Bekämpfung ausgeklügelter Desinformationskampagnen unter einem breiteren Sicherheitsaspekt. Resilienz erfordert v. a. Flexibilität und Raum für Wachstum. Genauso wie sich Technologien und Informationsplattformen verändern und wachsen, müssen auch die technischen Fähigkeiten so ausgerichtet sein, dass sie mitwachsen und sich an dieses Umfeld anpassen. Gruppen und Akteure werden immer neue Wege finden, um Einfluss auf die deutsche Politik und Gesellschaft zu nehmen und (Des-)Informationen zu verbreiten, wie der Wechsel der ursächlichen Verbreiter von Falschinformation von Telegram zu Discord und Bitchute oder von Facebook zu ByoBlu zeigt.

Um Desinformation von Grund auf effektiv bekämpfen zu können, müssen Deutschland und seine Partner in der NATO und anderswo erkennen, wie wichtig es ist, Ressourcen für diese Bemühungen bereitzustellen. Die Frage, ob diese Art von Angriffen bekämpft werden kann, steht nicht zur Diskussion, sondern nur das Wie. Obwohl Desinformationen als Angriffsmittel v. a. dort entwickelt wurden, wo man nicht über die gleiche technologische oder finanzielle Schlagkraft verfügt wie der Westen, stehen die europäischen Regierungen allzu oft noch auf verlorenem Posten.

Mit der demnächst anstehenden Aktualisierung der EU-Ratsrichtlinie 2008/114/EG könnten Telekommunikation und digitale Aspekte in die Definition einer europäischen Kritischen Infrastruktur (KI) aufgenommen werden.[216] Dies könnte bedeuten, dass je nach Tiefe und Umfang einer Desinformationskampagne – in Verbindung mit einem breiteren hybriden Angriff – diese ebenso als Angriff auf Europas Künstliche Intelligenz behandelt werden könnte. Um sich auf diese Realität vorzubereiten, wäre Deutschland gut beraten, Ressourcen für seine Schutz- und Melde-

mechanismen bereitzustellen – einschließlich nationaler Tabletopübungen zu hybriden Angriffen und der Teilnahme an ähnlichen Übungen auf EU- und NATO-Ebene.

In Anbetracht des internationalen Charakters der Bedrohung könnten solche Übungen, wenn sie in Verbindung mit kooperativen EU- und NATO-Diskussionen über Ermittlungs- oder Rechenschaftsmechanismen gegen Desinformationsverursacher durchgeführt und strategisch bekannt gemacht würden, an sich schon abschreckend auf die Verbreitung von Desinformation wirken. Abschreckung ist eine Kosten-Nutzen-Analyse, und das internationale diplomatische Umfeld besteht immer noch aus überwiegend rationalen Akteuren.

Fazit

Angesichts einer wachsenden Bedrohung braucht Deutschland einen neuen Ansatz, um Desinformation von unten und von oben zu bekämpfen. Die bloße Verbreitung von Fakten ist in Zeiten der Hochgeschwindigkeitskommunikation, die durch eine Vielzahl von nichttraditionellen Plattformen gekennzeichnet ist, nicht ausreichend. Ebenso wichtig ist die Fähigkeit, dem Publikum, das böswilligen Desinformationskampagnen zum Opfer gefallen ist, präzise Gegenargumente zu liefern.

Das wachsende Misstrauen in einer Bevölkerung, die einer Vielzahl von Informationsquellen ausgesetzt ist, schränkt die Regierung ernsthaft ein, Counter-Influence-Kampagnen effektiv durchzuführen. Es wird immer wichtiger, mit spezialisierten Akteuren aus dem privaten Sektor zusammenzuarbeiten, die die nächsten Schritte in der Technologie kennen und wissen, was diese Innovationen wirklich bedeuten.

Die Eindämmung sicherheitsrelevanter Desinformationskampagnen und die Steigerung des kritischen Denkens bei Internetnutzerinnen und -nutzern ist entscheidend für die dauerhafte Stärke des politischen Systems in Deutschland und in Europa. Da nur jeder zehnte Deutsche glaubt, Desinformation sicher identifizieren zu können, ist es für den Aufbau langfristiger Widerstandsfähigkeit gegen subversive Desinformationskampagnen unerlässlich, die Zivilgesellschaft in die Lage zu versetzen, Fakten von Fiktion zu unterscheiden. Eine kohärente Counter-Influence-Kampagne trägt auch dazu bei, ein besseres Verständnis der sich entwickelnden Informationsflüsse zwischen staatlichen Institutionen, Medien und der Öffentlichkeit zu erlangen.

Die Bedrohung von außen wird weiterwachsen. Auch wenn es sich um eine grenzüberschreitende Bedrohung handelt, die auch Mitgliedstaaten der NATO und der EU betrifft, sollte Deutschland bei der Vorstellung von Instrumenten zur Definition und Bekämpfung solcher Bedrohungen eine Vorreiterrolle einnehmen.

