Berlin, Juli 2026
Analyse und Beratung

KONRAD ADENAUER STIFTUNG

MONITOR

SICHERHEIT

Deutschland im hybriden Krieg: Sicherheit wahren, Demokratie schützen

Von Cyberattacken bis zu Desinformation – Deutschland braucht Reformen in der Sicherheitsarchitektur und ein neues gesellschaftliches Verantwortungsbewusstsein gegen hybride Angriffe

Dr. Edmund Ratka

- Die Sicherheitslage in Deutschland hat sich verändert – und verschärft. Hybride Angriffe (Spionage, Sabotage, Cyberattacken, Desinformation) nehmen zu, vor allem durch Russland.
- Deshalb braucht es eine Reform der Sicherheitsarchitektur, wie sie derzeit von der Bundesregierung auf den Weg gebracht wird, mit erweiterten Kompetenzen für die Sicherheitsbehörden. Neben der funktionalen muss auch die föderale Aufgabenteilung auf den Prüfstand.
- Demokratische Resilienz ist ein Schlüsselfaktor, um im hybriden Krieg zu bestehen. Populismus und Polarisierungsdiskurse bieten ein Einfallstor für Desinformation und gesellschaftliche Destabilisierung.
- Deutschland muss, im Verbund mit seinen Partnern in der Europäischen Union und der NATO, differenzierte Instrumente sowie den nötigen politischen Willen entwickeln, um auf hybride Angriffe offensiver als bisher zu reagieren und damit Abschreckungsfähigkeit herzustellen.
- Sicherheit ist als eine vernetzte, gesamtgesellschaftliche Aufgabe zu verstehen. Der nötige Wandel des Sicherheitsbewusstseins in der Bevölkerung und die Anpassung staatlicher Strukturen dürfen dabei nicht die demokratischen Werte gefährden, für die wir uns verteidigen wollen.

Inhaltsverzeichnis

Angriffe in der Grauzone: die neue hybride Bedrohungslage

„*Wir sind nicht im Krieg, aber wir sind auch nicht mehr im Frieden.*“[1] Die Aussage von Friedrich Merz vom September 2025 ist in doppelter Hinsicht bemerkenswert. Zum einen erklärt der Bundeskanzler damit die Phase der Friedensdividende nach dem Ende des Kalten Krieges und der Wiedervereinigung endgültig für beendet. Die von seinem Vorgänger anlässlich des russischen Angriffs auf die Ukraine im Februar 2022 ausgerufene Zeitenwende wird damit politisch ins Innere der Bundesrepublik gerückt. Zum anderen hebt Merz auf einen Zwischenzustand ab: auf eine Bedrohungslage, für die sich der Begriff „hybrider Krieg“ etabliert hat.

Allgemein wird hybride Kriegsführung als die Kombination regulärer und irregulärer, offener und verdeckter Kampfformen verstanden. Neben dem Einsatz von Soldaten geht es dabei vor allem um Spionage und Sabotage, Cyberangriffe und Desinformationskampagnen. In der Sprache der Militärs: Das Gefechtsfeld wird horizontal entgrenzt. Gekämpft wird nicht mehr nur auf dem Schlachtfeld, sondern die Gesellschaft des Gegners soll destabilisiert, ihre Moral untergraben werden.[2]

Mittlerweile hat sich ein etwas engeres Begriffsverständnis durchgesetzt, das *hybrid* ausschließlich auf nicht-militärische Handlungsfelder und Instrumente bezieht, die dann kombiniert zum Einsatz gebracht werden. In der Definition der Europäischen Union sind damit „schädliche Tätigkeiten gemeint, die mit böswilliger Absicht geplant und ausgeführt werden. Zweck ist es, ein Zielobjekt – einen Staat oder eine Institution – auszuhöhlen.“[3] Der Verfassungsschutz versteht hybride Bedrohungen als „koordinierte, illegitime Handlungen staatlicher und staatlich gelenkter Akteure zur Durchsetzung eigener Interessen zum Nachteil eines anderen Staates, die außerhalb des Rahmens eines konventionellen militärischen Angriffs bleiben.“[4]

