Nr. 564 | März 2026

Analysen & Argumente

KONRAD ADENAUER STIFTUNG

Mehr KI für Verteidigung und Resilienz

Impulse für eine agile und zukunftsfähige Bundeswehr

Natascha Zowislo-Grünewald, Franz Beitzinger, Ferdinand Gehringer, Dierk Spreen

- Künstliche Intelligenz (KI) muss von der Bundeswehr aktiv genutzt und in Kooperation mit der Wirtschaft entwickelt werden, um effizient abschrecken zu können und im Ernstfall für den modernen Krieg gerüstet zu sein. Das erfordert einen tiefgreifenden Mindset-Wandel in der Bundeswehr und im Bundesministerium der Verteidigung, eine Anpassung der Planungs- und Beschaffungsprozesse sowie digitale Souveränität.
- Derzeit bestehen vor allem erhebliche Fähigkeitslücken auf dem digitalen Schlachtfeld. Das kann nicht der Anspruch sein.
- Das Gleiche gilt für den Schutz von Bevölkerung und Infrastrukturen in Bezug auf hybride Bedrohungen. Der hybride Krieg findet nicht morgen, sondern bereits jetzt statt.
- Ziel ist es, mittels klarer Verantwortlichkeiten und grundsätzlichem Vertrauen in KI-gestützte eigene Fähigkeiten eine Entscheidungs- und Innovationslähmung zu verhindern.
- Im Folgenden wird für sechs Bereiche ein Überblick über Potenziale Künstlicher Intelligenz gegeben, woran sich eine KI-Strategie der Bundeswehr orientieren kann: Metaebene, Ethik und Recht, Strategische Aufklärung und Einsatzszenarien, Autonome Systeme, Kognitive Kriegführung und Cyberverteidigung, Betriebswirtschaftliche Planungsprozesse.

1. Einleitung

Die Bundeswehr befindet sich im Umfeld hochdynamischer, datenintensiver und multivektoraler Bedrohungen, wo Geschwindigkeit, Präzision und Resilienz über Handlungsfähigkeit entscheiden.

Künstliche Intelligenz (KI) ist hier von erheblicher Bedeutung: Sie kann bisher bestehende Fähigkeitslücken im Erkennen (Sensorik und Lagebild), Verstehen (Analyse und Entscheidungsunterstützung) sowie im Wirken und Unterstützen (teil-/autonome Systeme) schließen, während sie zugleich Verwaltungs-, Planungs- und Beschaffungsprozesse beschleunigt.

Bereits anerkannte Leitprinzipien zur Nutzung von KI durch die Bundeswehr **Software Defined Defence (SDD)**[1]**, Interoperabilität, Ethics-by-Design**[2] sowie **Human-in-Command** greifen jedoch zu kurz und tragen den strukturellen Rahmenbedingungen innerhalb der Bundeswehr nur unzureichend Rechnung.

Die Potenziale von KI können nur dann nachhaltig ausgeschöpft werden, wenn die Rahmenbedingungen ihrer Implementierung und ihres Einsatzes zielführend sind.

2. Angepasste Rahmenbedingungen sind Grundvoraussetzung

Die Bundeswehr muss über alle Planungszeithorizonte hinweg in der Lage sein, technologische Herausforderungen und gegnerische Fähigkeitsentwicklungen frühzeitig zu antizipieren sowie agil und umsetzungsorientiert darauf zu reagieren.

Dafür ist ein **grundlegender Mindset-Wandel** auf allen Hierarchieebenen erforderlich – hin zu mehr Offenheit, Mut und Tatkraft: getragen von einem innovationsfreundlichen Organisationsklima, agilen Entscheidungsprozessen und einer belastbaren Fehlerkultur.

Dies bedingt **angepasste Planungs- und Beschaffungsprozesse** mit einer konsequenten Verzahnung von Top-down- und Bottom-up-Ansätzen, um technologische, taktische und strategische Anpassungen zu beschleunigen.

Ergänzend ist eine **umfassende Digital- und Datensouveränität** notwendig, einschließlich eines abgesicherten strategischen Datenpools, vertrauenswürdiger nationaler und europäischer Einrichtungen sowie militärspezifisch trainierter KI-Modelle.

Bei der Umsetzung dieser Rahmenbedingungen kann Künstliche Intelligenz die Bundeswehr wirksam befähigen, aktuelle und künftige Bedrohungen zu bewältigen, Fähigkeitslücken zu schließen und die knappe Ressource Personal zu entlasten.

