ANALYSE

Mikhail Polianskii
Dezember 2025

Jenseits der Grauzone:

Europas Weg zu strategischer Klarheit gegen russische hybride Bedrohungen

Friedrich Ebert Stiftung

Impressum

Herausgeberin
Friedrich-Ebert-Stiftung e.V.
Godesberger Allee 149
53175 Bonn
Germany
https://www.russia.fes.de
info.russia@fes.de

Herausgebende Abteilung
International Cooperation Department,
Russia Program of the FES

Inhaltliche Verantwortung und Redaktion
Alexey Yusupov

Bildnachweise
Titelbild: Illustrationen von Freepik.com und Pixabay.com

November 2025

Weitere Publikationen der Friedrich-Ebert-Stiftung finden Sie hier:
↗ https://www.fes.de/publications

Friedrich Ebert Stiftung

Mikhail Polianskii
Dezember 2025

Jenseits der Grauzone:

Europas Weg zu strategischer Klarheit gegen russische hybride Bedrohungen

Inhalt

Begriffspräzision: Wenn »hybrid« zum Allzweckbegriff wird 4

Wortwahl und Eskalation: Die politischen Kosten der Kriegsrhetorik 5

Zwischen Sicherheit und Freiheit: Praktische Gegenmaßnahmen
und demokratische Schranken 7

Fazit 8

Jenseits der Grauzone:

Europas Weg zu strategischer Klarheit gegen russische hybride Bedrohungen

Europa sieht sich einer beispiellosen Eskalation böswilliger Aktivitäten gegenüber, die häufig russischen staatlichen und nichtstaatlichen Akteuren zugeschrieben werden und die traditionellen Grenzen zwischen Frieden und Krieg verwischen.[1] Allein in Deutschland meldete das Bundeskriminalamt (BKA) für das Jahr 2024 131.391 Cyberstraftaten im Inland sowie weitere 201.877 Straftaten aus dem Ausland.[2] Der Digitalverband Bitkom beziffert den jährlichen Schaden für deutsche Unternehmen auf 178,6 Milliarden Euro.[3] »Hybride Kriegsführung« hat sich als Sammelbegriff für ein breites Spektrum von Bedrohungen etabliert,[4] die sich gegen Deutschland und seine europäischen Verbündeten richten – von den genannten Cyberangriffen über Brandvorrichtungen an Frachtflugzeugen bis hin zur Sabotage von Seekabeln.[5] Doch gerade die weite Verbreitung dieses Begriffs, der in der Wissenschaft seit fast zwei Jahrzehnten kontrovers diskutiert und zunehmend in der politischen Debatte übernommen wird, schafft eine zusätzliche Begriffsunschärfe.

Während sich durch Russland geförderte böswillige Aktivitäten in Europa ausweiten, stehen die europäischen Entscheidungsträger:innen vor einem dringenden Dilemma: Wie lassen sich diese Bedrohungen angemessen kategorisieren und wirkungsvolle Gegenmaßnahmen entwickeln, ohne die demokratischen Werte und die Stabilität dabei zu untergraben? Die vorliegende Analyse untersucht diese konzeptionellen und praktischen Herausforderungen unter drei zentralen Gesichtspunkten: Begriffspräzision, Eskalationsdynamik und Demokratieschutz. Aus der Zusammenführung dieser Perspektiven ergibt sich eine Reihe von politischen Handlungsempfehlungen, wie Europa die Grauzone zwischen Frieden und offenem Konflikt strategischer begehen kann, ohne Sicherheit und Demokratie gegeneinander auszuspielen.

Erstens wird gezeigt, dass terminologische Präzision unmittelbar die Effektivität politischer Maßnahmen beeinflusst. Wenn jeder Cyberangriff, jede Desinformationskampagne oder jede Form wirtschaftlicher Nötigung unter dem weiten Dach der »hybriden Kriegsführung« subsumiert wird, verringert das die analytische Aussagekraft und begünstigt Fehlallokationen knapper Ressourcen.[6] Die Analyse plädiert deshalb für einen nuancierten Ansatz, den ich als »analytischen Föderalismus« bezeichne. Dieser Ansatz erkennt differenzierte Subkategorien von Angriffen in den Bereichen Cyber, Information, Physisches und weitere Domänen an, die jeweils eigene Betrachtung und spezifische Reaktionen erfordern. Ein derartiges Rahmenwerk könnte erleichtern, Gegenmaßnahmen passgenau zu gestalten und die Abstimmung zwischen Akteuren aus Verteidigung, Nachrichtendiensten und Diplomatie zu optimieren.

Zweitens wird argumentiert, dass europäische Entscheidungsträger:innen bei der Verwendung kriegsbezogener Terminologie gegenüber hybriden Bedrohungen äußerste Zurückhaltung walten lassen sollten – aufgrund ihrer tiefgreifenden politischen und eskalatorischen Während einige europäische Führungspersönlichkeiten die zunehmenden hybriden Angriffe bereits als de facto Kriegszustand sehen, beschreiben die meisten die aktuelle Lage weiterhin als eine »Grauzone« zwischen Frieden und offenem Konflikt.[7] Die Analyse erläutert die politischen Folgen solcher begrifflichen Entscheidungen und zeigt auf, wie sie direkt Eskalationsdynamiken, kollektive Verteidigungsmechanismen und den Zusammenhalt beeinflussen können.