Zwar ist dies kein neues Phänomen, Geheimdienstoperationen und Propaganda sind altbekannte Kriegstaktiken. Doch in seiner derzeitigen Wucht ist der hybride Krieg – wie er vor allem von Russland ausgeht – für die friedensverwöhnte Bundesrepublik eine neue Herausforderung. Zudem hat die technologische Entwicklung, mit Blick auf Digitalisierung und Künstliche Intelligenz (KI), und die damit einhergehende wachsende Verwundbarkeit moderner Gesellschaften, hybride Kriegsführung wesentlich einfacher und effektiver gemacht als früher – und damit gefährlicher.

Die hybriden Angriffe gegen Deutschland finden in einer politischen, und vor allem rechtlichen, Grauzone statt: unterhalb der Schwelle eines erklärten Krieges oder bewaffneten Konflikts. Das Grundgesetz kennt diesen Zwischenzustand nicht und unsere Sicherheitsarchitektur ist darauf (noch) nicht ausgerichtet. Inwiefern einzelne Maßnahmen – ein Drohnenüberflug über eine Militärkaserne oder über ein Kraftwerk hier, ein Cyberangriff dort und das Verbreiten von Fake News zu einem lokalen Vorfall ganz woanders – zusammenhängen, und wer jeweils dahintersteckt, ist oft schwer zu ermitteln. Es sind viele kleine Nadelstiche, die das Vertrauen der Bürgerinnen und Bürger in den Staat untergraben, Gesellschaften spalten und die Handlungsfähigkeit eines Landes beeinträchtigen sollen.

Autokratische Aggression: Russland als Hauptakteur

Dass westliche Demokratien nicht nur Zielscheibe, sondern auch besonders anfällig für hybride Kriegsführung sind, haben bereits die Präsidentschaftswahlen 2016 in den USA gezeigt. Mit der Veröffentlichung interner E-Mails der Demokraten sollte deren Kandidatin Hillary Clinton diskreditiert, über Social-Media-Kampagnen gesellschaftliche Friktionen vertieft und mittels Cyberangriffen auf die Wahlinfrastruktur das Vertrauen in die Stimmauszählung beschädigt werden. Amerikanische Ermittler konnten nachweisen, dass hinter diesen Operationen Russland steckte.

Dieses *playbook* bringt Moskau zunehmend auch bei Wahlen in Europa zum Einsatz. So zirkulierten beispielsweise im Vorfeld der Bundestagswahl 2025 gefälschte Videos, die angebliche Wahlmanipulation zeigen sollten (Stimmzettel, bei denen die AfD fehlt; Briefwahlunterlagen, die geschreddert werden). Auch bei den Wahlen vergangenes Jahr in Polen, Tschechien und der Republik Moldau wurde russische Informationsmanipulation festgestellt. EU-freundliche Kandidaten sollten verleumdet, Pro-Kreml-Narrative verbreitet werden.[5]

Von Russlands hybridem Krieg gegen den Westen ist Deutschland als Schlüsselstaat der EU und NATO sowie als wichtiger Unterstützer der Ukraine besonders betroffen. Anlässlich des jüngst veröffentlichten Verfassungsschutzberichts lässt Bundesinnenminister Alexander Dobrindt daran keinen Zweifel: „Der russische Staat möchte unsere Gesellschaft destabilisieren, unsere Demokratie unterwandern und unsere Unterstützung für die Ukraine unterminieren.“[6] Daneben hat der Verfassungsschutz die Volksrepublik China und die Islamische Republik Iran als Hauptakteure identifiziert, die durch ihre nachrichtendienstlichen Aktivitäten in Deutschland eine hybride Bedrohung darstellen. Dabei geht es in erster Linie um Spionage und die Repression von Dissidenten in der Diaspora, aber auch um Sabotage im Cyber- und Informationsraum.

