POLITIK

KARL MORITZ HEIL

RESILIENZ UND ABSCHRECKUNG BEI EU UND NATO

KOLLEKTIVE STRATEGIEN ZUR ABWEHR DIGITALER DESINFORMATION

Karl Moritz Heil

Kollektive Strategien zur Abwehr digitaler Desinformation

Resilienz und Abschreckung bei EU und NATO

Bibliografische Information der Deutschen Nationalbibliothek:

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Impressum:

Ein Imprint der GRIN Publishing GmbH, München

Druck und Bindung: Books on Demand GmbH, Norderstedt, Germany

Coverbild: GRIN Publishing GmbH | Freepik.com | Flaticon.com | ei8htz

Inhaltsverzeichnis

Abkürzungsverzeichnis

CCD COE	NATO Cooperative Cyber Defence Centre of Excellence
CIA	Central Intelligence Agency
COE	Centre of Excellence (von der NATO akkreditiert)
CSIS	Canadian Security Intelligence Service
DSGVO	Datenschutz-Grundverordnung
EAD	Europäischer Auswärtiger Dienst
EFP	Enhanced Forward Presence
ENISA	EU Agency for Network and Information Security
ESTF	East StratCom Task Force
EU	Europäische Union
EU INTCEN	EU Intelligence Analysis Centre
FSB	‚Föderaler Dienst für Sicherheit' (Федеральная служба безопасности Российской Федерации) – russischer Inlandsgeheimdienst
GASP	Gemeinsame Außen- und Sicherheitspolitik
GRU	‚Hauptverwaltung für Aufklärung' (Главное разведывательное управление) – russischer Militärnachrichtendienst
GSVP	Gemeinsame Sicherheits- und Verteidigungspolitik
Hybrid CoE	European Centre of Excellence for Countering Hybrid Threats
IRA	Internet Research Agency
JISD	Joint Intelligence and Security Division
KGB	‚Komitee für Staatssicherheit' (Комитет государственной безопасности) – Geheimdienst der Sowjetunion
NATO	North Atlantic Treaty Organization
NGO	Nongovernmental organization
NIS	Netzwerk- und Informationssicherheit
PACE	Parallel and Coordinated Exercises

RAP	Readiness Action Plan
RT	Russia Today (bis 2009)
SSZ	Ständige Strukturierte Zusammenarbeit
STRATCOM COE	NATO Strategic Communications Centre of Excellence
US SSCI	United States Senate Select Committee on Intelligence
USA	United States of America
VJTF	Very High Readiness Joint Task Force

Abbildungsverzeichnis

1 Einleitung und Fragestellung[1]

> „Falsehood flies, and truth comes limping after it, so that when men come to be undeceived, it is too late; the jest is over, and the tale hath had its effect." (Jonathan Swift 1710)[2]

Die Präsidentschaftswahlen 2016 stellen nicht nur eine Zäsur in der politischen Geschichte der Vereinigten Staaten von Amerika (USA) dar, sondern auch auf internationaler Ebene. Spätestens mit der Veröffentlichung des *Report On The Investigation Into Russian Interference In The 2016 Presidential Election* des Special Counsel Robert Mueller (US DOJ 2019) wurde das Ausmaß und die Raffinesse der Desinformationskampagne deutlich, mit der der Kreml den Ausgang der Wahlen in seinem Sinne beeinflussen wollte. Auch wenn sich nicht mit Sicherheit feststellen lässt, ob und inwieweit sich die Einflussnahme des Kreml in den Wahlergebnissen niedergeschlagen hat, ist schon allein die Kühnheit der Operation bemerkenswert.[3]