Grundlegende Wandel in Einstellungen und Prozessen bedingen technologische Anpassungen

3. Weitreichende Fähigkeitslücken im Schlachtfeld der Zukunft

Im Schlachtfeld der Zukunft offenbaren sich bei der Bundeswehr gravierende Fähigkeitslücken entlang der gesamten Wirkungskette.

Schon in der Wahrnehmungsebene treten kritische Defizite zutage: Sensorik und Aufklärung leiden unter fragmentierten Datenräumen, verstreuten militärischen und zivilen Quellen sowie einer mangelhaften Informationsfusion. Die Folge: unzureichende Abdeckung in Schlüsselräumen (Luft, See und Unterwasser) und gefährliche Schattenzonen, insbesondere im niedrigen Luftraum bei der Detektion von Kleindrohnen.

Diese eingeschränkte Wahrnehmung setzt sich auf der Ebene des Lagebildes und der Entscheidungsfindung fort. Langsame Observe-Orient-Decide-Act-Loops (OODA)[3], eine heterogene Werkzeuglandschaft sowie das Fehlen KI-gestützter Szenarienplanung und Wirkbewertung beeinträchtigen das Verständnis der Lage und verzögern Entscheidungen. Gleichzeitig mangelt es an responsiven Daten- und Kommunikationsfähigkeiten im Einsatz, da leistungsfähige Mission- oder Combat-Clouds sowie Fähigkeiten zur lokalen, dezentralisierten Datenverarbeitung (Edge Computing) weitgehend fehlen.

Auch in der Wirkung zeigen sich strukturelle Schwächen. Waffensysteme leiden unter einem ungünstigen „Cost-to-kill"-Verhältnis – etwa in der Drohnenabwehr, unter begrenzter Autonomie und Reaktionsgeschwindigkeit sowie unter mangelnder Standardisierung. Unklare Zuständigkeiten, etwa bei der Drohnenabwehr im Inland, verstärken diese Problematik zusätzlich. In der Cyberverteidigung fehlt ein dauerhaft gemeinsames Lagebild zwischen politischer Führung, zivilen Akteuren und Militär (gov–civ–mil); zugleich sind Detektion, Attribution und Mitigation nur gering automatisiert, was durch Interoperabilitätsdefizite weiter verschärft wird.

Im Informations- und kognitiven Raum ist die Bundeswehr nur eingeschränkt handlungsfähig. Es fehlt an Echtzeit-Analysen relevanter Themen und Netzwerke, simulationsbasierter Kommunikationsplanung sowie wirksamer Desinformationsabwehr. Insbesondere mangelt es an präventiven Ansätzen durch konsistente, glaubwürdige Narrative auf Basis vertrauenswürdiger Regierungsführung (sogenannte Prebunking-Ansätze).

Diese operativen Defizite werden durch organisationale und strukturelle Schwächen verstärkt. Zwischen Konzeptentwicklung und Umsetzung klafft ein „Tal des Todes" mit mehrjährigen Bearbeitungszyklen; zugleich wird KI in der Verwaltung trotz Personalmangels kaum genutzt. Geringe Fehlertoleranz, übervorsichtige Führung und eine rigide Auslegung des Vorsorgeprinzips hemmen Innovationsfähigkeit und kreatives Denken auf allen Ebenen.

Schließlich bestehen erhebliche Engpässe bei der Rechenleistung und Lieferketten. Die Abhängigkeit von globalen, störanfälligen Lieferketten, eine unklare Energiestrategie für KI-Workloads, fehlende Datensouveränität sowie das Ausbleiben einer hardwareseitigen Bevorratung schwächen die Durchhalte- und Anpassungsfähigkeit insgesamt.

In ihrer Gesamtheit gefährden diese Fähigkeitslücken die Einsatzfähigkeit der Bundeswehr im hochdynamischen Gefechtsfeld der Zukunft.

