Verteidigung im Informationsraum

Warum kommunikative Resilienz zur strategischen Kernfähigkeit werden muss

www.pwc.de

Executive Summary

Kommunikative Resilienz als strategische Kernfähigkeit moderner Verteidigung

Die sicherheitspolitische Realität demokratischer Staaten befindet sich in einem tiefgreifenden Wandel: Verteidigung verlief über Jahrzehnte primär entlang territorialer, militärischer und – zunehmend – cybertechnischer Linien. In den vergangenen Jahren hat sich jedoch der Informationsraum zu einer eigenständigen sicherheitskritischen Domäne entwickelt. Autoritäre Akteure, insbesondere Russland und China, nutzen Foreign Information Manipulation and Interference (FIMI) – koordinierte manipulative Verhaltensweisen in klassischen und digitalen Medien, etwa Falschnachrichten, falsche Nutzer:innenkonten oder künstlich verstärkte Reichweite – systematisch, um demokratische Gesellschaften zu destabilisieren. Im Zentrum steht dabei nicht punktuelle Desinformation, sondern die schleichende Erosion von Vertrauen in Institutionen, Medien und demokratische Entscheidungsprozesse.

Generative Künstliche Intelligenz, automatisierte Kampagnen, Deepfakes und hochskalierbare Verbreitungsmechanismen beschleunigen diese Entwicklung erheblich. Der Informationsraum ist damit nicht länger bloß ein Kommunikationsumfeld, sondern ein zentraler Wirkungsraum moderner Machtprojektion – mit ähnlicher strategischer Relevanz wie klassische militärische und cyberbezogene Domänen.

Europa erkennt diese Bedrohung analytisch sehr klar. Mit dem Strategic Compass, den FIMI-Threat-Reports des Europäischen Auswärtigen Dienstes (EEAS) sowie einer Vielzahl von Analyse- und Resilienzinitiativen verfügt die Europäische Union über ein weit entwickeltes Lageverständnis hybrider Einflussoperationen. Zugleich bleibt die operative, rechtsstaatlich eingebettete und demokratiekonforme Verteidigungsfähigkeit im Informationsraum fragmentiert. Zwischen präziser Analyse und wirksamer Reaktionsfähigkeit klafft eine sicherheitspolitische Lücke.

Der Informationsraum als neue Verteidigungslinie demokratischer Souveränität

Demokratien sind strukturell auf offene, pluralistische und vertrauensbasierte Kommunikationsräume angewiesen. Öffentliche Meinungsbildung, politische Willensbildung und institutionelle Legitimation entstehen im freien Diskurs. Wird dieser Raum systematisch manipuliert, fragmentiert oder polarisiert, verliert Demokratie ihre operative Funktionsfähigkeit. Der Schutz des Informationsraums ist daher keine sicherheitspolitische Nebenfrage, sondern eine demokratische Kernaufgabe. Kommunikative Resilienz dient nicht der Kontrolle von Meinung, sondern der Sicherung der Bedingungen demokratischer Selbstregierung.
Im Cyberraum wurden über Jahre belastbare Schutz- und Reaktionsarchitekturen aufgebaut – mit klaren Mandaten, standardisierten Incident-Response-Prozessen und institutionell verankerten Zuständigkeiten. Für den Informationsraum fehlt eine vergleichbare Architektur bislang. Regulatorische Ansätze, Medienkompetenzprogramme und präventive Kommunikationspolitik sind notwendig, genügen jedoch nicht, um den Informationsraum als kritische Infrastruktur moderner Staatlichkeit wirksam zu schützen.

Die zentrale These dieses Viewpoints lautet daher: Der Informationsraum ist keine „weiche“ politische Arena mehr, sondern eine sicherheitskritische Domäne. Ihr Schutz ist zur Voraussetzung demokratischer Handlungsfähigkeit und strategischer Souveränität geworden. Europa steht vor der Aufgabe, den Schritt von einer überwiegend regulatorisch-präventiven Informationspolitik hin zu einer operativ-resilienten, rechtsstaatlich eingebetteten und demokratiekonformen Sicherheitsarchitektur im Informationsraum zu vollziehen. Kommunikative Resilienz wird damit zur nächsten Verteidigungslinie demokratischer Souveränität. Kommunikative Resilienz wird in dieser Pubilkation als eigenständige sicherheitspolitische Kernfähigkeit verstanden – vergleichbar mit Cyberresilienz und militärischer Verteidigungsfähigkeit. Sie beschreibt die Fähigkeit von Staat und Gesellschaft, Informationsräume systematisch gegen hybride Bedrohungen, FIMI und koordinierte Einflussoperationen zu schützen und auch unter hohem Druck handlungsfähig zu bleiben, ohne demokratische Prinzipien zu unterminieren.

Internationale Best Practices aus Estland, Schweden, Litauen, den Vereinigten Staaten und Österreich zeigen, dass kommunikative Resilienz dort wirksam wird, wo sie institutionell verankert, operativ geführt und demokratiekonform ausgestaltet ist. Entscheidend sind nicht Einzelmaßnahmen, sondern eine kohärente Architektur aus Lageerfassung, Entscheidungsfähigkeit, koordinierter Reaktion und klarer Governance.

Der Viewpoint adressiert die strategische Leerstelle zwischen Analyse und Umsetzung und entwickelt dafür eine Narrative Defence Architecture mit zentralen Bausteinen wie Narrative Command (N-CMD), Narrative Incident Response (NIR), Narrative Integrity Protocols (NIP), Operational Trust Management (OTM), Kommunikationslagezentrum (K-LageZ) und Defence Skills Map (DSM).

Fest steht: Kommunikative Resilienz ist keine Option – sie ist eine Voraussetzung für die Sicherheit Europas im 21. Jahrhundert.

Die vorliegende Publikation ist Teil einer multiperspektivischen Beschäftigung mit dem Thema „Resilienz“ von PricewaterhouseCoopers (PwC Germany) and PwC Strategy& (Germany) GmbH. Ergänzende Studien und Gedankenpapiere zum Thema sind:

- **„Business into breach: Rethinking the Private Sector‘s role in Civil Defence“ (In Kooperation mit der Bundesakademie für Sicherheitspolitik)**
- **„Measuring What Matters: Introducing the National Security & Resilience Index (NSRI)“ (In Kooperation mit der Deutschen Gesellschaft für Auswärtige Politik e. V.)**

Inhaltsverzeichnis

Abstract

Hybride Bedrohungen richten sich zunehmend gegen die kognitiven und kommunikativen Grundlagen demokratischer Systeme. Autoritäre Akteure nutzen Foreign Information Manipulation and Interference (FIMI) – koordinierte manipulative Verhaltensweisen in klassischen und digitalen Medien, etwa Falschnachrichten, falsche Nutzer:innenkonten oder künstlich verstärkte Reichweite. Außerdem setzen sie auf KI-gestützte Einflussoperationen, Deepfakes sowie datenbasierte Manipulationsformen wie Data Poisoning, um Vertrauen in staatliche Institutionen zu unterminieren, politische Entscheidungsprozesse zu verzerren und gesellschaftliche Kohäsion zu schwächen. Der Informationsraum ist damit zu einer eigenständigen strategischen Konfliktdomäne geworden.

Während Europa über hochentwickelte militärische und cyberbezogene Verteidigungsarchitekturen verfügt, bleibt der Informationsraum institutionell und operativ unterverteidigt. Analyseinstrumente sind vorhanden, doch es fehlen standardisierte Verteidigungsmechanismen, klare Zuständigkeiten und integrierte Führungsstrukturen.