Drittens richtet sich das Augenmerk auf die praktischen Gegenmaßnahmen Europas und deren Wirkung auf die demokratischen Werte. Harter Durchgriff – etwa in Form von Medieneinschränkungen, ausgeweiteten Überwachungsbefugnissen oder repressiver Gesetzgebung – mag kurzfristig plausibel erscheinen, droht aber langfristig Freiheitsrechte auszuhöhlen und damit mittelbar den strategischen Zielen Moskaus Vorschub zu leisten. Gelingende Gegenstrategien müssen daher demokratische Widerstandsfähigkeit stärken: durch konsequente Faktenprüfung, systematische politische Bildung und den Ausbau gesellschaftlicher Resilienz über verstärkte zivilgesellschaftliche Partizipation.

1 Vgl. Juraj Majcin (2025): Russia's threat to Europe goes beyond the battlefields of Ukraine, European Policy Centre, 2025; verfügbar unter: https://www.epc.eu/publication/Russias-threat-to-Europe-goes-beyond-the-battlefields-of-Ukraine-6101fc

2 Bundeslagebild Cybercrime (2024): BKA setzt anhaltend hoher Cyberbedrohung zahlreiche Ermittlungserfolge entgegen. BKA; verfügbar unter: https://www.bka.de/DE/AktuelleInformationen/StatistikenLagebilder/Lagebilder/Cybercrime/2024/CC_2024.html

3 Bitkom (2024): Wirtschaftsschutz; verfügbar unter: https://www.bitkom.org/Bitkom/Publikationen/Studie-Wirtschaftsschutz

4 Der Deutsche Bundestag (2025) Neues Lagebild zu hybriden Bedrohungen, 2025; verfügbar unter: https://www.bundestag.de/presse/hib/kurzmeldungen-1103890?utm_source=substack&utm_medium=email

5 Vgl. NATO (2024): Countering hybrid threats, 7. Mai; verfügbar unter: https://www.nato.int/cps/en/natohq/topics_156338.htm

6 Vgl. Dan G. Cox, Thomas Bruscino and Alex Ryan (2012): Why hybrid warfare is tactics not strategy, Military Strategy Magazine, 4. April; verfügbar unter: https://www.militarystrategymagazine.com/article/why-hybrid-warfare-is-tactics-not-strategy

7 Vgl. Andre Bodeman (2025): Deutschland schon lange nicht mehr im Frieden, BR24; verfügbar unter: https://www.br.de/nachrichten/deutschland-welt/general-leutnant-deutschland-schon-lange-nicht-mehr-im-frieden,Ua8q55u

Diese drei Dimensionen sind eng miteinander verzahnt: Begriffspräzision ermöglicht angemessene Antworten, angemessene Antworten vermeiden unnötige Eskalationen, und das Vermeiden von Eskalation sichert den politischen Raum für demokratische Selbststeuerung. Zusammengenommen leisten sie den Beitrag zu einer kohärenteren europäischen Strategie im Zeitalter anhaltender Grauzonen-Konflikte.

Begriffspräzision: Wenn »hybrid« zum Allzweckbegriff wird

In den letzten Jahren hat sich in der europäischen Sicherheitsdebatte der Begriff »hybride Kriegsführung« zunehmend zum selbstverständlichen Begriff gewandelt. Diese weite Verbreitung hat jedoch ein Paradox geschaffen: Nur wenige Akteure sind sich darüber einig, was der Begriff tatsächlich umfasst, und noch weniger können plausibel darlegen, wie unterschiedliche Begriffsauffassungen zu verschiedenen politischen Maßnahmen führen sollten.[8] Diese konzeptuelle Aufblähung bringt praktische Probleme für Entscheidungsträger:innen mit sich, die zunehmend Schwierigkeiten haben, zwischen grundsätzlich verschiedenen Bedrohungsarten zu unterscheiden – Bedrohungen, die jeweils eigene Gegenreaktionen erfordern.

Das Problem tritt deutlich zutage, wenn man die institutionelle Verwirrung betrachtet, die die definitorische Pluralität in den europäischen Staaten stiftet. Die NATO charakterisiert »hybride Kriegsführung« als »militärische und nicht-militärische sowie verdeckte und offene Mittel (einschließlich Desinformation, Cyberangriffen, wirtschaftlichem Druck, Einsatz irregulärer bewaffneter Gruppen und Einsatz regulärer Streitkräfte), um die Grenze zwischen Krieg und Frieden zu verwischen und Gesellschaften zu destabilisieren und zu untergraben«.[9] Die EU hingegen wendet einen weiter gefassten Ansatz an und definiert hybride Bedrohungen als »koordinierte schädliche Aktivitäten, die mit böswilliger Absicht geplant und durchgeführt werden«.[10]

Diese definitorischen Differenzen spiegeln tiefere intellektuelle Debatten innerhalb der Forschung zu hybrider Kriegsführung wider, die seit mehreren Jahren geführt werden. Das NATO-Verständnis steht näher an der Sichtweise von Frank Hoffman, dem intellektuellen Urheber des Konzepts und ehemaligen US-Marine, dessen einflussreiche Studie von 2007 hybride Kriegsführung als »ein Spektrum unterschiedlicher Kriegsführungsformen, einschließlich konventioneller Fähigkeiten, irregulärer Taktiken und Formationen, terroristischer Akte und krimineller Unordnung« beschrieb, die für einen synergistischen Effekt koordiniert werden«.[11] Europäische Politiker:innen neigen demgegenüber eher zu Definitionen, die denen zeitgenössischer Wissenschaftler:innen ähneln, welche betonen, dass hybride Bedrohungen praktisch jede politische Aktivität umfassen können, die einer Sicherheitslogik unterzogen (securitisiert) werden kann.[12]