195 Bennett WL, Livingston S. (2018). The disinformation order: Disruptive communication and the decline of democratic institutions. European Journal of Communication, Vol. 33(2), S. 122–139, S. 132.

196 Lewandowsky, S., Ecker, U. K. H., & Cook, J. (2017). Beyond misinformation: Understanding and coping with the „post-truth" era. In: Journal of Applied Research in Memory and Cognition, 6 (4), S. 353–369, S.354–355.

197 Edda Humprecht (2019). Where 'fake news' flourishes: a comparison across four Western democracies. In: Information, Communication & Society, Vol. 22 (13), S. 1973–1988, S. 1976.

198 Rid, Thomas (2020). Active Measures: The Secret History of Disinformation and Political Warfare. New York: Farrar, Straus and Giroux, S. 436.

199 Ebd., S.437.

200 Hameleers, Michael, Powell, Thomas E. Van Der Meer, Toni G. L. A. & Bos, Lieke (2020). A Picture Paints a Thousand Lies? The Effects and Mechanisms of Multimodal Disinformation and Rebuttals Disseminated via Social Media. In: Political Communication, Vol. 37 (2), S. 281–301, S.284; Koch, Matthias (2020). FDP warnt vor Manipulation bei Bundestagswahl. Redaktionsnetzwerk Deutschland. 25.7.2020. https://www.rnd.de/politik/fdp-warnt-vor-manipulation-bei-bundestagswahl-2021-VOYBJFZO3RBJNKVFBSYJRUEMQQ.html (letzter Zugriff: 14.12.2020).

201 Russische Medien verbreiten Desinformation über Corona in Deutschland (2020). *Der Tagesspiegel*, 8.10.2020. https://www.tagesspiegel.de/politik/verfassungsschutz-beobachtet-propaganda-russische-medien-verbreiten-desinformation-ueber-corona-in-deutschland/26257112.html (letzter Zugriff: 14.12.2020).

202 Barker, Tyson (2020). Germany Is Losing the Fight Against QAnon. In: *Foreign Policy*, 2.9.2020. https://foreignpolicy.com/2020/09/02/germany-is-losing-the-fight-against-qanon/ (letzter Zugriff: 13.10.2020).

203 EEAS Special Report Update: Short Assessment of narratives and disinformation around the Cpvid-19 pandemic (2020). EU vs Disinfo, 1. 4.2020. https://euvsdisinfo.eu/eeas-special-report-update-short-assessment-of-narratives-and-disinformation-around-the-covid-19-pandemic/ (letzter Zugriff: 14. 12.2020).

204 China kontaktierte heimlich deutsche Beamte (2020). *Der Tagesspiegel*, 26. 4.2020, https://www.tagesspiegel.de/politik/bundesregierung-bestaetigt-einflussversuch-china-kontaktierte-heimlich-deutsche-beamte/25774498.html (letzter Zugriff: 14.12.2020).

205 Intelligence Studies: Cyber Intelligence. (o. J.) Newport, Rhode Island: U.S. Naval War College: https://usnwc.libguides.com/c.php?g=494120&p=3381599 (letzter Zugriff: 21.10.2020).

206 Williams, Heather J. & Blum, Ilana (2018). Defining Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise. Santa Monica: RAND Corporation, S. 8 https://www.rand.org/content/dam/rand/pubs/research_reports/RR1900/RR1964/RAND_RR1964.pdf (letzter Zugriff: 14.12.2020).

207 Zimmermann, Fabian & Kohring, Matthias (2020). Mistrust, Disinforming News, and Vote Choice: A Panel Survey on the Origins and Consequences of Believing Disinformation in the 2017 German Parliamentary Election. In: Political Communication, Vol. 37 (2), S. 215–237, S. 217.

208 Barasch, A., & Berger, J. (2014). Broadcasting and narrowcasting: How audience size affects what people share. In: Journal of Marketing Research, 51 (3); S. 286–299.

209 Scholz, Christin, Baek, Elisa C., O'Donnell, Matthew Brook & Falk, Emily B. (2019). Decision-making about broad- and narrowcasting: a neuroscientific perspective. In: Media Psychology, Vol. 23 (1), S. 131–155.

210 Medien- und Kommunikationsbericht der Bundesregierung 2018. BT-Drucks. 19/6970 (2019). http://dipbt.bundestag.de/doc/btd/19/069/1906970.pdf (letzter Zugriff: 12.12.2020).

211 OECD (2014). „Vertrauen in den Staat, Wirksamkeit des staatlichen Handelns und die Governance-Agenda." In: Regierung und Verwaltung auf einen Blick 2013, OECD Publishing, Paris, S. 33, https://www.oecd-ilibrary.org/docserver/9789264209541-6-de.pdf?expires=1607776169&id=id&accname=guest&checksum=108301392D1E2AD97525FFDA5CB970B9 (letzter Zugriff: 13.12.2020).