Diese Veröffentlichung definiert kommunikative Resilienz als strategische Kernfähigkeit moderner Verteidigung und verankert den Informationsraum als neue Verteidigungslinie demokratischer Souveränität. Auf Basis internationaler Best Practices (Estland, Schweden, Litauen, USA, Österreich) wird eine integrierte Narrative Defence Architecture entwickelt, die technische, organisatorische, operative und kommunikative Schutzmechanismen verbindet. Zentrale Instrumente umfassen unter anderem Narrative Command (N-CMD), Narrative Incident Response (NIR), Narrative Integrity Protocols (NIP), Operational Trust Management (OTM), ein Kommunikationslagezentrum sowie eine Defence Skills Map für das Informationszeitalter. Die Publikation zeigt, wie Demokratien ihre Handlungsfähigkeit sichern können, ohne autoritäre Mittel einzusetzen – durch rechtsstaatliche, transparente und demokratiekonforme Verteidigung des Informationsraums. Das Papier ist kein Forschungsbericht und kein Einsatzhandbuch. Es versteht sich als Strategic Viewpoint, der aufzeigt, wie demokratische Staaten ihre Handlungsfähigkeit im Informationsraum sichern können – rechtsstaatlich, transparent und demokratiekonform.

01

Einleitung

Für eine Narrative Defence Architecture

Die sicherheitspolitische Debatte in Europa hat sich in den vergangenen zehn Jahren grundlegend verschoben. Spätestens die Annexion der Krim im Jahr 2014, die Interventionen Russlands in Syrien, die systematische Destabilisierung der Ukraine sowie vielfältige Einmischungsversuche in westliche Wahlprozesse verdeutlichen, dass militärische Mittel nur noch einen Teil moderner Konfliktaustragung abbilden (Hybrid CoE 2022; Kaljulaid 2019). Der Strategic Compass der Europäischen Union beschreibt diese Entwicklung als einen „Kampf der Narrative“ („battle of narratives“) in einer Welt, in der alles als potenzielle Waffe dienen kann, von Energieinfrastruktur über Lieferketten bis hin zu Information und Kommunikation – „everything is weaponised“ (European Commission 2022).

Diese Verschiebung betrifft jedoch nicht nur militärische oder staatliche Institutionen, sondern die demokratische Ordnung selbst. Informationsräume bilden die infrastrukturelle Grundlage moderner Demokratien: Sie ermöglichen öffentliche Deliberation, gesellschaftliche Selbstverständigung und politische Legitimation. Ihre gezielte Manipulation stellt daher einen Angriff auf die Funktionsbedingungen demokratischer Selbstregierung dar.

Fünfte Generation der Kriegsführung

Sicherheitspolitische Auseinandersetzungen finden in zunehmendem Maß also auch in Räumen statt, die lange primär als politisch-gesellschaftliche, nicht jedoch als sicherheitsrelevante Domänen galten: öffentliche Diskurse, digitale Informationsökosysteme sowie kollektive Sinn- und Deutungsordnungen. Studien des Metis Institute fassen dies als „fünfte Generation“ der Kriegsführung, die vor allem über nicht-kinetische Mittel operiert: Desinformation, Social Engineering, Cyberoperationen und der Einsatz Künstlicher Intelligenz. Diese Art der Konfliktführung zielt darauf ab, Wahrnehmungen, Entscheidungsprozesse und gesellschaftliche Kohärenz zu beeinflussen (Metis Institute 2021; 2023). Zwar sind Angriffe im Informationsraum kein gänzlich neues Phänomen – Feindpropaganda, Desinformation und gezielte Narrativsteuerung sind immer Begleiterscheinungen von Kriegen gewesen – doch sind sie durch neue

Technologien umfassender, schneller und schwieriger zu verteidigen. Konflikte entfalten sich damit zunehmend in einer strategischen Grauzone unterhalb klassischer Kriegsschwellen, mit erheblichen Auswirkungen auf Stabilität, Legitimität und Souveränität demokratischer Staaten.

Die Europäische Union und ihre Mitgliedstaaten haben auf diese Entwicklung reagiert. Mit dem **Joint Framework on Countering Hybrid Threats**, dem **Action Plan against Disinformation** sowie dem Aufbau von Strukturen wie der **EU Hybrid Fusion Cell**, dem **Rapid Alert System** und dem **European Digital Media Observatory** (EDMO) ist ein komplexes Geflecht aus Analyse-, Koordinations- und Präventionsinstrumenten entstanden (European Commission 2016; 2018a; 2018b; 2019; 2020; 2021). Der **Strategic Compass** der Europäischen Kommission sowie sein Fortschrittsbericht von 2024 betonen ausdrücklich die Notwendigkeit, hybride Bedrohungen wie ausländische Foreign Information Manipulation and Interference (FIMI) wirksamer zu bekämpfen und die Resilienz europäischer Gesellschaften zu stärken (European Commission 2022; 2024).

Zugleich konzentrieren sich viele dieser Initiativen weiterhin auf regulatorische, präventive und demokratiefördernde Maßnahmen – etwa Plattformregulierung, Transparenzanforderungen, Wahlrechtsanpassungen und Medienkompetenzprogramme (European Commission 2018a; 2020; 2021). Insbesondere in Deutschland wird Desinformation primär als Herausforderung für Demokratie, Meinungsfreiheit und gesellschaftlichen Zusammenhalt behandelt und sicherheitspolitische Zuständigkeiten sowie operative Reaktionsmechanismen bleiben bislang nur begrenzt entwickelt (Bundestag 2020; BMI 2023; Bundesregierung 2024; DisinfoLab EU 2025).

Demgegenüber sind in anderen sicherheitspolitischen Bereichen hochentwickelte operative Schutzarchitekturen etabliert. Die US-amerikanische Cybersecurity and Infrastructure Security Agency (CISA) verfügt über detaillierte Incident-Response-Playbooks, die den Umgang mit Cybervorfällen von der Detektion über die Eindämmung bis zur Wiederherstellung systematisch strukturieren (CISA 2021). Estland hat mit seiner Cyber Security Strategy 2024–2030 sowie begleitenden Lage- und Resilienzstrukturen ein Modell geschaffen, das staatliche Funktionsfähigkeit auch unter verschärften Sicherheitsbedingungen absichern soll (RIA 2024; 2025). Charakteristisch für diese Ansätze sind klare Mandate, institutionalisierte Lagebilder und trainierte Reaktionsroutinen.

Für den Informationsraum existiert eine vergleichbare operative Verteidigungsarchitektur bislang allenfalls in Ansätzen. Die FIMI-Berichte des EEAS haben seit 2023 ein präzises analytisches Instrumentarium entwickelt: FIMI wird dort als überwiegend nicht-illegales, intentional und koordiniert betriebenes Verhaltensmuster definiert, das politische Prozesse, Werte und Verfahren bedroht und sich entlang einer modellierbaren Angriffskette („Kill Chain“) entfaltet (EEAS 2023; 2024; 2025). Mit Werkzeugen wie dem Threat Analysis Cycle, dem Response Framework und der FIMI Exposure Matrix bestehen konzeptionelle Grundlagen für eine strukturierte Reaktion (EEAS 2024; 2025).

Zwischen analytischer Fähigkeit und operativer Verteidigungswirkung klafft jedoch weiterhin eine strukturelle Lücke. Das Vorbild aus dem Cyberraum kann ein Ansatzpunkt sein, um diese Lücke gezielt zu schließen. Die Herausforderungen des Informationsraums werden im folgenden Kapitel weiter herausgearbeitet und weiterhin bestehende Ansätze für eine Sicherheitsarchitektur im Informationsraum betrachtet und weiterentwickelt.