Diese Differenz in den akademischen Grundlagen erklärt, warum die NATO sich auf militärisch-politische Schwellen (Krieg vs. Frieden) fokussiert, während EU-Ansätze stärker auf gesamtgesellschaftliche Koordination und Resilienz setzen. Die institutionelle Verwirrung ist demnach nicht nur bürokratischer Natur, sondern resultiert aus grundverschiedenen wissenschaftlichen Traditionen, die dem Gebrauch des Begriffs »hybride Kriegsführung« zugrunde liegen. Das führt mitunter dazu, dass die Verwendung dieses Begriffs die Lage eher weiter verschleiert als erklärt. Die Verbreitung dieses Begriffs in politischen Debatten über die »russische hybride Bedrohung« hat daher gelegentlich zu dem geführt, was man oft als »kategorische Verwirrung« bezeichnet: Entscheidungsträger:innen glauben, dieselbe Sprache zu sprechen, während ihre Worte in Wirklichkeit unterschiedliche Bedeutungen tragen.[13]

Besonders bemerkenswert ist, dass selbst engste europäische Verbündete öffentlich aneinander vorbeireden, wenn sie die gegenwärtigen russischen hybriden Bedrohungen diskutieren. Frankreichs Generalstabschef Thierry Burkhard betont, dass »die NATO, die eine defensive Militärallianz ist und in Begriffen von Friedens- und Kriegszeiten denkt«, nicht über Instrumente verfüge, »die für die Grauzone des Wettbewerbs und der Auseinandersetzung ausgelegt sind«. In demselben Politico-Interview unterstreicht der ehemalige deutsche Verfassungsschutzpräsident Thomas Haldenwang hingegen die Notwendigkeit, wirksame Antworten auf Russlands »Werkzeugkasten [hybrider Angriffe] von der Beeinflussung politischer Debatten über Cyberangriffe auf kritische Infrastrukturen bis hin zu Sabotage in erheblichem Umfang« zu entwickeln.[14] Die beiden Amtsträger beschreiben also dasselbe Phänomen aus völlig verschiedenen Perspektiven – die eine hebt die Ambivalenz der Grauzone (Krieg vs. Frieden) hervor, die andere die gesamte Bandbreite hybrider Angriffe. Ohne einen zentralisierten strategischen Dialog über hybride Bedrohungen zwischen den wichtigsten europäischen

8 Vgl. James Wither (2023): Hybrid Warfare Revisited: A Battle of ›Buzzwords‹, Connections QJ, 22(1), pp. 7–27; verfügbar unter: doi: 10.11610/Connections.22.1.02.

9 Vgl. NATO (2024): Countering hybrid threats, 7. Mai; verfügbar unter: https://www.nato.int/cps/en/natohq/topics_156338.htm

10 European Council (2025): Hybrid threats; verfügbar unter: https://www.consilium.europa.eu/en/policies/hybrid-threats

11 Frank G. Hoffman (2007): Conflict in the 21st Century: The Rise of Hybrid Wars, Potomac Institute for Policy Studies

12 Vgl. Andrew Mumford, and Pascal Carlucci (2023): Hybrid warfare: The continuation of ambiguity by other means, European Journal of International Security, 8(2), pp. 192–206; verfügbar unter: doi: 10.1017/EIS.2022.19

13 Vgl. Colin S. Gray (2020): Categorical Confusion? The Strategic Implications of Recognizing Challenges Either as Irregular or Traditional, Strategic Studies Institute Monograph, US Army War College; verfügbar unter: https://press.armywarcollege.edu/monographs/561

14 Beide zitiert in: Laura Kayali (2024): Europe is under attack from Russia. Why isn't it fighting back?, Politico, 25. November; verfügbar unter: https://www.politico.eu/article/europe-russia-hybrid-war-vladimir-putin-germany-cyberattacks-election-interference

Mächten ist zu erwarten, dass sie weiterhin divergierende politische Prioritäten verfolgen, die Russland gezielt ausnutzen kann.

Das Präzisionsproblem wird besonders gravierend, wenn jeder Vorfall pauschal als »hybride Kriegsführung« etikettiert wird, ohne auf seine spezifischen Merkmale einzugehen.[15] Werden Desinformationskampagnen, physische Sabotageakte und Cybervorfälle in einem einzigen Rahmen zusammengefasst, verlieren Entscheidungsträger:innen den Blick für die je unterschiedlichen Verwundbarkeiten, die ausgenutzt werden, und für die jeweils erforderlichen Gegenmaßnahmen. Cyberangriffe auf kritische Infrastruktur verlangen etwa technische Abwehrmaßnahmen, internationale Kooperation bei der Attribution und gegebenenfalls offensive Cybermaßnahmen.[16] Desinformationskampagnen erfordern hingegen strategische Kommunikationsarbeit, Medienkompetenzprogramme und zielgerichtete Sanktionen gegen Propagandastrukturen. Physische Sabotage bedarf verstärkter Sicherheitsvorkehrungen, nachrichtendienstlicher Zusammenarbeit und klassischer polizeilicher Ermittlungsarbeit. Jeder dieser Angriffsvektoren verfügt also über eigene Merkmale, nutzt andere Schwachstellen aus und spricht auf spezifische Gegenmaßnahmen an. Werden diese Unterschiede unter dem Sammelbegriff »hybride Kriegsführung« verwischt, führt das allzu oft zu Fehlallokationen, zu generischen statt zielgerichteten Reaktionen und zu Koordinationsproblemen, weil Behörden nicht klar ist, welche Rolle sie konkret übernehmen sollen.