Seit Beginn der russischen Vollinvasion der Ukraine am 24. Februar 2022 entwickelt sich die hybride Bedrohungslage für Deutschland rasant. So zählte das Bundeskriminalamt (BKA) 2025 über dreihundert Sabotagefälle und über eintausend verdächtige Drohnenüberflüge.[7] Jüngste Untersuchungen legen nahe, dass Russland eine koordinierte Drohnenkampagne in Europa lanciert hat, für die es seine in der Ostsee operierende „Schattenflotte“ zum Einsatz bringt. Neben den wirtschaftlichen und psychologischen Kosten, die mit den dadurch ausgelösten Flughafen-Sperrungen (u.a. in München und Berlin) einhergehen, können dadurch kritische Infrastruktur und militärisch relevante Einrichtungen ausspäht werden. Außerdem werden so die Abwehrmaßnahmen europäischer Staaten – und die diesbezüglichen Inkonsistenzen – ausgetestet. Deren

Luftverteidigung ist in vielen Fällen auf diese Art der Luftraumverletzung bislang weder operativ noch in politischer und rechtlicher Hinsicht ausgerichtet.[8]

Als liberale und föderale Demokratie zeichnet sich die Bundesrepublik durch eine besondere Verwundbarkeit gegenüber solchen hybriden Angriffen aus. Es liegt im Wesenskern offener Gesellschaften, dass sie hier Einfallstore bieten – sowohl im physischen als auch kognitiven Bereich. So kann beispielsweise Transparenz bei öffentlicher Infrastruktur für Anschlagsvorbereitungen genutzt werden; Presse- und Meinungsfreiheit setzen dem Vorgehen gegen Desinformation enge Grenzen. Gleichzeitig zielt hybride Kriegsführung auf einen unverzichtbaren Bestandteil demokratischer Gemeinwesen ab, der ohnehin unter Druck steht: Vertrauen.

Sicherheitsarchitektur effizienter gestalten

Ausgehend von der historischen Erfahrung des Nationalsozialismus besteht in der Sicherheitsarchitektur der Bundesrepublik ein doppeltes Trennungsgebot: erstens zwischen innerer und äußerer Sicherheit, wobei für erstere die Polizei und für letztere die Bundeswehr zuständig ist; zweitens zwischen exekutiven Polizeibehörden und den Nachrichtendiensten, die Informationen sammeln und auswerten. Hinzu kommt die föderale Struktur. Hybride Angriffe sind damit oft schwer zu fassen. Eine verdächtige Drohne über einem Hauptbahnhof beispielsweise fällt in die Zuständigkeit der Bundespolizei, ein paar Meter weiter ist die Landespolizei gefragt, jenseits der Landesgrenze dann diejenige des benachbarten Bundeslandes.

Grundsätzlich ist der Bevölkerungsschutz (darunter lassen sich alle nicht-polizeilichen und nicht-militärische Aufgaben und Maßnahmen zum Schutz der Bevölkerung fassen) in Deutschland zweigeteilt: Für den Katastrophenschutz (Schutz vor naturbedingten und technischen Gefahren) sind die Bundesländer zuständig, für den Zivilschutz (Schutz vor den Auswirkungen kriegerischer Auseinandersetzungen) die Bundesebene. Im Verteidigungsfall würde der Bund zwar auf die Instrumente der Länder zurückgreifen und die Prävention im Katastrophen- und Zivilschutz sind oft deckungsgleich bzw. verstärken sich gegenseitig. Dennoch ergibt sich dadurch ein erhöhter Koordinierungsbedarf, der in der dynamischen Bedrohungslage des hybriden Krieges hemmend wirken kann.