Ziele des Viewpoints

Dieses Papier argumentiert, dass Europa den Schritt von einer überwiegend regulatorisch-präventiven Informationspolitik hin zu einer operativ-resilienten, rechtsstaatlich eingebetteten Sicherheitsarchitektur im Informationsraum vollziehen muss. Kommunikative Resilienz wird damit zur nächsten Verteidigungslinie demokratischer Souveränität im digitalen Zeitalter – nicht als Instrument staatlicher Kontrolle, sondern als pluralismuskonforme Schutzarchitektur, die Freiheit, offene Diskurse und demokratische Selbstbestimmung absichert.

Kommunikative Resilienz bezeichnet in diesem Beitrag die Fähigkeit von Staat und Gesellschaft, informationsgestützte Angriffe frühzeitig zu erkennen, öffentliche Diskursräume unter Druck funktionsfähig zu halten, demokratiekonforme strategische Kommunikationslinien zu entwickeln und diese Funktionen in eine institutionell verankerte Verteidigungsarchitektur zu überführen. Dabei kann diese Fähigkeit je nach Kontext unterschiedlich ausgestaltet sein. Sie ist auch Teil eines Aushandlungsprozesses zu staatlicher Kontrolle, gesellschaftlicher Teilhabe und eines Maßes an systemischer Funktionalität, die durch die Widerstandsfähigkeit im Informationsraum – die kommunikative Resilienz – erhalten werden soll.

Die Studie verfolgt daher drei Ziele:

Erstens analysiert sie anhand internationaler Beispiele – insbesondere Estland, Schweden, Litauen, die Vereinigten Staaten und Österreich –, wie fortgeschrittene Modelle kommunikativer und psychologischer Verteidigung ausgestaltet sind und wo ihre strukturellen Grenzen liegen (RIA 2024; 2025; Swedish Psychological Defence Agency 2024; GAO 2023).

Zweitens untersucht sie die europäische und nationale Governance-Landschaft im Hinblick auf ihre Fähigkeit, eine kohärente, rechtsstaatlich legitimierte kommunikative Verteidigungslinie auszubilden (European Commission 2016; 2022; EEAS 2024; Bundesregierung 2024).

Drittens entwickelt sie Bausteine für eine Narrative Defence Architecture, die bewährte Konzepte der Cybersecurity auf den Informations- und Diskursraum überträgt – inklusive klarer demokratischer Leitplanken.

02

Problemstellung

Der Informationsraum als strategische Domäne moderner Sicherheitspolitik

Die sicherheitspolitische Umwelt demokratischer Staaten befindet sich in einem tiefgreifenden strukturellen Wandel. Während klassische Verteidigung lange Zeit primär auf territoriale Kontrolle, militärische Abschreckung und zunehmend auf cybertechnische Fähigkeiten fokussiert war, hat sich der Informationsraum in den vergangenen Jahren zu einer eigenständigen sicherheitspolitischen Domäne entwickelt.

Autoritäre Akteure – insbesondere Russland und China – nutzen heute systematisch FIMI, um demokratische Gesellschaften langfristig zu destabilisieren. Ziel ist nicht punktuelle Desinformation, sondern die strategische Erosion von Vertrauen in Institutionen, Medien und demokratische Entscheidungsprozesse. Der Informationsraum fungiert dabei als zentraler Wirkungsraum moderner Machtprojektion: In ihm werden Wahrnehmungen, Narrative, Identitäten und politische Handlungsfähigkeit zugleich beeinflusst. Der Informationsraum ist damit nicht mehr bloß ein Kommunikationsumfeld, sondern eine umkämpfte sicherheitskritische Infrastruktur moderner Staatlichkeit.

Technologische Eskalation hybrider Bedrohungen

Die sicherheitspolitische Relevanz des Informationsraums hat sich durch eine tiefgreifende technologische Transformation grundlegend verändert. Während hybride Einflussoperationen früher primär auf menschliche Akteure, klassische Medien und begrenzte digitale Werkzeuge angewiesen waren, ermöglichen neue Technologien heute eine bislang unbekannte Skalierung, Automatisierung und Präzision strategischer Einflussnahme. Drei Entwicklungen wirken dabei als zentrale technologische Multiplikatoren hybrider Bedrohungen:

1. generative Künstliche Intelligenz,
2. hochautomatisierte Desinformationsinfrastrukturen (Botnetze, Trollfarmen, Content-Fabriken) sowie
3. plattformspezifische algorithmische Verstärkung.

Studien des EEAS zeigen, dass moderne FIMI-Operationen zunehmend KI-gestützte Text-, Bild- und Videogenerierung einsetzen, um glaubwürdige und massenhaft verbreitbare Narrative zu erzeugen, die klassische Prüfmechanismen systematisch unterlaufen (EEAS 2024; 2025). Parallel unterstreichen Analysen des Metis Institute, dass hybride Akteure nicht mehr nur einzelne Kampagnen führen, sondern dauerhafte Einflussarchitekturen aufbauen (Metis Institute 2023). Damit verschiebt sich die Logik hybrider Bedrohungen: Nicht punktuelle Interventionen stehen im Vordergrund, sondern der Versuch dauerhafter kognitiver Raumkontrolle.

Verteidigungsmechanismen gegen derartig flächendeckende und in hoher Schlagzahl stattfindende Eingriffe in den Informationsraum sind bislang in der Regel unwirksam. Die Aufklärung von Desinformation geschieht zum Beispiel zumeist erst dann, wenn die Wirkung bereits entfaltet ist. Auch die Identifikation von Urhebern, das effektive Kontern sowie die Kontrolle und Abschottung bestimmter Informationsräume sind bislang regulativ, technologisch und personell den Angriffen nicht gewachsen.

KI und die strukturelle Überforderung klassischer Sicherheitsinstrumente

Der Einsatz generativer KI markiert einen qualitativen Wendepunkt der hybriden Bedrohungslandschaft. KI-Systeme sind heute in der Lage, realistische Deepfakes zu erzeugen, personalisierte Narrative in Echtzeit anzupassen, Diskursdynamiken algorithmisch zu modellieren und emotionale Trigger gezielt zu verstärken. Gleichzeitig überfordert diese Entwicklung klassische staatliche Reaktionsmodelle: Prüfstellen, Medienaufsicht, Faktenchecks und Plattformregulierung sind strukturell zu langsam, fragmentiert und überwiegend reaktiv.

Sicherheitspolitisch entsteht damit eine institutionelle Asymmetrie: Angreifer operieren mit automatisierter Skalierung, während staatliche Verteidigungsstrukturen weiterhin überwiegend auf manuellen Prozessen beruhen.

Data Poisoning als strukturelle Bedrohung kognitiver Infrastrukturen

Eine bislang unterschätzte Dimension hybrider Bedrohungen ist gezieltes Data Poisoning. Der Begriff beschreibt die systematische Manipulation von Daten, die zur Ausbildung, Feinjustierung oder operativen Nutzung algorithmischer Systeme verwendet werden – insbesondere von KI-gestützten Analyse-, Moderations- und Entscheidungssystemen. Im Kontext des Informationsraums zielt Data Poisoning nicht primär auf einzelne Narrative, sondern auf die epistemische Grundlage, auf der Wahrnehmung, Bewertung und Reaktion überhaupt erst möglich werden.