Die praktische Lösung kann aber nicht darin bestehen, den Begriff »hybride Kriegsführung« gänzlich aufzugeben – wie einige Analysten gefordert haben. Vielmehr sollten Politik und Analyse erwägen, einen »analytischen Föderalismus« einzuführen: den Begriff des »hybriden Krieges« als strategischen Oberbegriff beizubehalten, zugleich aber präzise Unterkategorien für die operative Planung zu schaffen. Das würde es europäischen Entscheidungsträger:innen erleichtern, zwischen cyberbasierten Hybridbedrohungen (die technische Antworten erfordern), informationsbasierten Bedrohungen (die Kommunikationsmaßnahmen erfordern) und kinetischen Bedrohungen (die konventionelle Sicherheitsmaßnahmen benötigen) zu differenzieren.

Zusammenfassend ist der Begriff »hybride Kriegsführung« problematisch und wird es voraussichtlich auch noch Jahrzehnte bleiben. Seine weite Verbreitung zeigt jedoch, dass er einem echten analytischen Bedürfnis entspricht, wenn es darum geht, die gegenwärtigen Angriffe auf europäischem Boden – etwa aus Russland – zu beschreiben. Ein stärker vereinheitlichter Meta-Begriff, erreicht durch strategischen Dialog, kombiniert mit größerer analytischer Präzision auf operativer Ebene, könnte entscheidend sein, um effektivere Politikgestaltung und eine gezieltere Ressourcenverteilung zu ermöglichen. Ein solches Rahmenwerk würde europäischen Politiker:innen helfen zu erkennen, wie einzelne Angriffe in breitere Strategien eingebettet sind und zugleich angemessen auf die spezifischen Charakteristika jedes Angriffs zu reagieren. Diese analytische Grundlage gewinnt zusätzlich an Gewicht, wenn man die Eskalationsdynamiken bedenkt, die begriffliche Entscheidungen auslösen können. Darauf geht der folgende Abschnitt ein.

Wortwahl und Eskalation: Die politischen Kosten der Kriegsrhetorik

Die Investigative Journalism Network der Europäischen Rundfunkunion hat seit 2022 Hunderte bestätigter oder mutmaßlicher russischer Aktivitäten gegen Europa dokumentiert – von Brandvorrichtungen in DHL-Frachtmaschinen, »so stark, dass sie ein Frachtflugzeug hätten zum Absturz bringen können«, über durchtrennte Seekabel, die die Kommunikation im Ostseeraum störten,[17] bis hin zu GPS-Spoofing mit Auswirkungen auf die zivile Luftfahrt und hochentwickelten Cyberangriffen auf kritische Infrastrukturen.[18] Einzelne Vorfälle mögen auf den ersten Blick relativ begrenzt erscheinen; ihre summative Wirkung wirft jedoch eine grundlegende Frage auf: Stellen diese Handlungen zusammengenommen de facto einen nicht erklärten Krieg dar?[19]

Die Art und Weise, wie europäische Entscheidungsträger:innen diese Frage beantworten, hat weitreichende Folgen, die weit über semantische Präferenzen hinausreichen.[20] Die Entscheidung, kriegsbezogene Terminologie zu verwenden – oder bewusst zu vermeiden – kann unmittelbar Eskalationsdynamiken, kollektive Verteidigungsmechanismen und innenpolitische Unterstützung beeinflussen.

Die politischen Kosten scharfer Kriegsrhetorik wurden besonders deutlich in der Kontroverse um die Aussage der damaligen deutschen Außenministerin Annalena Baerbock, »wir führen einen Krieg gegen Russland«, geäußert bei einer Sitzung des Europarats. Die Bundesregierung sah sich umgehend gezwungen zu präzisieren, dass Baerbock die Unterstützung der ukrainischen Verteidigung meinte und damit keine Erklärung eines direkten Kriegszustands beabsichtigte, nachdem kritisiert worden war, ihre Äußerung

15 Vgl. Alina Bârgăoanu and Elena Negrea-Busuioc (2024): Hybrid warfare is less than warfare: a dangerous illusion, Irregular Warfare Center; verfügbar unter: https://irregularwarfarecenter.org/wp-content/uploads/P_19_Hybrid_Warfare_is_Less_Than_Warfare.pdf

16 Mikhail Polianskii (2025): Digitale Zeitenwende: Aktive Cyberabwehr als Antwort auf Russlands hybride Kriegsführung, PRIF-Spotlight 6; verfügbar unter https://blog.prif.org/en/2025/07/16/digitale-zeitenwende-aktive-cyberabwehr-als-antwort-auf-russlands-hybride-kriegsfuehrung

17 CNN (2024): Baltic Sea internet cables cut: European officials cry sabotage, 19. November; verfügbar unter: https://www.cnn.com/2024/11/18/europe/undersea-cable-disrupted-germany-finland-intl

18 EBU Investigative Journalism Network (2025): Playing with fire: EBU investigates Russia's hybrid attacks on Europe, 12. März; verfügbar unter: https://investigations.news-exchange.ebu.ch/playing-with-fire-are-russias-hybrid-attacks-the-new-european-war