Unser auf Subsidiarität in Friedenszeiten (Verantwortung bei Kommunen und Ländern) und zentrale Steuerung im Krieg (durch den Bund) ausgelegtes System bietet hybriden Angreifern eine offene Flanke. So sind beispielsweise im Rahmen der kommunalen Selbstverwaltung Städte und Gemeinden selbst für die Sicherheit ihrer IT-Systeme zuständig – und stehen damit den ungleich größeren Ressourcen und der Professionalität feindlicher Hacker-Gruppen gegenüber, die im Auftrag mächtiger Staaten agieren. Gleiches gilt für kritische Infrastruktur, von der Wasser- bis zur Energieversorgung, die oftmals in kommunaler Hand ist.

Deutschland wird also nicht umhinkommen, im Sicherheitsbereich Kompetenzen neu zu sortieren. Die Leitfrage sollte dabei sein, welche Ebene und welcher Akteur eine bestimmte Gefahr am besten abwehren kann. Es gilt, der Versuchung zu widerstehen, neuen Gefahren in erster Linie mit neuen Institutionen zu begegnen, die dann noch dazu in Doppelstrukturen münden. Dieses Risiko besteht derzeit etwa bei der Abwehr von Drohnen und Desinformation, wo sowohl der Bund als auch mehrere Bundesländer jeweils eigene Einheiten aufbauen – ohne dass die Zuständigkeiten immer klar sind.

Potenzial des Föderalismus nutzen

Gleichzeitig gilt es, die Stärken des Föderalismus zu erhalten: Probleme können oft dort am unmittelbarsten bewältigt werden, wo sie auftreten. Das bewährte 3-K-Prinzip im Bevölkerungsschutz („in der Krise Köpfe kennen") ist in Städten, Gemeinden und Landkreisen längst gelebte Realität. Die 1,7 Millionen Ehrenamtlichen (rechnet man die unter 18-Jährigen dazu, sind es fast zwei Millionen), die sich in Deutschland im Bevölkerungsschutz engagieren, sind in der Regel in lokale Strukturen eingebettet. Zudem ergibt sich aus der dezentralen Organisation unserer Verwaltung und Daseinsvorsorge „funktionale Redundanz" – mit einem erfolgreichen Angriff kann nicht sofort der ganze Staat lahmgelegt werden, sondern eben nur eine bestimmte Region oder eine kleinere Einheit.

Seitens Bund und Länder gilt es also, Rahmenbedingungen zu schaffen für professionelle Flankierung von ehrenamtlichem Engagement vor Ort, für materielle Unterstützung und Ausbildung sowie zentrale Koordinierung bei überregionalen Großschadenslagen. Der im Mai 2026 lancierte und mit 10 Milliarden Euro ausgestattete „Pakt für Bevölkerungsschutz" ist hierfür zumindest in budgetärer Hinsicht ein Meilenstein – nicht zuletzt für das Technische Hilfswerk (THW). Doch auch andere Blaulichtorganisationen wie das Deutsche Rote Kreuz (DRK), die für den Bevölkerungsschutz eine elementare Rolle spielen, benötigen langfristige Planungssicherheit.

Kompetenzen von Sicherheitsbehörden erweitern

Das Bundesinnenministerium hat seine Rolle als Schlüsselakteur im Bereich zivile Verteidigung inzwischen voll angenommen. Es hat sich dafür organisatorisch neu aufgestellt und nachgeordnete Behörden wie das Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) gestärkt. Durch Gesetzesreformen, wie beim Luftsicherheitsgesetz im Frühjahr 2026, können konkrete Gefahrensituationen besser bewältigt werden. So kann die Bundeswehr nunmehr ohne komplizierte Verfahren im Rahmen der Amtshilfe Drohnen bekämpfen.