Hybrid agierende Akteure nutzen offene Informationsökosysteme, soziale Medien, Foren und Nachrichtenseiten, um systematisch verzerrte, polarisierende oder falsche Inhalte in jene Datenströme einzuspeisen, aus denen algorithmische Systeme lernen. Auf diese Weise können Desinformationsmuster, extreme Deutungen oder strategische Narrative schleichend normalisiert und in automatisierte Erkennungs- und Bewertungssysteme eingeschrieben werden (Brundage et al. 2018; NIST 2023).

Im Unterschied zu klassischer Desinformation wirkt Data Poisoning langfristig und strukturell. Frühwarnsysteme, Lagebilder und KI-gestützte Entscheidungsunterstützung werden dadurch selbst Teil der Angriffsfläche. Klassische Instrumente der Plattformaufsicht, Faktenprüfung und Medienkompetenz greifen hier nur begrenzt, da die Manipulation nicht auf Ebene einzelner Inhalte, sondern auf Ebene datenbasierter Lernprozesse stattfindet.

FIMI als neue Systembedrohung

Die FIMI Threat Reports des EEAS definieren FIMI nicht als reines Inhaltsproblem, sondern als strategisches Verhaltensmuster: koordiniert, intentional, überwiegend nicht illegal und gezielt auf politische Prozesse sowie gesellschaftliche Stabilität gerichtet (EEAS 2023; 2024). FIMI ist damit eine Form indirekter Machtprojektion im strategischen Wettbewerb zwischen Staaten.

Im Jahr 2024 dokumentierte der EEAS FIMI-Aktivitäten gegen mehr als 80 Staaten und über 200 Institutionen weltweit. Besonders betroffen waren die Europäische Union, NATO-Mitgliedstaaten, Wahlbehörden, Medienhäuser sowie sicherheitspolitische Akteure (EEAS 2025). Nationale Studien – etwa zur Desinformationslandschaft in Deutschland – dokumentieren langfristige Einflusskampagnen, die gezielt Vertrauen in Institutionen, Medien und demokratische Prozesse unterminieren (DisinfoLab EU 2025; BMI 2023). Die Ukraine fungiert in diesem Kontext als operatives Testfeld für neue hybride Operationsformen, deren Wirkmechanismen die Aggressoren anschließend systematisch auf andere Regionen und politische Kontexte übertragen.

Governance-Lücken im europäischen Sicherheitsgefüge

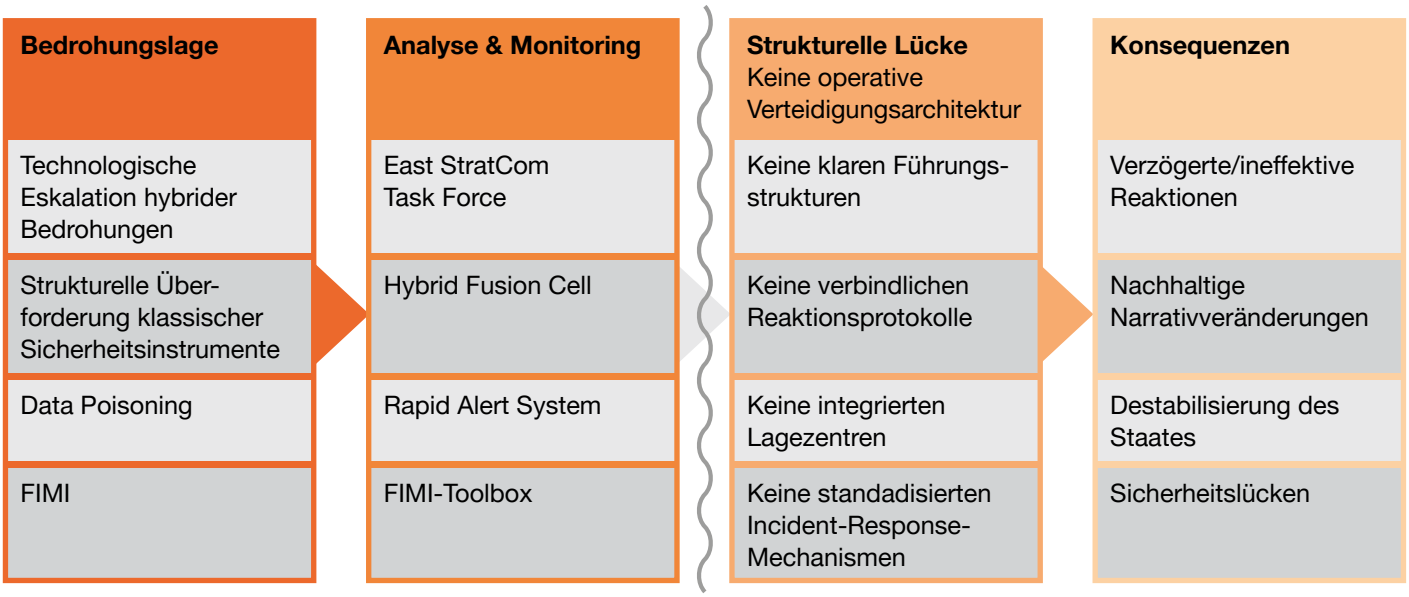
Trotz dieser Bedrohungslage bleibt die institutionelle Antwort Europas strukturell fragmentiert. Zwar existiert ein breites Set an Analyse- und Koordinationsinstrumenten, doch es fehlt eine kohärente operative Verteidigungsarchitektur: durchgängige Führungsstrukturen, verbindliche Reaktionsprotokolle, integrierte Lagezentren und standardisierte Incident-Response-Mechanismen. Diese operative Lücke wird zusätzlich durch föderale Zuständigkeiten, sektorale Silostrukturen und unklare Mandate vertieft (European Commission 2019; EEAS 2024).

Der Schutz des Informationsraums darf zudem nicht mit autoritären Kontrollmechanismen verwechselt werden. Kommunikative Resilienz zielt nicht auf Inhaltssteuerung, Zensur oder staatliche Propaganda, sondern auf die Sicherung der strukturellen Voraussetzungen demokratischer Deliberation: Transparenz, Meinungsfreiheit, Pluralismus und institutionelles Vertrauen. Operative Verteidigungsfähigkeit bedeutet in diesem Kontext die Fähigkeit, demokratische Kommunikationsräume gegen gezielte Destabilisierung zu schützen – nicht sie politisch zu kontrollieren.

Informationsräume bilden die infrastrukturelle Grundlage moderner Demokratie: öffentliche Meinungsbildung, politische Willensbildung und institutionelle Legitimation entstehen im Diskurs. Wird dieser Raum systematisch manipuliert, gerät Demokratie selbst in eine strukturelle Verteidigungslage. Abwehrmechanismen dürfen dabei nicht in Autoritarismus, Zensur oder staatliche Propaganda kippen. Die zentrale Herausforderung moderner Sicherheitspolitik besteht darin, Verteidigungsfähigkeit und demokratische Normbindung gleichzeitig zu sichern.

Im Folgenden betrachten wir internationale Best Practices und neuartige Ansätze der kommunikativen Resilienz. Wir beleuchten, welche institutionellen Modelle kommunikativer Resilienz unter realen sicherheitspolitischen Bedingungen wirksam sind, um daraus Rückschlüsse für eine stringente Verteidigungsstrategie im Informationsraum zu gewinnen.

Abbildung 1 – Die strukturelle Lücke in der Verteidigungsarchitektur im Informationsraum



03

Internationale Best Practices

Die Analyse hybrider Bedrohungen im Informationsraum ist in Europa weit fortgeschritten. Weniger entwickelt ist hingegen die systematische Übersetzung dieses Lagewissens in dauerhaft wirksame institutionelle Strukturen. Ein international vergleichender Blick ist daher nicht nur illustrativ, sondern analytisch notwendig. Er erlaubt es, jene staatlichen Arrangements zu identifizieren, in denen kommunikative Resilienz nicht als punktuelle Maßnahme, sondern als sicherheitspolitische Fähigkeit bereits institutionalisiert ist.