212 Vertrauen in Regierung erreicht in Corona-Krise Höchstwert (2020). *Der Tagesspiegel*, 11.5.2020, https://www.tagesspiegel.de/politik/rekordwert-in-der-pandemie-vertrauen-in-regierung-erreicht-in-corona-krise-hoechstwert/25819304.html (letzter Zugriff: 14.12.2020).

213 Oelsner, Karoline & Heimrich, Linette (2015). Social Media Use of German Politicians: Towards Dialogic Voter Relations? In: German Politics, Vol. 24 (4), S. 451–468, S. 465; Stier, Sebastian, Bleier, Arnim, Lietz, Haiko & Strohmaier, Markus (2018). Election Campaigning on Social Media: Politicians, Audiences, and the Mediation of Political Communication on Facebook and Twitter. In: Political Communication, Vol. 35 (1), S. 50–74, S. 63.

214 Walker, Shawn, Mercea, Dan & Bastos, Marco (2019). The disinformation landscape and the lockdown of social platforms. In: Information, Communication & Society, Vol. 22 (11), S. 1531–1543, S. 1535.

215 Thomasson, Emma (2019). Germany insists self-regulation not enough for Facebook. Reuters. 8.7.2020. https://www.reuters.com/article/us-facebook-ads-boycott-germany-idUSKBN2491IO (letzter Zugriff: 14.12.2020).

216 Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (Text with EEA relevance) (2008). OJ 32008L0114. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2008.345.01.0075.01.ENG (letzter Zugriff: 14.12.2020).

Autorinnen und Autoren

Jan Wilhelm Ahmling ist Politikwissenschaftler und arbeitet als Referent bei der Hermann Ehlers Stiftung e. V. Zuvor arbeitete er für den Bundesverband der Deutschen Industrie und den Ost-Ausschuss der deutschen Wirtschaft.

Christian Bell ist Oberstleutnant am Zentrum Operative Kommunikation der Bundeswehr. Er ist dort als Sachgebietsleiter für Propaganda Awareness eingesetzt.

Dr. Cedric Bierganns, Historiker und Referent für Sicherheitspolitik und Bundeswehr bei der Konrad-Adenauer-Stiftung e. V. Im Herbst 2021 erscheint sein neuestes Buch, das sich mit den amerikanischen Kommunikationsstrategien zum NATO-Doppelbeschluss befasst: Geistige Nachrüstung. Ronald Reagan und die Deutschlandpolitik der U. S. Information Agency 1981–1987.

Johannes Feige ist Public Affairs Consultant bei Avisa Partners in Paris. Seine besonderen Schwerpunkte sind die Analyse von Fake News und das Erstellen von Bekämpfungsstrategien.

Stefan Gruhl ist promovierter Politikwissenschaftler und seit 2017 Kommandeur am Zentrum Operative Kommunikation der Bundeswehr.

Dr. Julian Hajduk ist Senior Research Fellow und Senior Project Manager der Professur für Unternehmenskommunikation an der Universität der Bundeswehr München. Hajduk studierte Geschichte und Philosophie in München, Paris und Leiden (NL) und promovierte an der Universität

der Künste Berlin mit einer Arbeit zum Thema Medienframing. Zu seinen Forschungsschwerpunkten zählen strategisches Kommunikationsmanagement & Nachhaltigkeit sowie kommunikative Frühaufklärung & Wirkungsforschung.

Falko Hark ist Bildungs- und Erziehungswissenschaftler und Hauptmann am Zentrum Operative Kommunikation der Bundeswehr.

Philipp Huber ist psychologischer Fachberater am Zentrum Operative Kommunikation der Bundeswehr. Er ist dort als Teamleiter im Bereich der Konzept- und Fähigkeitsentwicklung eingesetzt.

Holger Knappenschneider ist Rechtsanwalt und Experte für strategische Kommunikation. Als Inhaber und Partner von Agenturen im Bereich politische Kommunikation verfolgt und analysiert er seit Jahren die Entwicklungen und Herausforderungen der politischen Meinungsbildung in unserer Gesellschaft.

Lion König ist promovierter Politikwissenschaftler und Major am Zentrum Operative Kommunikation der Bundeswehr. Er ist dort u. a. mit der Analyse gegnerischer Propaganda und Desinformation betraut.

Jakob Landwehr-Matlé ist wissenschaftlicher Mitarbeiter an der Professur Internationale Beziehungen der Technischen Universität Chemnitz. Seine Promotionsforschung konzentriert sich auf Konfliktprävention, -analyse und -lösung sowie Verhandlungs- und Mediationstheorien und die Vereinten Nationen und regionale Akteure.