Regierung und Parlament beraten derzeit außerdem über mehrere so genannte Sicherheitsgesetze, mit denen die Befugnisse von Sicherheitsbehörden ausgeweitet und an die neue Bedrohungslage angepasst werden. So soll etwa der Verfassungsschutz (BfV) „aktive Cyberabwehr" betreiben können, also beispielsweise ausländische Server hacken, von denen Bedrohungen gegen die Bundesrepublik ausgehen. Dem Bundesnachrichtendienst (BND) soll unter anderem die Möglichkeit gegeben werden, in weitaus größerem Umfang als bisher internationale Datenströme abzuschöpfen und in einer Bedrohungslage auszuwerten.

Ein rechtlicher und rechtsstaatskonformer Rahmen muss dabei genauso gewährleistet bleiben wie demokratische Aufsicht, wie sie bisher etwa über das Parlamentarische Kontrollgremium (PKGr) ausgeübt wird. Doch die Entwicklung der entsprechenden Behörden in Deutschland zu „echten Geheimdiensten" mit operativen Kompetenzen und Fähigkeiten ist unabdingbar, wenn wir im hybriden Krieg, den insbesondere autoritäre Staaten gegen uns führen, bestehen wollen.

Demokratische Resilienz stärken

Westliche Demokratien haben seit einigen Jahren zunehmend mit Populismus, Polarisierung und Vertrauensverlust zu kämpfen. Feindlich gesinnte Akteure machen sich diesen Umstand zu Nutze und setzen gezielt an Triggerpunkten einer Gesellschaft an, um deren Zersetzung und Zerfaserung zu befördern. Dazu dienen die auch unter dem Begriff *Foreign Information Manipulation and Interference* (FIMI) gefassten Desinformationskampagnen. Diese Spielart hybrider Kriegsführung hat mit der weiterhin laufenden KI-Revolution noch einmal einen neuen Schub bekommen. Neben KI als Beschleuniger bei der Erstellung und Verbreitung von Desinformation ergeben sich durch die rasant wachsende Nutzung von KI als Informations-Infrastruktur und autonome KI-Agenten ganz neue Angriffsflächen für hybride Kriegsführung.[9]

Dem gilt es mit offensiver und transparenter staatlicher Kommunikation zu begegnen. Auch die Regulierung von Online-Plattformen sollte ausgebaut werden, am besten im europäischen Verbund. Zentraler Hebel dafür ist der Digital Services Act (DSA). Diese EU-Verordnung gilt seit 2024 in allen Mitgliedsländern und verpflichtet große Online-Plattformen und Suchmaschinen, die Verbreitung von Desinformation zu verhindern. Deutschland sollte weiterhin an der Umsetzung und Weiterentwicklung des DSA mitwirken, selbst wenn dies Unstimmigkeiten auch mit amerikanischen Tech-Konzernen und der gegenwärtigen US-Administration bedeutet. Das jüngst von der EU veröffentliche *FIMI Deterrence Playbook* zeigt auf, wie durch Strafverfolgung und Sanktionen gegen „Mittelsmänner", die in Desinformationskampagnen involviert sind, die für FIMI nötige Infrastruktur zerschlagen werden kann, selbst wenn deren Urheber bzw. Auftraggeber nicht zweifelsfrei zu ermitteln sind.[10]

Doch letztendlich sind die beste Verteidigung gegen Desinformation mündige Bürgerinnen und Bürger, die in der demokratischen Praxis kritisches Denken verinnerlicht haben. Dieses gilt es, einschließlich der nötigen Medienkompetenz, von der Schule bis in die Erwachsenenbildung hinein zu fördern. Und auch die politische Ebene steht in der Pflicht: Denn populistischer, spaltender und ausgrenzender Diskurs setzt Fliehkräfte frei, die eine Gesellschaft anfälliger machen für gezielte Informationsmanipulation von außen. Das alltägliche politische Bemühen um das Vertrauen der Bevölkerung, bei der intermediären Akteuren wie Parteien eine Schlüsselrolle zukommt, gewinnt also an sicherheitspolitischer Bedeutung. Je geringer die Kluft zwischen Staat und Bürger, desto größer die Wehrhaftigkeit im hybriden Krieg.