Mehrere demokratische Staaten haben in den vergangenen Jahren begonnen, psychologische, kommunikative und kognitive Verteidigungskomponenten systematisch in ihre nationale Sicherheitsarchitektur zu integrieren. Empirische Vergleichsstudien belegen, dass diese Staaten über eine signifikant höhere Krisenresilienz, schnellere Reaktionsfähigkeit und geringere gesellschaftliche Verwundbarkeit gegenüber hybriden Einflussoperationen verfügen (Hybrid CoE, 2022; GAO, 2023).

Die internationalen Best Practices sind nicht als Vorbilder im normativen Sinne zu verstehen, sondern als analytische Referenzpunkte. Sie zeigen, welche institutionellen Arrangements unter realen politischen, rechtlichen und gesellschaftlichen Bedingungen funktionieren – und welche trotz hoher Analysekapazität strukturell reaktiv bleiben. Für Europa ist dies besonders relevant, da die Bedrohungslage hochgradig vergleichbar ist, die institutionellen Antworten jedoch stark variieren.

Der Mehrwert der Analyse liegt somit darin, übertragbare Strukturprinzipien zu identifizieren: Welche Rolle spielen klare Mandate? Wie werden operative Reaktionsmechanismen organisiert? Wie wird demokratische Legitimität gesichert? Diese Fragen bilden den analytischen Rahmen des folgenden Ländervergleichs.

3.1. Untersuchungslogik und Auswahl der Fallstudien

Ziel der folgenden Fallstudien ist eine strukturierte sicherheitspolitische Analyse, die jene institutionellen Muster herausarbeitet, durch die kommunikative Resilienz operativ wirksam wird. Gleichzeitig soll sie strukturelle Schwächen sichtbar machen, die auch in hochentwickelten Demokratien fortbestehen.

Erstens wird der Institutionalisierungsgrad kommunikativer Verteidigung betrachtet, also die Frage, ob entsprechende Strukturen dauerhaft und mit Mandaten abgesichert und organisatorisch verankert sind. Zweitens wird analysiert, in welchem Umfang staatliche, sicherheitspolitische und gesellschaftliche Akteure integriert werden. Drittens wird geprüft, ob operative Führungs- und Reaktionsstrukturen existieren, die über reine Analyse hinausgehen. Viertens wird die demokratische und rechtsstaatliche Einbettung der Maßnahmen bewertet. Fünftens wird die Übertragbarkeit auf den europäischen Kontext berücksichtigt.

Untersucht werden Estland, Schweden, Litauen, die Vereinigten Staaten und Österreich. Diese Länder repräsentieren unterschiedliche Entwicklungsstufen kommunikativer Resilienz – von hochinstitutionalisierten Modellen bis hin zu emergenten, fragmentierten Ansätzen. Die Analyse ergibt so ein breites analytische Bild verschiedener Ansätze und Stadien kommunikativer Resilienzsysteme.

3.2 Estland – Systemische Cyber- und Informationsresilienz

Estland gilt international als Referenzmodell für die Integration digitaler und informationeller Sicherheit in die staatliche Kernarchitektur. Zentrales Merkmal des estnischen Ansatzes ist das Verständnis von Resilienz nicht als technisches Spezialthema, sondern als Voraussetzung staatlicher Souveränität und Funktionsfähigkeit im digitalen Zeitalter (RIA, 2024). Estland zählt zu den ersten Staaten, die aufgrund seiner frühen digitalen Transformation systematisch Ziel hybrider Bedrohungen wurden. Die koordinierten Angriffe auf staatliche Institutionen, Medienhäuser und kritische Infrastrukturen im Jahr 2007 markieren einen Wendepunkt in der europäischen Sicherheitsarchitektur und prägen bis heute das estnische Sicherheitsverständnis (RIA 2025). In der Folge entwickelte Estland ein Sicherheitskonzept, das weit über klassische technische Cyberabwehr hinausgeht und Informationssicherheit, Vertrauen in staatliche Kommunikation und den Schutz öffentlicher Diskursräume integrativ mit Cyberresilienz verknüpft.

Die estnische Cyber Security Strategy 2024–2030 definiert Cyber- und Informationssicherheit explizit als Querschnittsaufgabe staatlicher Steuerungsfähigkeit. Technische Schutzmaßnahmen werden systematisch mit Governance-, Kommunikations- und Krisenmechanismen verbunden, um staatliche Entscheidungsfähigkeit auch unter hybriden Druckbedingungen zu sichern (RIA, 2024). Der Informationsraum wird damit nicht als nachgelagerte Kommunikationsarena verstanden, sondern als sicherheitsrelevante Wirkdomäne, die strukturell mit Verwaltungs-, Verteidigungs- und Cyberstrukturen gekoppelt ist (RIA, 2025). Staatliche Institutionen, private Plattformen und zivilgesellschaftliche Akteure sind dabei strukturell in den Schutz öffentlicher Diskursräume eingebunden. Charakteristisch ist insbesondere die institutionelle Verzahnung von Lageanalyse, Entscheidungsfindung und staatlicher Kommunikation. Dauerhaft etablierte Analysekapazitäten ermöglichen eine kontinuierliche Bewertung hybrider Bedrohungen, während klar definierte Reaktionslogiken sicherstellen, dass politische Entscheidungen und öffentliche Kommunikation kohärent und belastbar bleiben. Dafür setzt Estland auf ein hoch professionalisiertes Incident-Response-System, ein nationales Cyber-Lagezentrum (RIA), laufende Sensibilisierungskampagnen für Behörden, Unternehmen und Gesellschaft sowie eine klare Perspektive auf den digitalen Raum als „souveräne Grenze“ eines Staates (RIA, 2025). Kommunikative Resilienz entsteht in Estland nicht durch einzelne Kampagnen, sondern durch institutionelle Kontinuität, klare Verantwortlichkeiten und trainierte Routinen.

3.3 Schweden – institutionalisierte, rechtsstaatlich kontrollierte und demokratiekonforme psychologische Verteidigung

Schweden hat mit der Swedish Psychological Defence Agency (Psykologiskt Försvar) eines der wenigen explizit institutionalisierten Modelle psychologischer und kommunikativer Verteidigung in Europa geschaffen. Die Behörde verfügt über ein klares gesetzliches Mandat zur Abwehr ausländischer Informationsmanipulation, zur Förderung gesellschaftlicher Medienresilienz sowie zur systematischen Schulung staatlicher und öffentlicher Akteure im Umgang mit Informationsbedrohungen (Swedish Psychological Defence Agency 2024; MSB 2021). Der schwedische Ansatz ist insofern bemerkenswert, als kommunikative Sicherheit hier nicht als Instrument der Gegenpropaganda, sondern als Schutzfunktion demokratischer Diskursräume konzipiert wird (Swedish Psychological Defence Agency 2024).

Die Behörde agiert durch Analyse und Koordination von Maßnahmen gegen informationsgestützte Einflussoperationen. Operative Maßnahmen zielen nicht auf Inhaltskontrolle, sondern auf die Stabilisierung öffentlicher Kommunikation durch belastbare Lagebilder, institutionelle Abstimmung und die Befähigung staatlicher

sowie gesellschaftlicher Akteure (Swedish Government, 2022). Schweden verankert diese Fähigkeiten fest in seiner nationalen Sicherheitsarchitektur und verzahnt sie eng mit ziviler Krisenvorsorge, strategischer Kommunikation, Nachrichtendiensten, Medienstrukturen und der Zivilgesellschaft. Dadurch entsteht eine operative Verteidigungsarchitektur, die den Informationsraum als eigenständiges sicherheitspolitisches Handlungsfeld behandelt und international als Best Practice gilt.