Wenngleich Desinformationskampagnen kein neues Phänomen darstellen, bieten sich durch die zunehmende globale Vernetzung im Zuge der Digitalisierung beispiellose neue Möglichkeiten zur gezielten Beeinflussung demokratischer Prozesse. Die russische Einmischung in die US-Wahlen stellt somit nur einen vorläufigen Höhepunkt des strategischen Einsatzes von Desinformation zur außenpolitischen Einflussnahme dar. Russland nimmt zwar in Qualität und Quantität eine Vorreiterrolle ein, ist jedoch nicht der einzige Akteur in diesem Bereich. Besonders für autoritäre Regime eröffnen sich eine Vielzahl neuer Strategien, um öffentliche Meinungen im In- und Ausland zu manipulieren und ihre relative Machtposition auf internationaler Ebene zu stärken.[4] Hierbei kommt ihnen eine Asymmetrie der Offenheit zwischen ihren restriktiven Systemen und den liberalen Systemen

---

1 Diese Arbeit hat den Anspruch, gendergerechte Sprache zu verwenden, die alle Geschlechtsidentitäten umfasst. Mitunter wird zwar das generische Maskulinum genutzt, dies betrifft allerdings nur Subjekte die keine explizite Geschlechtsidentität beanspruchen, wie etwa Staaten, Organisationen und sonstige Körperschaften.

2 In: *The Examiner* 14, 9. November 1710.

3 Angesichts des knappen Ausgangs der Wahl, ist dies nicht unwahrscheinlich.

4 So stellen Bradshaw und Howard (2019) fest, dass zwischen 2017 und 2019 staatlich organisierte Desinformationskampagnen zur außenpolitischen Einflussnahme auch durch China, Iran, Venezuela, Pakistan, Saudi-Arabien und Indien strategisch eingesetzt wurden (dies soll nicht heißen, dass all diese Länder als autoritär einzuordnen sind). Der weniger anspruchsvolle Einsatz von Desinformation in der Innenpolitik ist wesentlich weiter verbreitet, vor allem durch autoritäre Regime (vgl. ebd.), aber auch nicht staatliche Akteure.

westlicher Demokratien entgegen, wodurch autoritäre Regime es wesentlich leichter haben, ihre Narrative in demokratischen Gesellschaften zu platzieren als umgekehrt.

Die Gefahr dieser Entwicklung für die Demokratie, Stabilität, Sicherheit und Souveränität westlicher Gesellschaften und Institutionen gewinnt zunehmend an politischer und medialer Aufmerksamkeit, wie sich etwa in Diskursen um *fake news* und *hybrider Kriegsführung* zeigt. Aufgrund des grenzüberschreitenden Charakters dieser neuen Herausforderungen stehen bei der politischen Bearbeitung der Problematik verstärkt kollektive Akteure im Mittelpunkt. Eine besondere Rolle kommt dabei der Europäischen Union (EU) und der Organisation des Nordatlantikvertrags (NATO) zu, da diese zu den bedeutendsten westlichen Akteuren kollektiver Sicherheit auf internationaler Ebene gehören und zugleich, bzw. auch deshalb, selbst Feindbilder und Ziele russischer Desinformationskampagnen darstellen. Für die Mitglieder dieser Organisationen bieten sich Antworten auf kollektiver Ebene an, da sie alleine meist nicht über die nötigen Fähigkeiten und Ressourcen verfügen, um der Problematik in ihrer Gesamtheit begegnen zu können.

Das Phänomen der digitalen Desinformation[5] erstreckt sich über eine Reihe von Politikfeldern und Themen, zu denen sich unter anderem Demokratie und Wahlprozesse, Presse- und Meinungsfreiheit, Mediengesetze, Außen- und Sicherheitspolitik und Digitalpolitik zählen lassen. Diese Vielschichtigkeit stellt EU und NATO vor besondere Herausforderungen, da ihre Handlungsoptionen mit den begrenzten Kompetenzen und spezifischen Ermächtigungen vorgegeben sind, die ihnen durch ihre Mitglieder gewährt werden. Da sich beide Organisationen in Beschaffenheit, Evolution und Mandat grundlegend voneinander unterscheiden, können folglich auch ihre Instrumente und Strategien im Umgang mit Desinformation je nach Politikfeld variieren. Während die EU als Staatenverbund mit eigener Rechtspersönlichkeit und weitreichenden zivilen Kompetenzen sich als demokratisches Friedensprojekt und gemeinsamer Markt versteht, ist die NATO als Militärbündnis vor allem auf kollektive Sicherheit und Verteidigung ausgerichtet.