Von der Abwehr zur Abschreckung

So wichtig die Stärkung von Resilienz im physischen wie kognitiven Bereich auch ist (*deterrence by denial*), muss sie durch eine angepasste Form der klassischen Abschreckung ergänzt werden (*deterrence by punishment*), um die Sicherheit unseres Landes im Zeitalter hybrider Kriegsführung zu gewährleisten. Hybride Kriegsführung ist zwar kein Alleinstellungsmerkmal autoritärer Staaten. Doch diese setzen sie in der Praxis häufiger ein und machen sich dabei die rechtlichen und normativen Beschränkungen zu Nutze, die sich westliche Demokratien, gerade auch Deutschland, auferlegt haben.

In der Reziprozität der Abschreckung (*Tit-for-Tat*) klafft damit eine Lücke. Zum einen ist die Attribuierung bei hybriden Angriffen schwieriger. Zum anderen kann ein Rechtsstaat eine rechtswidrige Aktion (wie eine Desinformationskampagne oder ein Cyberangriff auf für die Versorgung der Zivilbevölkerung relevante Infrastruktur) nicht mit der gleichen Aktion beantworten, wenn diese aus seiner (und völkerrechtlicher) Sicht ebenso rechtswidrig ist.

Um dieses Dilemma zumindest zu entschärfen, muss die Abschreckung im hybriden Zeitalter domänenübergreifend, asymmetrisch, kumulativ und akteursspezifisch sein, wie es auch eine Gruppe deutscher Sicherheitsexperten in einem jüngst veröffentlichten DGAP-Papier darlegte.[11] Gezielte Sanktionen wie das Einfrieren von Vermögen und die Beschlagnahmung beispielsweise von Schiffen, die an hybriden Operationen mitwirken, sollten dabei die bevorzugten Mittel sein. Doch auch die Unterminierung feindlicher Regime – sei es durch Kommunikationskampagnen oder die (auch militärische) Unterstützung Dritter – ist in europäischen Fachkreisen mittlerweile kein Tabuthema mehr.[12]

Deutschland sollte die Entwicklung und Anwendung seiner hybriden Abschreckungsfähigkeiten möglichst eng in den EU- und NATO-Rahmen einbetten. Die Grundlagen hierfür sind gelegt. So hat die NATO schon im Jahr 2014 auf ihrem Gipfel in Wales festgestellt, dass Cyberattacken wie bewaffnete Angriffe gewertet werden und damit die kollektive Verteidigung unter Artikel 5 auslösen können. Auf EU-Ebene wird seit einigen Jahren an einem Instrumentarium gearbeitet, hybride

Angriffe offensiver zurückzuschlagen. Beispielsweise sind derzeit, basierend auf der 2017 lancierten *Cyber Diplomacy Toolbox*, 19 Personen und sieben Einheiten mit Sanktionen belegt, denen Verbindungen zu russischen und chinesischen Cyberoperationen nachgewiesen werden konnten.[13] Dieses Instrumentarium gilt es nun auszubauen und weitaus entschlossener als bisher anzuwenden.

Sicherheit vernetzt denken

So vielfältig die Angriffsflächen hybrider Kriegsführung sind, so umfassend muss unsere Antwort darauf sein. Die Zeiten, als die Gewährleistung von Sicherheit an Spezialisten delegiert werden konnte – seien es die entsprechenden Behörden im Inland oder die Bundeswehr im Ausland bzw. im Verteidigungsfall – sind vorbei. Sicherheit bleibt natürlich eine staatliche Kernfunktion, muss aber darüber hinaus als gesamtgesellschaftliche Aufgabe verstanden werden. Bürgerinnen und Bürger, Unternehmen, zivilgesellschaftliche Organisationen und Bildungsträger sind unabdingbare Akteure, um Deutschland und seine demokratische Ordnung zu verteidigen.