19 Vgl. Center for Strategic and International Studies (2025): Russia's Shadow War Against the West, 18. März; verfügbar unter: https://www.csis.org/analysis/russias-shadow-war-against-west

20 Vgl. Lawrence Freedman (2023): The Language of War; verfügbar unter: https://samf.substack.com/p/the-language-of-war

könne dahingehend missverstanden werden, Deutschland sei nun Kriegspartei.[21]

Dieser Vorfall verdeutlicht, wie kriegsbezogene Sprache strategische Verwirrung stiften kann, wenn Worte nicht mit politischem Handeln übereinstimmen. Das untergräbt sowohl innenpolitische Glaubwürdigkeit als auch internationale Koordination. Wenn einzelne europäische Führungspersonen zur Kriegsrhetorik greifen, während die NATO zugleich betont, sie »sei nicht im Krieg mit Russland«, entsteht eine Dissonanz, die unter den Verbündeten Verunsicherung sät und Moskau Raum für die Verbreitung seiner Propagandanarrative bietet.[22] Die russische Propaganda instrumentalisiert diese Verwirrung in zweifacher Hinsicht: erstens, indem sie zugespitzte westliche Äußerungen aus dem Kontext reißt, um eine Eskalation zu rechtfertigen; zweitens, indem sie anschließend europäische Dementis als Beleg vermeintlicher Schwäche darstellt.[23]

Die Risiken eines missbräuchlichen Gebrauchs kriegsbezogener Terminologie reichen jedoch über Propagandakämpfe hinaus. Wenn Medien und Entscheidungsträger:innen in Europa fortwährend von »Krieg« sprechen – ergänzt durch das Etikett »hybrid« oder nicht – und Vergeltung fordern,[24] können gefährliche Echokammer entstehen, in denen jede Seite behauptet, die Gegenseite habe die Kriegsschwelle überschritten. Diese Dynamik kann Eskalations- und Gegeneskalationszyklen in Gang setzen und das Risiko eines Fehlers deutlich erhöhen, der eine reale militärische Konfrontation auslösen könnte. Wie Daniel Byman vom CSIS zurecht anmerkt, sollten europäische Führungskräfte bei der Diskussion über Formen der Durchführung eines »hybriden Krieges« gegen Russland äußerste Vorsicht walten lassen, sonst könnten sie »in einen Konflikt hineingezogen werden, auf den sie nicht vorbereitet sind«.[25]

Kollektive Verteidigungsmechanismen fügen für NATO-Mitglieder in Europa eine weitere Komplexitätsebene hinzu. Auf dem Gipfel von Vilnius 2023 erklärte das Bündnis, »hybride Operationen gegen Bündnispartner könnten das Niveau eines bewaffneten Angriffs erreichen und den Rat dazu veranlassen, Artikel 5 des Washingtoner Vertrags auszurufen«.[26] Artikel 5 bleibt jedoch bekanntermaßen vage und spricht lediglich von » Maßnahmen ... die sie [Mitgliedstaaten] für erforderlich erachtet« – eine Formulierung, die großen Interpretationsspielraum eröffnet.[27] Während strategische Ambiguität wichtige Zwecke erfüllt[28] – indem sie die Planungen Moskaus auf mehreren Ebenen erschwert – legt das bisher beobachtete russische Verhalten nahe, dass diese Unsicherheit Moskau nicht wesentlich abschreckt. Der Kreml hat erkannt, dass es keine automatischen Mechanismen zur Auslösung von Artikel 5 bei hybriden Angriffen gibt, und hat bislang erfolgreich Grenzen unterhalb definierter Schwellen getestet, wodurch Lücken in der Abschreckungsarchitektur der NATO offenkundig wurden.[29]

Vor diesem Hintergrund argumentieren manche Kritiker in politischen Kreisen, die derzeitige Begrifflichkeit des »hybriden Krieges« reiche nicht aus, um russische Angriffe ausreichend abzuschrecken. Der ehemalige litauische Außenminister Gabrielius Landsbergis etwa forderte: »Wenn Russland in direkte kinetische Angriffe [in Europa] verwickelt ist, sollten wir dafür einen anderen Namen finden. Ich würde es lieber als staatlich unterstützten Terroranschlag, bezeichnen«.[30] Auch die dänische Ministerpräsidentin Mette Frederiksen meinte: »Wir sind einfach zu höflich (wenn wir es »hybrid‹ nennen)«.[31] Beide sehen in der verhüllenden Sprache ein Hindernis, das die Ernsthaftigkeit der Lage verschleiert und Russland ermöglicht, seine Aggression ohne Furcht vor robusten Gegenmaßnahmen fortzusetzen.

Der künftige Kurs muss ein ausgewogenes Verhältnis zwischen bewusst gewahrter Unklarheit über endgültige Antwortoptionen und klaren, gestuften Maßnahmen gegen spezifische Arten hybrider Angriffe finden. Indem man innerhalb des vorgeschlagenen »analytischen Föderalismus« präzise Gegenmaßnahmen entwickelt – symmetrische und adäquate Reaktionen für cyberbasierte, informationsbasierte, wirtschaftliche und kinetische Hybridbedrohungen – können europäische Führungskräfte die kollektive Abschreckung stärken, ohne in eine tückische Eskalationsspirale mit Russland hineingezogen zu werden. Ein solches ausgewogenes Vorgehen würde die strategische Flexibilität schaffen, die nötig ist, um russischer hybrider Aggression auf allen Ebenen wirksam zu begegnen und gleichzeitig die demokratischen Schranken zu wahren, denen solche Maßnahmen unterliegen müssen. Darauf wird im vorletzten Abschnitt ausführlich eingegangen.