Im Bericht Strengthening Civil Preparedness betont die schwedische Zivilschutzbehörde MSB, dass Resilienz nicht allein Aufgabe staatlicher Institutionen ist, sondern auf einem konsequenten „whole-of-society approach“ beruht. Staatliche Stellen, Medien, Zivilgesellschaft, Privatwirtschaft und Bürger*innen müssen gemeinsam an der Widerstandsfähigkeit gegenüber Desinformation, psychologischer Einflussnahme und hybriden Bedrohungen arbeiten (MSB 2021). Besonders hervorgehoben wird dabei die Rolle von Vertrauen: Vertrauen in staatliche Institutionen, Medien und öffentliche Kommunikation wird explizit als sicherheitsrelevante Ressource definiert. Die Stärkung dieses Vertrauens gilt in Schweden als zentrale Voraussetzung für gesellschaftliche Stabilität, Krisenfestigkeit und demokratische Handlungsfähigkeit.

Für den europäischen Kontext ist Schweden besonders relevant, weil das Beispiel zeigt, dass kommunikative Verteidigung rechtsstaatlich, transparent und pluralismuskonform organisiert werden kann. Zuständigkeiten sind klar definiert, politische Einflussnahme ist begrenzt und gesellschaftliche Akteure werden systematisch eingebunden. Resilienz wird in Schweden damit als sicherheitspolitische Fähigkeit operationalisiert – nicht als reine Präventions- oder Kommunikationsmaßnahme.

3.4 Litauen – Gesellschaftlich integrierte strategische Kommunikation

Litauen verfolgt einen der umfassendsten europäischen Ansätze zur Integration strategischer Kommunikation in die nationale Sicherheitsarchitektur. Litauen zählt zu den europäischen Staaten mit der am weitesten entwickelten und operativ integrierten Architektur aus strategischer Kommunikation, Sicherheitsbehörden und gesellschaftlicher Resilienz in eine kohärente nationale Verteidigungsarchitektur. Aufgrund seiner geopolitischen Lage und der langjährigen Erfahrung mit russischen Einflussoperationen behandelt Litauen den Informationsraum ausdrücklich als sicherheitsrelevantes Operationsfeld. Zentrale Rolle spielt das nationale Strategic Communication Office, das sicherheitsrelevante Kommunikation, Lageanalyse, Frühwarnung und gesellschaftliche Resilienz organisatorisch bündelt. Maßnahmen zur Bekämpfung von Desinformation, zur Stärkung der Medienkompetenz und zur Einbindung zivilgesellschaftlicher Akteure sind fest in der nationalen Sicherheitsstrategie verankert (Government of

Lithuania 2021). Vor dem Hintergrund wiederholter hybrider Einflussoperationen wird kommunikative Resilienz hier explizit als Bestandteil nationaler Verteidigungsfähigkeit verstanden (Government of Lithuania, 2021; Hybrid CoE, 2022).

Die National Security Strategy des Landes verknüpft Informationssicherheit unmittelbar mit staatlicher Handlungsfähigkeit, gesellschaftlicher Stabilität und der Abwehr hybrider Bedrohungen. Strategische Kommunikation fungiert nicht als unterstützende Nebenfunktion, sondern als sicherheitsrelevante Steuerungsressource, die eng mit sicherheitspolitischer Analyse und Entscheidungsfindung verbunden ist (Government of Lithuania, 2021). Besonders hervorzuheben ist die institutionelle Verzahnung von staatlicher Lageanalyse und öffentlicher Kommunikation. Die Lithuanian Intelligence Services dokumentieren in ihrem **Strategic Communication Report 2012–2022**, dass Litauen systematisch Fähigkeiten zur narrativen Frühwarnung, zur schnellen strategischen Reaktion auf Informationsangriffe und zur Stabilisierung öffentlicher Diskurse aufgebaut hat (Lithuanian Intelligence Services 2022).

Litauen demonstriert damit exemplarisch, wie kommunikative Resilienz nicht als isolierte Kommunikationsfunktion, sondern als integraler Bestandteil nationaler Sicherheitsarchitektur operationalisiert werden kann – mit klaren Zuständigkeiten, operativen Schnittstellen und dauerhafter institutioneller Verankerung. Besonders charakteristisch ist für Litauen die systematische Einbindung gesellschaftlicher Akteure. Medien, Bildungseinrichtungen, Zivilgesellschaft und staatliche Institutionen werden in koordinierten Formaten zusammengeführt. Gesellschaftliches Vertrauen wird explizit als sicherheitsrelevante Ressource behandelt und institutionell geschützt. Litauen verdeutlicht damit, dass kommunikative Resilienz nur dort entsteht, wo staatliche Steuerungsfähigkeit und gesellschaftliche Eigenresilienz strukturell miteinander verbunden sind.

3.5 Vereinigte Staaten – Cognitive Security und Homeland Resilience

Die Vereinigten Staaten verfügen über umfangreiche analytische und forschungsbasierte Kapazitäten zur Untersuchung ausländischer Desinformations- und Einflussoperationen, weisen jedoch eine stark fragmentierte institutionelle Zuständigkeitsstruktur auf. Der Bericht Foreign Disinformation: Defining and Detecting Threats des Government Accountability Office (GAO) kommt zu dem Ergebnis, dass in den USA keine zentrale Behörde existiert, die die Bekämpfung von Desinformation oder Foreign Influence Operations strategisch koordiniert (GAO, 2023).

Die Zuständigkeiten verteilen sich auf eine Vielzahl von Akteuren – darunter Department of Homeland Security, State Department, FBI, CISA, DoD und weitere Behörden – ohne übergreifende Führungs- oder Integrationsstruktur. Diese Fragmentierung erschwert eine kohärente operative Reaktion auf komplexe, langfristige Einflusskampagnen. Gleichzeitig liefern US-amerikanische Analysen einige der präzisesten öffentlich verfügbaren Modelle zur Struktur autoritärer Einflussoperationen. Besonders hervorzuheben ist eine Studie zur kognitiven Sicherheit und demokratischen Resilienz, die detailliert die mehrschichtigen Akteursnetzwerke, Proxy Strukturen, Verstärkungsmechanismen und psychologischen Wirklogiken moderner Desinformationskampagnen dokumentiert (Nabila & Thompsen, 2024).

Der US-Fall zeigt damit exemplarisch: Hohe analytische Exzellenz allein erzeugt keine Verteidigungsfähigkeit, solange institutionelle Integration, klare Zuständigkeiten und operative Steuerungsmechanismen fehlen.Gleichzeitig zeigen Evaluierungen des Government Accountability Office, dass der Umgang mit Desinformation und Foreign Influence Operations durch fragmentierte Zuständigkeiten und fehlende strategische Koordination geprägt ist. Trotz hoher Analysekapazität bleibt dadurch die operative Wirksamkeit begrenzt (GAO, 2023). Das Beispiel USA illustriert, dass Resilienz ohne kohärente Governance – trotz technischer und operativer Exzellenz – unvollständig bleibt.

Für Europa sind die Vereinigten Staaten damit zugleich Best Practice und Warnsignal: Standardisierte Reaktionslogiken sind notwendig, aber ohne klare Mandate, Führungsstrukturen und strategische Integration bleibt kommunikative Verteidigung strukturell limitiert.