Mängel bei fortschrittlichen Anwendungen

4. Handlungsfelder, Ziele und Maßnahmen

4.1 Metaebene: Fähigkeit zum KI-Fähigkeitsaufwuchs

Zielbild: Befähigung zur kontinuierlichen Anpassung an sich erhöhende Komplexität des strategischen Umfelds und wachsende Datenbasis; Verkürzung des Entscheidungsfindungsprozesses (Bestandsprozesse unterstützen und Schaffung von „KI-Readiness“)

Maßnahmen:

- Schaffung eines **strukturellen, rechtssicheren Rahmens für eine schnelle Fähigkeitserweiterung**; gleichzeitig bestehende Rechtsrahmen ausschöpfen statt übererfüllen (Vergabeprozesse vereinfachen und beschleunigen, unbürokratische Direktvergaben)
- **Fähigkeitsaufwuchs als iterativen Prozess** gestalten (Reinforced Learning by Doing) und Schaffung des Bewusstseins der Notwendigkeit dieses Prozesses anstelle auf die ultimative Lösung zu warten
- **Kurzfristige Innovationspartnerschaften** in direkt-/freihändiger Vergabe zur Erreichung eines spezifischen Technologie-Reifegrads (Technology Readiness Level) ermöglichen
- **Souveräne KI-Basismodelle** (einschließlich großer Sprachmodelle/LLMs) und **Lieferketten** für militärische Anwendungen generieren; wo es sinnvoll ist: hybride Nutzung kommerzieller Komponenten in abgeschotteten Domänen
- **Hohen Ausbildungsstand sicherstellen,** um das Chancen-Risiko-Verhältnis im KI-Einsatz zu optimieren

Komplexität erfordert verschiedene Maßnahmen wie Innovationspartnerschaften

4.2 Grundlagen: Framework für Ethik und Recht

Zielbild: Ein verbindliches KI-Governance-Framework mit Ethik-, Rechts- und Sicherheitsanforderungen als integrale Elemente des Systemdesigns und der Qualifikation.

Maßnahmen:

- KI-Governance-Ordnung (Policy, Rollen, Freigabestufen) inklusive **Ethik-Board** und **Safety-/Red-Teams;** Einführung eines **Human-in-Command**-Standards (Entscheidungsrechte, Übersteuerung/Override, Prüfpfade/Audit-Trails)
- **Pflicht zur Verteidigung der Demokratie**, der Menschenrechte und der kollektiven Selbstbestimmung müssen Leitmotiv des KI-Governance-Frameworks sein
- **Kommunikation** des Sinns des ethischen Frameworks einschließlich Abschreckung unethisch verfahrender Gegner
- **Maschinelles Lernen** für Verteidigung: Prozesse, Werkzeuge, Test-/Zertifizierungsumgebungen (Mensch/Maschine, Maschine/Maschine), reproduzierbare Benchmarks

- **Ethics-by-Design** in Pflichtenheften und Zulassungsunterlagen; „Hippokrates-Ethos“ analog zum Arztgelöbnis des Hippokrates für militärische KI-Entwicklung und Nutzung (Ausbildung, Innere Führung)

- **Klare Festlegung von Verantwortlichkeiten und Vertrauen in die Technologie:** KI – ob militärisch oder zivil – beeinflusst Menschen: Für Fehler haften nicht Algorithmen, sondern Entwickler, Betreiber und Anwender. Klare Verantwortlichkeiten und Vertrauen in die Technik verhindern Entscheidungs- und Innovationslähmung.

Einbettung der KI in ethischen und rechtlichen Rahmen nötig

4.3 Strategische Aufklärung & Einsatzszenarien („Nebel des Krieges“)

Zielbild: KI-gestützte Aufklärung mit durchgängiger Datenkette, die historische und (annähernd) Echtzeit-Daten aus Sensorik und allen weiteren verfügbaren Datenquellen fusioniert, Szenarien simuliert und Entscheidungen beschleunigt.

Maßnahmen:

- Es ist ein **strategischer Datenpool** als nationale/europäische Ressource (Asset) einzurichten, weil Training über Daten bei der Entwicklung von KI eine zentrale Rolle spielt. Darüber hinaus sind vertrauenswürdige Rahmenbedingungen für Entwicklungsaufgaben (**Trusted Facilities**), verbindliche Datenlieferpflichten und eine Qualitätssicherung zu schaffen.

- **Iterative Fähigkeitsentwicklung** (Reinforced Learning by Doing): Ermöglichung kurzfristiger Innovationspartnerschaften zwischen Bundeswehr und Wirtschaft, z. B. direkte Vergaben zur Optimierung der Technologie-Reifegrade, inklusive der Einrichtung gemeinsamer Test-/Verifikationsumgebungen.

- **Wechselseitige Schnittstellen** von Sensorik und Datenverarbeitung zu **NATO-JISR** (Joint Intelligence, Surveillance, and Reconnaissance) sollten hergestellt werden.

- Bei **Standardprozessen** ist **KI-Assistenz** umfassend einzuführen (z. B. für Zielkandidatenbildung, Mustererkennung, Veränderungsdetektion).