21 Deutsche Welle (2023): Germany says it is not a warring party in Ukraine, 27. Januar; verfügbar unter: https://www.dw.com/en/germany-says-it-is-not-a-warring-party-in-ukraine/a-64541484

22 NATO (2024): Setting the record straight: de-bunking Russian disinformation on NATO, NATO HQ; verfügbar unter: https://www.nato.int/cps/en/natohq/115204.htm

23 Vgl. Sergey Lavrov (2025): Virtually all of Europe is at war against Russia, TASS; verfügbar unter: https://tass.ru/politika/23862257

24 Europe is under attack from Russia. Why isn't it fighting back?, Politico, 25. November 2024; verfügbar unter: https://www.politico.eu/article/europe-russia-hybrid-war-vladimir-putin-germany-cyberattacks-election-interference

25 Ibid.

26 NATO Vilnius Summit Communiqué, 11. Juli 2023. Section 64; verfügbar unter: https://www.nato.int/cps/en/natohq/official_texts_217320.htm

27 Eitvydas Bajarūnas (2025): Using NATO's Article 5 Against Hybrid Attacks, CEPA, 13. Februar; verfügbar unter: https://cepa.org/article/using-natos-article-5-against-hybrid-attacks

28 Vgl. War in Ukraine: Strategic Ambiguity finds renewed significancy in 21st-century Nuclear Deterrence, Le Monde; verfügbar unter: https://www.lemonde.fr/en/opinion/article/2022/11/28/war-in-ukraine-strategic-ambiguity-finds-renewed-significance-in-21st-century-nuclear-deterrence_6005911_23.html

29 Vgl. Viktorija Rusinaitė (2025): Turning strategy into praxis: Lessons in hybrid threat deterrence, Hybrid CoE; verfügbar unter: https://www.hybridcoe.fi/publications/turning-strategy-into-praxis-lessons-in-hybrid-threat-deterrence

30 Lithuanian Ministry of Foreign Affairs (2024): Landsbergis at the NATO summit, 12. Juli; verfügbar unter: https://www.urm.lt/en/news/928/landsbergis-at-the-nato-summit-a-very-strong-message-is-being-sent-to-moscow:42922

31 Quoted in »Europe is under attack from Russia. Why isn't it fighting back?«,

Zwischen Sicherheit und Freiheit: Praktische Gegenmaßnahmen und demokratische Schranken

Europas Auseinandersetzung mit russischen Hybridbedrohungen erzeugt ein grundlegendes Dilemma: Wie lassen sich robuste Abwehrmaßnahmen entwickeln, ohne die Freiheiten und demokratische Prinzipien zu untergraben? Dieses Problem ist von besonderer Tragweite, weil ein zentrales Ziel russischer Hybridkampagnen darin besteht, demokratische Normen gezielt zu schwächen – indem das Vertrauen in Institutionen, Pressefreiheit und Rechtsstaatlichkeit beschädigt wird.[32]

Die Versuchung zu harten Gegenmaßnahmen ist nachvollziehbar, wenn Demokratien anhaltenden hybriden Angriffen ausgesetzt sind. Desinformationskampagnen rufen nach erweiterten Befugnissen in der Inhaltsmoderation, die sich jedoch leicht missbrauchen lassen, um legitime Kritik und abweichende Meinungen zu unterdrücken.[33] Cyberangriffe erfordern zwar entschlossenes Handeln, können aber zugleich als Vorwand dienen, Überwachungsbefugnisse auszuweiten und damit Datenschutz sowie Privatsphäre auszuhöhlen. Auch ausländische Einflussoperationen erzeugen Druck, zivilgesellschaftliche Organisationen, wissenschaftliche Kooperationen und internationalen Austausch – das Rückgrat offener Gesellschaften – einzuschränken.[34] Jede dieser Maßnahmen mag kurzfristig Schutz bieten; langfristig jedoch besteht die Gefahr, dass Demokratien sich schrittweise in Systeme verwandeln, die jenen autoritären Regimen ähneln, gegen die sie sich eigentlich verteidigen.

Genau hierin liegt die strategische Falle, die Moskau bewusst stellt: Reagieren europäische Demokratien auf hybride Bedrohungen, indem sie ihre eigenen Freiheitsräume einschränken, erringt Russland einen strategischen Sieg – unabhängig davon, ob die ursprünglichen Angriffe erfolgreich waren. Russische hybride Kriegsführung zielt nicht nur auf unmittelbare taktische Erfolge, sondern vor allem darauf, Überreaktionen zu provozieren, die demokratische Institutionen über die Zeit schwächen.

Das Beispiel Polen veranschaulicht diese Dynamik: Die früheren Versuche der Regierungspartei PiS, die öffentlich-rechtlichen Medien zu kontrollieren und ausländische Eigentumsanteile an Verlagen zu begrenzen, weckten gewichtige Bedenken hinsichtlich Pressefreiheit und demokratischer Kontrolle.[35] Zwar wurden solche Maßnahmen mit dem Ziel gerechtfertigt, ausländischen Einfluss und Desinformation – darunter auch aus Russland – zu bekämpfen; Kritiker warnten jedoch früh davor, dass die Instrumente gegen die innenpolitische Opposition instrumentalisiert werden könnten.[36] Befugnisse, die vordergründig der Abwehr hybrider Bedrohungen dienten, blieben nicht auf diesen Zweck beschränkt und wurden teils als parteipolitische Steuerungsinstrumente benutzt, was die demokratische Rechenschaftspflicht unterminierte.