Prof. Dr. Florian Meißner ist Professor für Medienmanagement und Journalistik an der Macromedia University of Applied Sciences in Köln. Meißner ist zudem Advisor Germany bei NewsGuard, einem Unternehmen, das anhand grundlegender journalistischer Kriterien die Glaubwürdigkeit und Transparenz von Nachrichten- und Informationswebsites bewertet.

Dipl. Inform. Albert Pritzkau ist wissenschaftlicher Mitarbeiter der Forschungsgruppe „Informationsanalyse" am Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie (FKIE). Sein Forschungsschwerpunkt liegt in Detektion und Bewertung von Informationskampagnen auf Online-Plattformen.

Prof. Dr. Ulrich Schade leitet die Forschungsgruppe „Informationsanalyse" am Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie (FKIE), die auf die automatisierte Auswertung von Textdokumenten und „Social Media"-Beiträgen spezialisiert ist. Herr Schade lehrt darüber hinaus im Masterstudiengang „Applied Linguistics" der Rheinischen Friedrich-Wilhelms-Universität Bonn.

Jürgen Schulz ist Professor für Strategische Kommunikationsplanung im Studiengang Gesellschafts- und Wirtschaftskommunikation an der Universität der Künste Berlin. Zu seinem didaktischen Programm zählen u. a. Strategic Wargames zur Simulation von Public Affairs.

Amelie Stelzner ist Referentin für Bundeswehr und Gesellschaft in der Hauptabteilung Analyse und Beratung der Konrad-Adenauer-Stiftung e. V. Sie engagiert sich als Mitglied im erweiterten Vorstand von Women in International Security (WIIS).

Frau Sonja Verschitz ist Linguistin und Politologin und war bis Mitte März 2021 als Projektleiterin des Instituts für Politische Wissenschaft der RWTH Aachen für die akademische Begleitung der nicht-technischen Studie *Propaganda Awareness* des Kommando Cyber- und Informationsraum der Bundeswehr (KdoCIR) zuständig (Indikationen Sprache, Diskursanalytisches Begleitdokument). Als extern Promovierende am Institut für Politische Wissenschaft der RWTH Aachen arbeitet Frau Verschitz - unterstützt KdoCIR der Bundeswehr – an ihrem Promotionsvorhaben zum Thema *Information Awareness*.

Nils Wörmer leitet die Abteilung Internationale Politik und Sicherheit innerhalb der Hauptabteilung Analyse und Beratung der Konrad-Adenauer-Stiftung e.V. Zuvor war er als Leiter der Auslandsbüros Afghanistan sowie Syrien/Irak der Stiftung tätig und arbeitete als wissenschaftlicher Mitarbeiter für die Stiftung Wissenschaft und Politik. Nils Wörmer ist Oberstleutnant der Reserve.

Prof. Dr. Natascha Zowislo-Grünewald ist Professorin für Unternehmenskommunikation an der Universität der Bundeswehr München. Sie erwarb ihren Master of Arts an der Paul H. Nitze School of Advanced International Studies der Johns Hopkins University in Washington, D. C. Anschließend promovierte sie in Mannheim und war in der Unternehmenskommunikation zweier internationaler Unternehmen tätig. 2010 habilitierte sie sich an der Kulturwissenschaftlichen Fakultät der Universität Bayreuth. Ihre Forschungsgebiete sind Kommunikationsmanagement in Politik und Wirtschaft sowie Kommunikation im Kontext von Sicherheitspolitik.

Kontakt

Steven Bickel
Referent Innere Sicherheit
Analyse und Beratung
T +49 30 / 26 996-3927
steven.bickel@kas.de

Amelie Stelzner
Referentin Bundeswehr
und Gesellschaft
Analyse und Beratung
T +49 30 / 26 996-3795
amelie.stelzner@kas.de

Freiheitliche Gesellschaften sehen sich zunehmend Bedrohungen durch hybride Kriegsführung, Meinungsmanipulation, Desinformationskampagnen, Fake News und anderen Formen delegitimierender Kommunikation ausgesetzt. Gerade die stark wachsenden Bereiche Künstliche Intelligenz und soziale Medien verstärken diese Entwicklung noch. Doch wie sieht eine geeignete sicherheitspolitische Antwort auf diese kommunikative Bedrohungslage aus?

Die im vorliegenden Band vereinten Beiträge analysieren und bewerten diese sicherheitspolitisch relevanten Bedrohungsszenarien im Informations- und Diskurs-raum aus dem Blickwinkel verschiedener Fachdisziplinen. Hierauf aufbauend werden auch Strategien aufgezeigt, wie freiheitliche Gesellschaften solchen kommunikativen Bedrohungslagen wirksam gegenübertreten können.

Konrad-Adenauer-Stiftung e. V.