Diese Arbeit wird sich im Folgenden der zentralen Frage widmen, wie sich die Herangehensweisen der EU und der NATO zur Abwehr und Bekämpfung digitaler

[5] Der Übergang zwischen dem digitalen und dem analogen Raum ist bei der Verbreitung von Desinformation fließend. Der Fokus dieser Arbeit auf den *digitalen* Aspekt der Desinformation entspringt der Anerkennung der zentralen Bedeutung des digitalen Raums, besonders in Gestalt der sozialen Medien, für die Renaissance des Phänomens der Desinformation.

Desinformation unterscheiden und worauf diese Unterschiede zurückzuführen sind. Ein besonderes Augenmerk soll bei dieser Untersuchung darauf liegen, inwiefern die strukturellen Eigenarten beider Organisationen ihre Strategien im Umgang mit Desinformation beeinflussen und welche jüngeren historischen Entwicklungen dabei zu beobachten sind. Daran anschließend lassen sich Erkenntnisse dazu erhoffen, wie beide Akteure auf komplexe Herausforderungen reagieren, die über ihr spezifisches Spektrum an Fähigkeiten, Instrumenten und möglichen Strategien hinausgehen. Es wird zudem interessant sein zu beobachten, wie internationale Organisationen neue Konzepte angesichts geänderter äußerer Umstände adaptieren und institutionalisieren und welche Hindernisse dabei eine Rolle spielen. Für die Untersuchung ist dabei irrelevant, ob die tatsächliche Bedrohung durch Desinformation im digitalen Raum überschätzt sein sollte,[6] da die politischen Antworten von EU und NATO durchaus real sind und es deshalb lohnenswert erscheint, sich mit den Strategien auseinanderzusetzen, die diesen Bemühungen zugrunde liegen.

Angesichts der Neuartigkeit und Komplexität der Thematik ist es für diese Arbeit zunächst erforderlich, eine eindeutige Terminologie zu etablieren und die wesentlichen Elemente der Problematik der digitalen Desinformation zu erörtern. In diesem Sinne bietet Kapitel 2 sowohl eine kritisch-explorative Übersicht zur Unterscheidung gängiger Begrifflichkeiten und Konzepte als auch eine grundlegende Erläuterung der Funktionsweise von Desinformation im digitalen Raum. Eine zentrale Rolle als *game changer* nehmen hierbei die sozialen Medien sowie die psychologischen und technischen Mechanismen ein, mit denen Desinformation im digitalen Raum verstärkt wird.

Kapitel 3 richtet daraufhin den Blick auf den staatlich organisierten Einsatz digitaler Desinformation zur außenpolitischen Einflussnahme und somit auf die Dimension der Problematik, die in Umfang und Zielsetzung die größte Bedrohung für EU und NATO darstellt. Am Beispiel russischer Desinformationskampagnen soll gezeigt werden, welche geschichtlichen Hintergründe vorliegen, wie staatlich organisierte Desinformation funktioniert und mit welchen Konzepten sie wissenschaftlich eingeordnet wird. In der Debatte um politische Antworten auf russische Desinformationskampagnen erfreuen sich Konzepte der hybriden Kriegsführung (*hybrid warfare*) und Informationskriegsführung (*information warfare*) sowohl bei EU

[6] In diesem Sinne argumentiert beispielweise Lanoszka (2019).

und NATO als auch in der Wissenschaft hoher Beliebtheit, weshalb es sinnvoll ist, im Rahmen dieser Arbeit genauer auf sie einzugehen.