- **Hybride Architekturen** sollten genutzt werden (Cloud-, Edge- und Fog-Computing): lokale Datenvorverarbeitung an der Quelle (Fog), Weiterverarbeitung in der Zwischenschicht (Edge), Auslagerung umfangreicher Rechenprozesse in die Cloud mit Zuordnung je nach Anforderungen.

- Insbesondere sind **rechtssichere Datenfreigaben** und interinstitutioneller Austausch vor allem zwischen Organen innerer und äußerer Sicherheit mit klarer Steuerung und Verantwortung zu ermöglichen. Verteidigung findet nicht nur an den Außengrenzen statt und beginnt im Zeitalter hybrider und kognitiver Kriegführung auch nicht erst mit dem Verteidigungsfall.

Aufklärung und Datenverarbeitung durch KI vereinfacht

4.4 Autonome Systeme, inklusive Waffensysteme

Zielbild: Teil- bis hochautonome Wirkmittel mit verlässlichen, auditierbaren KI-Funktionen, die Cost-to-kill verbessern und Reaktionszeiten drastisch senken – bei klarer Einbindung in die Rules of Engagement (RoE) und menschlicher Verantwortlichkeit.

Maßnahmen:

- **Hochskalieren der Menge der Drohnen pro Operateur mithilfe von KI:** Eins-zu-n-Beziehung, Cost-to-kill-Ratio erhöhen, günstige Technologie, welche ggf. teuer abgewehrt werden muss

- **Aufklärung und Schutz des Unterwasserraums mittels autonom beweglicher Sensoren:** im Vergleich zu bemannten Systemen (U-Booten) kostengünstiger, 24/7-Awareness

- **Autonomisierung von Decide und Act im Loop:** prinzipiell autonom operierende und entscheidende Systeme in einer festgelegten Einsatzzone (Engagement-Box), d. h. weniger Anfälligkeit gegen Störung und hohe Reaktionsgeschwindigkeiten; Aufschalten menschlicher Entscheider jedoch möglich

- **KI-gestütztes Luftraummanagement, KI-gestützte Luftraumauswertung und KI-Wachtposten:** Ermöglicht einerseits die flexible Variation eigener Angriffsvektoren im Luftraum und andererseits die Früherkennung von feindlichen Angriffsvektoren anhand von Drohneneinsatzmustern.

- **Counter-Swarming:** situative lokale Luftüberlegenheit, Ermöglichung von Bodenoperationen mit schwerem Gerät und Infanterie (operative Entlastung, Schutz, Überwindung der Todeszone, Meistern des gläsernen Gefechtsfeldes), hoher Nachschub an Drohnen nötig

- **KI-gestütztes Sensornetzwerk Luft:** 4G-Kontrolle (Drohnen sind quasi „fliegende Handys“) und/oder KI-Auswertung akustischer Informationen (z. B. Akustiksensoren an Laternenmasten, die das typische Drohnensurren erkennen) ermöglichen Früherkennung von Drohnen. Aufbauend darauf ist eine automatische Klassifizierung von Alarmszenarien möglich.

- **KI-basierte Erste Hilfe/Krisenmanagement im Falle von Großschadensereignissen:** koordinierte und schnelle Evakuierung von Zielbereichen (Flughäfen, Bahnhöfe etc.) im Falle von Angriffen, schnelle Koordination der Ersten Hilfe sowie automatische Hilfskräfterekrutierung (Sofortkoordination Ersthelfer)

- **Synthetisierende Warn-App**, die Nutzereinspeisungen (Drohnensichtungen etc.) aufnimmt, bewertet und ohne Zeitverlust die betroffene Bevölkerung warnt: Schließen von Warnlücken, schnelle und breite Warnung

- **KI-gestützte Bilderkennung:** schnelles Erkennen und Klassifizieren von Objekten/Personen, Reduktion von Fehlern und Täuschungen, konstant hohe 24/7-Awareness

- **KI-Erkennung von ungewöhnlichen Teilnehmern in Netzwerken** (WLAN, Mobiltelefonie, z. B. IMSI-Catcher[4]): Schutz vor Spionage und feindlicher Aufklärung, Erkennung unbekannter Teilnehmer in Funknetzen von Sicherheitsbereichen, Drohnendetektion

KI bietet große Potenziale für Waffensysteme

4.5 Kognitive und kommunikative Kriegführung, Cyberverteidigung

Zielbild: Angestrebt wird die Etablierung eines durchgängigen, KI-gestützten Kommunikationszyklus, der die Kommunikation in Social Media und anderen Netzwerken in Echtzeit versteht, resilient gegen Desinformation ist und zielgruppengerecht gegen Desinformationskampagnen wirkt. Ziel ist die Fähigkeit, ein Echtzeit-Cyberlagebild zu erstellen, das KI-gestützte Attribution ermöglicht und Schutzmaßnahmen einleitet. Ein Kommunikationszyklus besteht aus der Folge von Analyse → Planung → Produktion → Distribution und → Evaluation.