3.6 Österreich – Emerging Model mit strukturellen Lücken

Auch Österreich erkennt die sicherheitspolitische Relevanz hybrider Bedrohungen und des Informationsraums zunehmend an. Die Österreichische Sicherheitsstrategie 2024 sowie der Nationale Lagebericht 2025 adressieren Desinformation, hybride Einflussnahme und Konzepte der „intellectual defence“ ausdrücklich als sicherheitspolitische Herausforderungen (Bundesregierung Österreich, 2024; Bundeskanzleramt Österreich, 2025).

Initiativen wie TRANSCEND sowie ausgeweitete Analyseaktivitäten verdeutlichen ein wachsendes strategisches Problembewusstsein. Gleichzeitig bleibt die Umsetzung bislang fragmentiert. Es fehlen dauerhaft institutionalisierte Lagezentren, verbindliche Reaktionsmechanismen und eine durchgängige Koordinationsarchitektur. Kommunikative Resilienz ist damit konzeptionell anerkannt, jedoch operativ noch nicht verankert. Österreich steht insofern exemplarisch für viele europäische Staaten: Die analytische Fähigkeit ist

vorhanden, doch ohne institutionelle Integration bleibt kommunikative Verteidigung überwiegend reaktiv.

Mehrere der Aktivitäten Österreichs zur Stärkung kommunikativer Resilienz sind nicht ausschließlich nationalstaatlich angelegt, sondern Teil europäischer Kooperations- und Pilotprojekte. Programme wie TRANSCEND sind EU-geförderte Vorhaben, an denen österreichische Akteure – darunter staatliche Stellen sowie Organisationen wie das Österreichische Rote Kreuz – beteiligt sind. Diese Projekte leisten einen wichtigen Beitrag zur Erprobung, Vernetzung und konzeptionellen Weiterentwicklung kommunikativer Resilienz auf europäischer Ebene. Sie ersetzen jedoch keine dauerhaft institutionalisierte nationale Verteidigungsarchitektur für den Informationsraum.

Die Relevanz Österreichs im Ländervergleich liegt daher weniger in der bereits erreichten operativen Reife, sondern in seiner Rolle als Test- und Lernumfeld innerhalb europäischer Resilienzinitiativen. Der Fall Österreich verdeutlicht exemplarisch die strukturelle Lücke zwischen projektbasierter Innovationsförderung und sicherheitspolitischer Institutionalisierung kommunikativer Verteidigung.

3.7 Die Verteidigung des Informationsraums als operative Sicherheitsaufgabe

Der Ländervergleich zeigt ein konsistentes Muster: Entscheidend ist nicht die Existenz einzelner Instrumente, sondern die Kombination aus klaren Mandaten, dauerhaften Lage- und Analysefähigkeiten, trainierten Reaktionsroutinen und gesellschaftlicher Einbettung (Hybrid CoE, 2022; GAO, 2023). Dort, wo kommunikative Resilienz institutionell verankert, operativ geführt und gesellschaftlich eingebettet ist, ist die staatliche Handlungsfähigkeit im Informationsraum signifikant größer.

Operativ – unter klarer rechtsstaatlicher Kontrolle und demokratischer Legitimation – lässt sich diese Aufgabe in drei miteinander verzahnte Funktionsbereiche gliedern. Erstens erfordert sie **dauerhafte Hybrid-Detection-Fähigkeiten**, die über reine Medienbeobachtung hinausgehen. Dazu zählen die systematische Erkennung von Bedrohungsindikatoren, die Analyse koordinierter Einflussmuster sowie die frühzeitige Identifikation hybrider Eskalationsdynamiken. Ohne ein kontinuierliches Lagebild bleibt staatliches Handeln reaktiv und zeitlich verzögert (Hybrid CoE, 2022).

Zweitens ist eine **Narrative Incident Response** erforderlich, die informationsgestützte Angriffe nicht nur analysiert, sondern operativ beantwortet. Dazu gehören die Bewertung narrativer Wirkung, die Priorisierung von Reaktionsoptionen sowie koordinierte kommunikative Maßnahmen. Entscheidend ist dabei nicht Gegenpropaganda, sondern die Sicherung staatlicher Handlungsfähigkeit und öffentlicher Orientierung unter Krisenbedingungen (CISA, 2021; GAO, 2023).

Drittens setzt wirksame kommunikative Verteidigung eine **belastbare Governance- und Response-Architektur** voraus. Klare Zuständigkeiten, institutionalisierte Lagezentren, definierte Alarmketten und abgestimmte Koordinationsmechanismen sind die Voraussetzungen dafür, dass Analyse, Entscheidung und Kommunikation nicht fragmentiert nebeneinanderstehen, sondern operativ zusammenwirken. Internationale Vergleichsstudien zeigen, dass gerade diese Governance-Ebene in vielen europäischen Staaten die zentrale Schwachstelle darstellt (Hybrid CoE, 2022).

Die Verteidigung des Informationsraums ist damit keine Erweiterung bestehender Kommunikationspolitik, sondern erfordert eine sicherheitspolitische Transformation: Kommunikative Resilienz wird zu einer operativen Fähigkeit, die Analyse, Reaktion und Governance systematisch verbindet. Für Europa folgt daraus: Die Stärke liegt bereits in Analyse und Koordination – die zentrale Schwäche bleibt die fehlende operative Integration in eine kohärente Verteidigungsarchitektur des Informationsraums. Die internationale Vergleichsanalyse zeigt konsistent: Kommunikative Resilienz entfaltet ihre sicherheitspolitische Wirkung nur dort, wo sie institutionell verankert, operativ geführt und demokratisch legitimiert ist. Entscheidend ist dabei nicht die Vielzahl einzelner Instrumente, sondern ihre systematische Integration in eine kohärente Sicherheitsarchitektur.

Aus diesen empirischen Befunden ergibt sich eine grundlegende strategische Schlussfolgerung: Der Schutz des Informationsraums ist nicht länger eine ergänzende Kommunikationsaufgabe, sondern eine Frage strategischer Souveränität. Die Fähigkeit, öffentliche Diskursräume, institutionelles Vertrauen und demokratische Entscheidungsprozesse unter Bedingungen hybrider Einflussnahme stabil zu halten, wird selbst zu einem zentralen Macht- und Sicherheitsfaktor moderner Staatlichkeit. Vor diesem Hintergrund wird im folgenden Kapitel die konzeptionelle Einordnung kommunikativer Resilienz als neue Dimension strategischer Souveränität vorgenommen.

04

Kommunikative Resilienz als Dimension strategischer Souveränität

Kommunikative Resilienz entfaltet dort ihre volle sicherheitspolitische Wirkung, wo sie als eigenständige Fähigkeit verstanden und institutionell verankert wird. Aus der vergleichenden Analyse internationaler Fallstudien ergibt sich eine zentrale strategische Schlussfolgerung: Der Schutz des Informationsraums ist keine Ergänzung bestehender Sicherheitskonzepte, sondern eine Kernfrage strategischer Souveränität im digitalen Zeitalter.

Während für physische Infrastrukturen, militärische Systeme und den Cyberraum hochentwickelte Schutz- und Reaktionsarchitekturen exsistieren, fehlt für den Informationsraum bislang eine vergleichbare Sicherheitsarchitektur. Regulierung, Medienkompetenz und Präventionsprogramme sind notwendige Bestandteile demokratischer Resilienz, reichen jedoch nicht aus, um diesen Raum als kritische Infrastruktur moderner Staatlichkeit wirksam zu schützen. Erforderlich ist ein Paradigmenwechsel: von überwiegend präventiv-regulativen Ansätzen hin zu einer operativ-resilienten, rechtsstaatlich eingebetteten Verteidigungsarchitektur.