Die theoretische Grundlage zum Vergleich des Vorgehens von EU und NATO wird in Kapitel 4 gelegt. Hierzu werden geläufige und idealtypische Strategien im Umgang mit digitaler Desinformation beschrieben und operationalisiert, anhand derer die Antworten von EU und NATO anschließend eingeordnet werden sollen. Strukturiert sind die Strategien zur Bekämpfung von Desinformation entlang der grundlegenden Konzepte der Resilienz und Abschreckung, die repräsentativ für Ansätze nach der Logik der Schadensbegrenzung bzw. Prävention stehen.

Kapitel 5 und 6 widmen sich schließlich dem konkreten Vorgehen von EU und NATO im Detail. Hierzu wird zunächst ein Überblick über die historische Entwicklung des Vorgehens und der Problemwahrnehmung sowie über proklamierte Ansätze, getroffene Maßnahmen und Institutionalisierungen erstellt. Daran anschließend sollen die Herangehensweisen in das Spektrum der Strategien und Konzepte zur Bekämpfung digitaler Desinformation eingeordneten werden. Darüber hinaus gilt es, die Ursachen für die Auswahl der vorliegenden Strategien zu beleuchten, indem die Strukturen, Kompetenzen und das Rollenverständnis beider Organisationen als kollektive Akteure einbezogen werden.

Eine Erwartung kann hierbei lauten, dass die EU als Akteurin mit Schwerpunkt auf normativen und zivilen Machtressourcen eher eine Strategie verfolgt, die passiver ausgerichtet ist und auf Resilienz, *Soft Power* und *Public Diplomacy* vertraut. Die NATO, als Militärbündnis in der Tradition des Kalten Krieges, könnte hingegen womöglich stärker auf eine konfrontative Strategie setzen, die auf Abschreckung, *Hard Power* und *Containment* basiert.

Nach einer vergleichenden Gegenüberstellung und Diskussion der bisherigen Untersuchungsergebnisse in Kapitel 7 richtet Kapitel 8 abschließend den Fokus auf die Zusammenarbeit von EU und NATO im Bereich der hybriden Bedrohungen und der digitalen Desinformation. Von besonderem Interesse ist dabei, wie sich die Kooperation beider Organisationen konkret gestaltet und welche Auswirkungen sich daraus auf ihre jeweiligen Herangehensweisen ableiten. Auch wenn die Kooperation und Koordinierung zwischen EU und NATO eine trennscharfe Unterscheidung der jeweiligen Ansätze erschwert, ergeben sich zugleich interessante Einblicke sowohl in die Arbeitsteilung zwischen kollektiven Akteuren als auch in die daraus resultierende Evolution von Fähigkeiten, Instrumenten und Strategien beider Organisationen.

2 Problematik

Bevor im Detail auf die Vorgehensweisen von EU und NATO gegen Desinformation im digitalen Raum eingegangen werden kann, ist es notwendig, das Phänomen der digitalen Desinformation in seiner gesamten Komplexität zu erfassen und einzugrenzen. In diesem Sinne sollen die folgenden Unterkapitel eine Orientierung darüber geben, was unter dem Begriff der Desinformation zu verstehen ist, welche Erscheinungsformen dazugezählt werden können, wie sich Desinformation im digitalen Raum verhält, welche Gefahren von ihr ausgehen und welche psychologischen als auch technischen Aspekte bei der Problematik eine Rolle spielen. Bei diesem Vorhaben stellen die Neuartigkeit des Phänomens sowie die daraus resultierende Vielfältigkeit von Definitionen und Deutungsversuchen eine besondere Herausforderung dar. Aus diesem Grund zielt Kapitel 2.1 darauf ab, ein gemeinsames Verständnis der Problematik und Terminologie zu etablieren, indem zunächst die gängigen Begrifflichkeiten und Konzepte kritisch-explorativ erschlossen werden. Kapitel 2.2 wird daraufhin den Einfluss des digitalen Raums auf ihre Verbreitung diskutieren. Hierbei liegt ein besonderes Augenmerk auf der besonderen Rolle der sozialen Medien (Kapitel 2.2.1) sowie auf den psychologischen und technischen Aspekten, die zur Wirkungsweise von Desinformation im digitalen Raum beitragen (Kapitel 2.2.2).