Maßnahmen:

- **Analyse/Data Fusion:** Themen-/Akteurs-/Netzwerkanalyse in Echtzeit (militärisch/zivil), d. h. Echtzeiterkennung und Verlaufsverfolgung von Desinformationskampagnen (Risiko- und Wirkungsassessment)

- **Planung und Simulation:** Identifikation von Zielgruppensegmenten, Szenarien und A/B-Tests[5], Identifikation von Wirkpfaden („effects-based“)

- **Produktion:** KI-Assistenz für Text/Bild/Audio/Video (inkl. synthetischer Medien) in gesicherten Umgebungen; Fact-Checking, Ursprungsanalyse von Desinformationen

- **Distribution & Netzwerkmanagement:** Reichweitenaufbau in Zielgruppen, Takedown-/Counter-Narratives identifizieren und zielgruppengerecht einspeisen, automatisiertes proaktives Prebunking kombiniert mit automatisiertem Debunking (z. B. Faktenckecks) – auch im Sinne einer offensiven Abschreckungsfunktion

- **Evaluation:** Erfolgsmetriken entlang der Prozesskette; Feedback in Trainingsdaten zurückführen

- **Schutzkomponente:** Desinformationsdetektion, Täuschungsresilienz, Schutz kritischer Kommunikationsinfrastruktur

- **Echtzeit-Lagebild** in der Cyberabwehr: Etablierung eines gemeinsamen, synchronen cyber-situativen Lagebildes (gov–civ–mil) mit KI-gestützter Detektion, Attribution und Mitigation, das auf Kollaboration, Automatisierung und aktiver Cyberabwehr beruht

- **Automatisierte Anomaliedetektion** und systematisches Penetrationstesting (kombiniert mit systematischem **Red-Teaming**): Ziel ist es, eigene Verwundbarkeiten im Cyberraum durch simulierte Angriffe und Übernahme von Gegnerperspektiven proaktiv zu erkennen, Resilienz und operative Kreativität aufzubauen und ggf. nötige aktive Cyberabwehroperationen zu ermöglichen.

Beschleunigung und Abwehr in Kommunikation und Cyberraum

4.6 Betriebswirtschaftliche Planungsprozesse und Organisation

Zielbild: Schaffung einer KI-fähigen Organisation, die Prozesse beschleunigt, Sense-Making stärkt und das „Tal des Todes“ zwischen Konzept und Einsatz schließt – mit resilienten Lieferketten und digitaler Souveränität

Maßnahmen:

- **KI in der Verwaltung zulassen** (sichere, nicht-öffentliche Modelle), **Mitzeichnungsprozesse** verschlanken, Dokumentenerzeugung und -prüfung automatisieren („Mission e“).
- **Sense-Making** (Cognitive Dominance): KI-gestützte Lage- und Planungsarbeit in Stäben (z. B. KI-Taktik-Chat im Gefechtsstand) etablieren und Effects Based Operations (EBO) unterstützen.
- **Innovationsbrücken** kreieren, indem ein militärisches **SPRIND-Pendant (Bundesagentur für Sprunginnovationen)** geschaffen wird, bestehende Initiativen vernetzt und Start-ups frühzeitig eingebunden werden; KI kann dazu dienen, Fähigkeitslücken und funktionale Forderungen zu identifizieren.
- **Beschaffung/Logistik:** KI-gestützte Bedarfsprognosen anwenden; Bestands-/Order-Management; Angebotsbewertung nach Wirtschaftlichkeit/Nutzwert; Software-Upgrades im Betrieb
- **Personal:** KI-Unterstützung bei Personalgewinnung, Lernpfaden und arbeitsplatzintegrierter Weiterbildung
- **Souveränität und Lieferketten:** europäische Kapazitäten aufbauen; exportkontrollkonforme Betriebsmodelle etablieren, Lieferunterbrechungen vermeiden bzw. antizipieren und abfedern.