Dafür braucht es zum einen Sensibilisierung in der Bevölkerung insgesamt – auch durch eine klare Kommunikation von staatlicher Seite, die Panikmache vermeidet, aber das dynamische Lagebild ehrlich vermittelt. Zum anderen braucht es Mobilisierung auf jeder Ebene. Dies kann durch Aufklärungs- und Informationskampagnen erfolgen, etwa mit Blick auf den heimischen Notfallvorrat oder Ermutigung zu ehrenamtlichem Engagement. In besonders sensiblen Bereichen sind Mindeststandards durch gesetzliche Regelungen unvermeidbar, etwa beim Schutz kritischer Infrastruktur oder der IT-Sicherheit öffentlicher und systemrelevanter Einrichtungen.

Daneben gilt es, zu lernen und zu üben. So können sich Kommunen über Best-Practice-Beispiele zur Krisenbewältigung austauschen; durch Szenarien-Workshops und Planspiele werden Koordinationsmechanismen etabliert. Selbst wenn der nationale Kontext jeweils unterschiedlich ist, lohnt sich der Blick auf Staaten wie Schweden und Finnland, in denen seit Jahrzehnten ein umfassendes Sicherheitskonzept *(whole of government-, whole of society-approach*) zur Anwendung kommt.

Ein gestärktes Bewusstsein für sicherheitspolitische Realitäten ist dabei strikt abzugrenzen von einem autoritären Sicherheitsdiskurs, der unter dem Primat der Schutzgarantie dann Menschenrechte – sei es in der Innen- oder Außenpolitik – und politische Mitwirkungsmöglichkeiten einschränkt. Stattdessen gilt es, im hybriden Krieg zu bestehen, ohne dabei genau diejenigen Werte zu beschädigen, für die wir uns verteidigen wollen, wie Freiheit, Pluralität und Rechtsstaatlichkeit. Dafür müssen jetzt Strukturen angepasst werden und sich Staat und Gesellschaft auf ein Sicherheitskonzept verständigen, das der neuen Bedrohungslage gerecht wird. Die dafür nötige Resilienz kann die Bundesrepublik gerade auch aus den spezifischen Eigenheiten ihres föderalen Staatsaufbaus und demokratischen Gemeinwesens heraus entwickeln.

---

1 Friedrich Merz hat diese Formulierung öffentlich erstmals am 29.09.2025 in Düsseldorf genutzt und bei seiner Rede auf dem CDU-Parteitag im Februar 2026 in Stuttgart wiederholt: https://rp-online.de/politik/deutschland/kanzler-merz-beim-staendehaus-treff-in-duesseldorf-nicht-im-krieg-auch-nicht-im-frieden_aid-135896829; https://www.tagesschau.de/inland/innenpolitik/cdu-parteitag-merz-114.html (zuletzt aufgerufen am 15.07.2026).

[2] Schmid, Johann 2022: Krieg in der Grauzone von Schnittstellen. Was ist hybride Kriegsführung? Zentrum für Militärgeschichte und Sozialwissenschaften der Bundeswehr, Potsdam. https://opus4.kobv.de/opus4-zmsbw/frontdoor/index/index/docId/596 (zuletzt aufgerufen am 15.07.2026).

[3] Europäischer Rat 2026: Hybride Bedrohungen (Hintergrund). https://www.consilium.europa.eu/de/policies/hybrid-threats/ (zuletzt aufgerufen am 15.07.2026).

[4] Bundesministerium des Inneren 2026: Verfassungsschutzbericht 2025, S. 335: https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/sicherheit/BMI26012-vsb2025.pdf?__blob=publicationFile&v=7 (zuletzt aufgerufen am 15.07.2026).

[5] Europäische Union 2026: 4th EEAS Report on Foreign Information Manipulation and Interference Threats: https://euvsdisinfo.eu/uploads/2026/03/EEAS-4th-Threat-Report_web-version.pdf (zuletzt aufgerufen am 15.07.2026).