Ähnliche Herausforderungen stellen sich auf europäischer Ebene, etwa durch den Digital Services Act. Zwar zielt die Verordnung darauf ab, Desinformation und ausländische Manipulationen einzudämmen; zugleich räumt sie Plattformen und Regulierungsbehörden weitreichende Befugnisse zur Entfernung als schädlich oder irreführend eingestufter Inhalte ein.[37] Kritiker warnen, dies könne den Boden für umfassende Zensur bereiten und rechtmäßige, wahre Meinungsäußerungen unter dem Vorwand von Compliance und Sicherheit einschränken.[38] Die eigentliche Herausforderung besteht also darin, zwischen gezielten, fremdgesteuerten Manipulationskampagnen und legitimer politischer Auseinandersetzung zu unterscheiden – eine Aufgabe, die in polarisierten Gesellschaften zunehmend schwerfällt, wenn unbequeme Informationen reflexhaft als »Desinformation« oder »Fakenews« abgetan werden.[39]

Solche reaktiven Maßnahmen liefern dem Kreml genau die Munition, die er für seine Propaganda benötigt. Russische Staatsmedien instrumentalisieren westliche Einschränkungen von Meinungs- und Pressefreiheit als Beleg dafür, dass demokratische Werte in Europa nur Fassade seien. Maßnahmen gegen Sender wie RT oder Sputnik werden wiederholt als Beweis für Heuchelei angeführt: Moderation von Inhalten und verstärkte Überwachung seien kaum von autoritärem Vorgehen zu unterscheiden.[40] Auch wenn dies die russische Propaganda keineswegs rechtfertigt, wären flächendeckende Verbote russischer und anderer ausländischer Sender kontraproduktiv: Sie nähren Polarisierung, erzeugen neue Konflikte und entfremden womöglich die Zielgruppen, die man eigentlich erreichen will.

32 Vgl. Carol Atkinson (2018): Hybrid Warfare and Societal Resilience: Implications for Democratic Governance, Information & Security: An International Journal, 39(1), pp. 63–76; verfügbar unter: doi: 10.11610/ISIJ.3906.

33 Jon Bateman and Dean Jackson (2024): Countering Disinformation Effectively: An Evidence-Based Policy Guide; verfügbar unter: https://carnegieendowment.org/research/2024/01/countering-disinformation-effectively-an-evidence-based-policy-guide?lang=en&utm

34 Vgl. The Civil Society State of Union 2024 – Report; verfügbar unter: https://civilsocietyeurope.eu/wp-content/uploads/2023/09/CSE-State-of-the-Union-DIGITAL-accessible-in-progress.pdf

35 Reuters (2021): EU voices concern over Polish media bill, impact on press freedom; verfügbar unter: https://www.reuters.com/business/media-telecom/eu-voices-concern-over-polish-media-bill-impact-press-freedom-2021-12-20

36 Agata Pyka (2025): Resisting foreign interference: Poland's presidential election and the Russian challenge, New Eastern Europe; verfügbar unter: https://neweasterneurope.eu/2025/06/10/resisting-foreign-interference-polands-presidential-election-and-the-russian-challenge/#:~:text=Based%20on%20those%20measures%2C%20Poland,if%20necessary%2C%20take%20it%20down

37 European Commission, Digital Services Act, 2022; verfügbar unter: https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package

38 Adina Portaru (2025): Unpacking the EU Digital Services Act, ADF International, 28. Januar; verfügbar unter: https://adfinternational.org/commentary/eu-digital-services-act-one-year#:~:text=The%20EU%20Digital%20Services%20Act's,principles%20it%20claims%20to%20protect

39 Ibid.

40 The EU's "Ban" on RT and Sputnik: A Lawful Measure against Propaganda for War, Verfassungsblog, 8. März 2022; verfügbar unter: https://verfassungsblog.de/the-eus-ban-of-rt-and-sputnik

Der Weg nach vorn muss daher über gezielte, verhältnismäßige Maßnahmen führen, die demokratische Institutionen stärken, statt sie zu schwächen. Das verlangt eine sorgfältige Ausgestaltung von Gegen-Hybrid-Strategien mit klaren gesetzlichen Schranken, unabhängiger Aufsicht und transparenter Kommunikation über Notwendigkeit, Umfang und ggf. Befristung der Maßnahmen. Effektive Antworten sollten nicht den demokratischen Raum beschneiden, sondern ihn erweitern: durch Förderung von Medienkompetenz, den Ausbau von Fact-Checking Kapazitäten und die Stärkung gesellschaftlicher Resilienz über verstärkte zivilgesellschaftliche Beteiligung.

Indem Europa auf Angriffe gegen Demokratie mit mehr Demokratie antwortet, kann es Moskau sowohl die unmittelbaren taktischen Ziele als auch das übergeordnete strategische Ziel der Legitimationsuntergrabung verwehren. Die Herausforderung besteht darin, die moralische und politische Autorität unter gezielten Angriffen von Moskau zu bewahren – und zugleich sicherzustellen, dass Abwehrmaßnahmen demokratische Institutionen stärken statt sie auszuhöhlen.