Resiliente Lieferketten und digitale Souveränität

5. KI nur mit Nutzen entfalten

KI kann die Bundeswehr schneller, präziser und widerstandsfähiger machen – vorausgesetzt, die Organisation ist bereit für einen strategischen Wandel. Ein innovationsfreundlicher Mindset, agile Prozesse in Forschung, Entwicklung und Beschaffung sowie schnelle, bedarfsträgerorientierte Entscheidungen sind Voraussetzung, um die Potenziale von KI effektiv zu nutzen: **Keine KI ohne Nutzwert, aber auch keine Beschränkung ihres Potenzials.**

Ethisch und führungstechnisch bedeutet dies, das Vorsorgeprinzip kritisch zu hinterfragen: Innerhalb der Organisation stärkt es Innovationsfähigkeit und Fehlerkultur; im Konfliktfall ermöglicht es robuste Verteidigungsmittel und die Einhaltung ethischer und rechtlicher Rahmenbedingungen.

Die Bundeswehr kann mit kluger, verantwortungsvoller KI-Nutzung ihre Handlungsfähigkeit und Abschreckung deutlich steigern sowie zugleich die ethische Integrität sichern. Das sollte sie auch angesichts der dynamischen Entwicklungen des Sicherheitsumfeldes jetzt priorisiert angehen.

---

1 Softwaredefinierte Verteidigung zielt darauf, die Potenziale von Software als Motor der militärischen Fähigkeitsentwicklung vollumfänglich nutzbar zu machen.

2 Ethics-by-Design meint die Beachtung von ethischen Aspekten bereits im Entwicklungsprozess.

3 Beobachtungs-Orientierungs-Entscheidungs-Handlungs-Schleifen.

4 Mittels IMSI-Catchern kann der Standort eines Mobiltelefons innerhalb einer Funkzelle eingegrenzt werden.

5 Testmethode zur Bewertung zweier Varianten eines Systems.

Am 30. Oktober 2025 führten das Institut für Organisationskommunikation der Universität der Bundeswehr München (UniBwM), die Estnische Militärakademie (EMA) und die Konrad-Adenauer-Stiftung einen ganztägigen Workshop zur KI-Strategie der Bundeswehr durch. Das vorliegende Papier geht auf diesen Workshop und die Kompetenz der 53 Teilnehmerinnen und Teilnehmer aus Deutschland und Estland zurück, die mit ihrer ausgezeichneten Sachexpertise aus den Bereichen Wissenschaft, Wirtschaft, Verwaltung, Politik und Militär die vorliegende Analyse ermöglicht haben.

Die Autorin und die Autoren:

Natascha Zowislo-Grünewald ist Professorin am Institut für Organisationskommunikation an der Universität der Bundeswehr in München. Ihre Spezialgebiete sind strategische Kommunikation, Sicherheitspolitik, kommunikative Verteidigung und Cognitive Warfare.

Franz Beitzinger ist Soziologe und Senior Research Consultant am Institut für Organisationskommunikation an der Universität der Bundeswehr in München. Seine Spezialgebiete sind Organisationssoziologie und -kommunikation, politische Soziologie und strategische Kommunikation, Digitalisierung, Data Science und empirische Sozialforschung.

Ferdinand Gehringer ist Sicherheitsexperte, Jurist und zertifizierter Mediator. Er ist für ein internationales Wirtschaftsberatungsunternehmen tätig. Seine Expertise umfasst hybride Bedrohungen, Schutz kritischer Infrastrukturen, Cybersicherheit und Krisenvorsorge.

Dierk Spreen ist Soziologe und Gastprofessor für Gesellschaftswissenschaften an der HWR Berlin sowie Senior Project Manager am Institut für Organisationskommunikation an der Universität der Bundeswehr in München. Zu seinen Spezialgebieten zählen disruptive Technologien, Sicherheits- und Militärsoziologie, strategische Kommunikation und kognitive Kriegführung.

Impressum

Herausgeberin: Konrad-Adenauer-Stiftung e. V., 2026, Berlin

Kontakt:
Martin Bieber
Bundeswehr und Gesellschaft
Analyse und Beratung
martin.bieber@kas.de
Tel. +49 30 26996-3525

Bildnachweis Titelseite: IMAGO / Sven Simon
Gestaltung und Satz: Konrad-Adenauer-Stiftung e. V.
Hergestellt mit finanzieller Unterstützung der Bundesrepublik Deutschland.

ISBN 978-3-98574-350-6