[6] Bundesministerium des Inneren 2026: Verfassungsschutzbericht 2025, S. 1: https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/sicherheit/BMI26012-vsb2025.pdf?__blob=publicationFile&v=7 (zuletzt aufgerufen am 15.07.2026).

[7] Bewarder, Manuel/Diel, Jörg/Flade, Florian 2026: Hybride Bedrohungen. BKA zählt mehr als 320 Sabotage-Verdachtsfälle, in: tagesschau, 05.02.2026: https://www.tagesschau.de/investigativ/ndr-wdr/bka-sabotage-verdacht-100.html (zuletzt aufgerufen am 15.07.2026).

[8] Edwards, Charlie/O'Loughlin, Rex Fox/Bearn, Luis 2026: Russia's UAV Campaign Over Europe, The International Institute for Strategic Studies (IISS): https://www.iiss.org/globalassets/media-library---content--migration/images-delta/publications/research-papers/2026-new/russia-uav/ammended-file/russia_uav-campaign-over-europe.pdf (zuletzt aufgerufen am 15.07.2026).

[9] Munoz, Katja 2026: KI und hybride Bedrohungen 2.0, DGAP Policy Brief: https://dgap.org/system/files/article_pdfs/DGAP%20Policy%20Brief_Nr-5_MRZ-2026_xxS.pdf (zuletzt aufgerufen am 15.07.2026).

[10] Europäische Union 2026: 4th EEAS Report on Foreign Information Manipulation and Interference Threats. S. 20-23: https://euvsdisinfo.eu/uploads/2026/03/EEAS-4th-Threat-Report_web-version.pdf (zuletzt aufgerufen am 15.07.2026).

[11] Kleine-Brockhoff, Thomas u.a. 2026: Aufklären, Abschrecken, Verteidigen: Ein Konzept zur Abwehr des hybriden Krieges gegen Deutschland, DGAP White Paper, Karl Kaiser Forum, S. 3: https://dgap.org/de/mediathek/ein-konzept-zur-abwehr-des-hybriden-krieges-gegen-deutschland (zuletzt aufgerufen am 15.07.2026).

[12] Brown, Will u.a. 2026: From Shield to Sword. Europe's Offensive Strategy for the Hybrid Age, ECFR Policy Brief: https://ecfr.eu/wp-content/uploads/2026/03/From-shield-to-sword-Europes-offensive-strategy-for-the-hybrid-age.pdf (zuletzt aufgerufen am 15.07.2026).

[13] Tothova, Linda 2026: The EU response to hybrid threats, European Parliamentary Research Service. https://www.europarl.europa.eu/RegData/etudes/BRIE/2026/789374/EPRS_BRI(2026)789374_EN.pdf (zuletzt aufgerufen am 15.07.2026).

Impressum

Der Autor

Dr. Edmund Ratka ist Referent für Europäische Sicherheit in der Hauptabteilung Analyse und Beratung der Konrad-Adenauer-Stiftung in Berlin. Von 2014 bis 2025 war er in der Abteilung Naher Osten und Nordafrika der Konrad-Adenauer-Stiftung tätig, die letzten fünf Jahre als Leiter des Auslandsbüros Jordanien. Er hat an der Ludwig-Maximilians-Universität München und am Institut d'Etudes Politiques in Aix-en-Provence Politikwissenschaft studiert und mit einer Arbeit zur Europäisierung der deutschen Außenpolitik promoviert.

Konrad-Adenauer-Stiftung e. V.

Dr. Edmund Ratka
Referent Europäische Sicherheit
Hauptabteilung Analyse und Beratung

T +49 30 / 26 996-3953
edmund.ratka@kas.de

Herausgeberin: Konrad-Adenauer-Stiftung e. V.
Gestaltung: yellow too Pasiek & Horntrich GbR

Hergestellt mit finanzieller Unterstützung der Bundesrepublik Deutschland.