Fazit

Die drei in dieser Analyse untersuchten Dimensionen sind eng miteinander verknüpft und können zusammen ein stimmiges Rahmenwerk für eine europäische Strategie im Zeitalter der »Grauzonen«-Konflikte bilden. Begriffspräzision ermöglicht angemessene Antworten, weil sie klärt, welche Bedrohungen welche Maßnahmen erfordern – nicht zuletzt durch den hier vorgeschlagenen »analytischen Föderalismus« Ansatz. Angemessene Antworten tragen dazu bei, unnötige Eskalationen zu vermeiden, indem Mittel und Zwecke besser aufeinander abgestimmt und der Zusammenhalt der Allianz gewahrt werden. Und das Vermeiden von Eskalation sichert den politischen Raum für demokratische Regierungsfähigkeit, weil so krisengetriebener Autoritarismus verhindert wird – genau jenes Ergebnis, das Moskaus Strategie anstrebt.

Die europäische Strategie bei der Bekämpfung hybrider Bedrohungen sollte – und muss in der Praxis – ganzheitlich statt sektoral angelegt sein. Begriffsfragen lassen sich nicht losgelöst von Eskalationsfragen behandeln, und Resilienz kann nicht aufgebaut werden, ohne die demokratischen Schranken zu berücksichtigen. Der vorgeschlagene »analytische Föderalismus« bietet hierfür einen praktikablen Weg: Er belässt »hybride Kriegsführung« als strategischen Integrationsbegriff, schafft zugleich aber präzise Unterkategorien für die operative Planung. Auf diese Weise werden zielgerichtete Gegenmaßnahmen möglich, die spezifische Verwundbarkeiten adressieren, ohne unnötige Eskalation auszulösen oder demokratische Werte zu kompromittieren.

Klare Begriffe ermöglichen klare Entscheidungen – und klare Entscheidungen ermöglichen wirksame Strategien. In einer Zeit, in der konzeptuelle Verwirrung vor allem jenen nützt, die darauf abzielen, demokratische Regierungsfähigkeit und europäische Sicherheit zu untergraben, ist solche Klarheit sowohl analytisches Gebot als auch strategische Notwendigkeit. Es geht hier nicht nur um akademische Debatten, sondern um die grundsätzliche Frage, wie demokratische Gesellschaften sich neuen Formen der Auseinandersetzung anpassen können, ohne ihren unverzichtbaren Charakter preiszugeben.

Über den Autor

Dr. **Mikhail Polianskii** ist wissenschaftlicher Mitarbeiter am Leibniz-Institut für Friedens- und Konfliktforschung – Peace Research Institute Frankfurt (PRIF) und forscht zu russischer Außenpolitik, europäischer Sicherheit und hybrider Kriegsführung. 2024 promovierte er an der Goethe-Universität Frankfurt am Main mit der Dissertation „Better Shared Than Dead? Russia's Dissociation from the Post-Cold War European Security Order". Derzeit arbeitet er im Forschungsprojekt PATTERN: *How Does the Past Matter? The Russian War of Aggression Against Ukraine and the Cold War*, das untersucht, ob und in welcher Form Lehren aus dem Kalten Krieg dazu beitragen können, die heutige Konfrontation mit Russland und anderen antagonistischen Großmächten in geregelte Formen von Abschreckung, Koexistenz oder Kooperation zu überführen.

Jenseits der Grauzone:

Europas Weg zu strategischer Klarheit gegen russische hybride Bedrohungen

→

Europa sieht sich einer zunehmend intensiven Kampagne ausgesetzt, in der russische staatliche und nichtstaatliche Akteure Cyber-, Informations- und kinetische Operationen einsetzen, um die Grenze zwischen Frieden und Krieg gezielt zu verwischen. Der Begriff „hybride Kriegsführung“ hat sich dabei als Sammelbezeichnung für dieses Bedrohungsspektrum etabliert, doch sein undifferenzierter Gebrauch erzeugt analytische Unschärfe und begünstigt politisches Überreagieren.

→

Dieses Papier vertritt die These, dass strategische Wirksamkeit mit begrifflicher Klarheit beginnt. Sie plädiert für einen Ansatz des **„analytischen Föderalismus“**, der hybride Aktivitäten in die Dimensionen Cyber, Information, Wirtschaft und kinetische Angriffe differenziert, um maßgeschneiderte Gegenmaßnahmen und eine kohärentere institutionelle Koordination zu ermöglichen.

→

Zugleich warnt die Studie davor, dass unreflektierte Kriegsrhetorik unnötige Eskalationen fördern, den inneren Zusammenhalt der Allianz schwächen und diplomatische Ausstiegsoptionen verengen kann. Ebenso könnten überzogene Abwehrmaßnahmen – etwa Medieneinschränkungen oder ausgeweitete Überwachung – genau jene demokratischen Normen untergraben, die Europa zu verteidigen sucht.

→

Indem die Analyse begriffliche Präzision, abgestufte Reaktionsfähigkeit und demokratische Resilienz miteinander verbindet, bietet sie Entscheidungsträger:innen einen praxisorientierten Leitfaden, um die Grauzone zwischen Frieden und offenem Konflikt strategisch zu navigieren – ohne Sicherheit oder liberale Werte preiszugeben.

Further information on this topic can be found here:
↗ **www.fes.de**

Friedrich Ebert Stiftung