2.1 Terminologie: Schlagwörter im Überfluss

> „The words we choose to describe media manipulation can lead to assumptions about how information spreads, who spreads it, and who receives it. These assumptions can shape what kinds of interventions or solutions seem desirable, appropriate, or even possible.“ (Jack 2017: 1)

Der Einfluss problematischer Informationen auf Debatten und die öffentliche Meinungsbildung im Netz erfährt spätestens seit 2016 mit der Kampagne um den Austritt des Vereinigten Königreichs aus der EU und dem US-Präsidentschaftswahlkampf 2016 eine erhöhte Aufmerksamkeit. Die Diskussion beschränkt sich dabei längst nicht mehr auf wissenschaftliche Kreise, sondern hat bereits ihren Weg in die breite Öffentlichkeit und auf die Agenda politischer Entscheidungsträger*innen gefunden.

Im Zuge des gewachsenen wissenschaftlichen, politischen und öffentlichen Interesses explodierte schließlich auch die Vielfalt der Begrifflichkeiten, die versuchen, die neuen Phänomene zu beschreiben, zu analysieren und zu erklären. Unter der Fülle

an gängigen Begriffen und Konzepten tut sich dabei eine Unmenge an Überschneidungen, Abweichungen und Widersprüchen auf, die sowohl die wissenschaftliche als auch die politische Auseinandersetzung mit der Thematik erschweren. Darüber hinaus besteht mit der undifferenzierten Vereinnahmung der Problematik durch Politik und Allgemeinheit das Risiko, dass Begriffe und Konzepte zu *buzzwords* verkommen, die zwar klangvoll sind, deren analytischer Nutzen jedoch vollends verpufft.

Der Anspruch dieser Arbeit kann es dabei nicht sein, eine allgemeingültige Terminologie aufzustellen, vielmehr soll eine begriffliche und konzeptionelle Grundlage geschaffen werden, mit der die Fragestellung unmissverständlich beantwortet werden kann. Ziel dieses Abschnittes wird es deshalb sein, ein eindeutiges Vokabular zu etablieren, mit dem das Phänomen der digitalen Desinformation in seiner Mannigfaltigkeit sinnvoll beschrieben und eingegrenzt werden kann.[7]

Im Sinne der Fragestellung dieser Arbeit ist es jedoch nicht nur wichtig, herauszustellen, welche Begriffe, Definitionen und Konzepte zu der Problematik existieren und verwendet werden (sollten), sondern auch, auf welche davon von EU und NATO Bezug genommen wird. Dies soll an späterer Stelle bei der Analyse der jeweiligen Akteure (Kapitel 5 und 6) im Detail vorgenommen werden. Mit Blick auf die angestrebte Untersuchung der Strategien von EU und NATO kann die Diskussion darüber, wie das Phänomen digitaler Desinformation korrekterweise einzuordnen und zu benennen ist, zunächst als nachrangig eingestuft werden. Von Interesse ist eher, welche Begriffe EU und NATO tatsächlich gebrauchen und welche Konsequenzen aus dieser Benennung für ihren Umgang mit Desinformation entstehen. Gleichwohl wird sich dieses Kapitel zunächst der allgemeinen Beschreibung der Problematik widmen, um einen Rahmen zu bilden, in den das Vorgehen beider Organisationen, ihr Problemzugang und ihre Bedrohungswahrnehmung schließlich eingestuft werden können.

Im Mittelpunkt dieser Arbeit steht der Begriff der **Desinformation**, aber was ist darunter konkret zu verstehen? Kurz gefasst lässt sich Desinformation als falsche oder irreführende Information beschreiben, die zudem auch die *Funktion* hat, in die Irre zu führen (vgl. Fallis 2015: 413). Nach Fallis (2015) zeichnet sich Desinformation demnach durch drei Merkmale aus:

---

[7] Bei Ermangelung gängiger deutscher Übersetzungen werden englische Begriffe im Original belassen.