Kommunikative Resilienz als neue sicherheitspolitische Kernfähigkeit

Kommunikative Resilienz bezeichnet die Fähigkeit von Staat und Gesellschaft, den Informationsraum als kritische Infrastruktur zu stabilisieren, ihn systematisch vor hybriden Angriffen zu schützen und auch unter hohem Druck dauerhaft handlungsfähig zu bleiben.

Diese Fähigkeit erfüllt alle Kriterien einer sicherheitspolitischen Kernfähigkeit:

- Sie schützt staatliche Steuerungsfähigkeit,
- sie sichert gesellschaftliches Vertrauen,
- sie verhindert strategische Destabilisierung unterhalb klassischer Kriegsschwellen,
- und sie entscheidet über die Wirksamkeit sämtlicher anderer Verteidigungsinstrumente.

Kommunikative Resilienz steht damit auf einer Ebene mit militärischer Verteidigungsfähigkeit, Cyberresilienz sowie wirtschaftlicher und ziviler Krisenfestigkeit. Sie ist keine Ergänzung bestehender Sicherheitskonzepte, sondern eine eigenständige sicherheitspolitische Domäne.

Ein zentrales Missverständnis gegenwärtiger Debatten besteht darin, kommunikative Resilienz mit Zensur, staatlicher Propaganda oder Einschränkung der Meinungsfreiheit gleichzusetzen. Die Fallstudien aus Schweden, Litauen und Estland zeigen jedoch, dass demokratiekonforme Verteidigung im Informationsraum möglich ist.

Rechtsstaatliche kommunikative Resilienz bedeutet daher:
- Verteidigung ohne Autoritarismus,
- Sicherheit ohne Zensur,
- Resilienz ohne Propaganda.

In diesem Sinne wird Verteidigung nicht zur Einschränkung demokratischer Freiheit, sondern zu ihrer strukturellen Voraussetzung. Kommunikative Resilienz bildet damit eine zentrale Verteidigungslinie demokratischer Souveränität im digitalen Zeitalter.

Aus dieser Analyse folgt eine klare sicherheitspolitische Konsequenz: Der Informationsraum muss in Europa formell als kritische Infrastruktur anerkannt und entsprechend geschützt werden. Dies erfordert den systematischen Aufbau einer operativ-resilienten, rechtsstaatlich eingebetteten Sicherheitsarchitektur, die Analyse, Governance und Reaktionsfähigkeit institutionell integriert.

05

Neues Innovationspaket

Operative Architektur kommunikativer Resilienz

Die zentrale strategische Leerstelle europäischer Sicherheitspolitik liegt nicht im Mangel an Analyse, sondern im Fehlen einer operativen Verteidigungsarchitektur. Während für den Cyberraum über Jahre hinweg – wie bereits beschrieben – Incident-Response-Strukturen, Frühwarnsysteme, Fähigkeitsprofile und Governance-Modelle aufgebaut wurden, existiert für den Informationsraum bislang kein vergleichbares, institutionell verankertes Verteidigungsmodell (EEAS 2024; Hybrid CoE 2022). Nachfolgend beschreiben wir ein integriertes Innovationspaket, das diese Lücke schließt und kommunikative Resilienz als vollwertige Verteidigungsdomäne operationalisiert. Dabei wird sich an bereits etablierten Strukturen aus anderen Sicherheitsstrukturen orientiert, die als etablierte Architekturen bereits eine vernetzte Wirksamkeit unter Beweis stellen konnten. Die daraus entstehende Narrative Defence Architecture überführt kommunikative Resilienz von einem abstrakten Leitbild in eine konkret handhabbare staatliche Fähigkeit.

Narrative Command (N-CMD)

Narrative Command (N-CMD) wird als neue strategische Führungsdomäne definiert, die operativ wirksam, rechtsstaatlich legitimiert und demokratiekonform ausgestaltet ist. Moderne Konflikte werden zunehmend durch die Kontrolle von Deutungsräumen, Wahrnehmungen und gesellschaftlichem Vertrauen (mit) entschieden. Dennoch existiert bislang keine institutionell verankerte Führungsdomäne für diese Wirkdimension. Narrative Command (N-CMD) ist diese neue strategische Führungsdomäne – analog zu etablierten Domänen (Land, Luft, See, Cyber und Weltraum).

N-CMD umfasst

- eine kontinuierliche narrative Lageführung,
- die Integration narrativer Effekte in die Operationsplanung (OPLAN/CONOPS),
- die strategische Steuerung staatlicher Kommunikationslinien sowie
- die systematische Wirkungsanalyse von Informationsoperationen.

Damit entsteht eine kohärente narrative Führungsfähigkeit auf strategischer und operativer Ebene.

Narrative Incident Response (NIR)

Der Informationsraum benötigt ein funktionales Pendant zur Cyber-Incident-Response.

Narrative Incident Response (NIR) beschreibt ein standardisiertes Verfahren zur

- Erkennung narrativer Angriffe,
- Eindämmung schädlicher Wirkungen,
- Stabilisierung öffentlicher Diskursräume und
- Wiederherstellung gesellschaftlichen Vertrauens.

NIR operiert mit klar definierten Eskalationsstufen, Zuständigkeiten, Reaktionsprotokollen und politischen Freigabemechanismen – analog zu bewährten Cyber-Playbooks (CISA 2021; EEAS 2024).

Damit wird der Übergang vom reaktiven Krisenmanagement hin zu systematischer Verteidigung des Informationsraums vollzogen. Narrative Incident Response zielt nicht auf Gegen-Narrative oder staatliche Deutungshoheit, sondern auf die Stabilisierung öffentlicher Orientierung und institutioneller Handlungsfähigkeit unter Bedingungen gezielter Manipulation.

Narrative Integrity Protocols (NIP)

Während technische Systeme durch Cybersecurity-Standards abgesichert werden, fehlt bislang ein vergleichbarer institutioneller Schutzrahmen für staatliche Kommunikation. Narrative Integrity Protocols (NIP) schließen diese Lücke.

Sie umfassen unter anderem

- Validierungsroutinen staatlicher Kommunikation,
- Konsistenzprüfungen zwischen Behörden,
- klar definierte Kommunikationskorridore in Krisenlagen,
- abgestufte Eskalationsmodelle,
- verbindliche Transparenzstandards sowie
- forensische Verfahren zur Erkennung und Attribution von Deepfakes.

NIP standardisieren die narrative Verteidigungsfähigkeit staatlicher Institutionen und erhöhen damit strukturell die Widerstandsfähigkeit des Informationsraums (EEAS 2024; Hybrid CoE 2022).

Operational Trust Management (OTM)

Vertrauen ist keine abstrakte Größe, sondern ein strategischer Wirkfaktor moderner Sicherheitspolitik. Operational Trust Management (OTM) integriert Vertrauen systematisch in

- Lagebilder,
- Entscheidungsprozesse,
- Krisenkommunikation und
- Einsatzplanung.

In diesem Rahmen entstehen neue Rollenprofile – etwa Strategic Trust Officers –, die Vertrauensindikatoren kontinuierlich bewerten und die Stabilität gesellschaftlicher Wahrnehmung aktiv steuern.

Kommunikationslagezentrum (K-LageZ)

Analog zu nationalen Cyber-Lagezentren wird ein Kommunikationslagezentrum (K-LageZ) etabliert, das die kontinuierliche Echtzeit-Analyse von

- Narrativen,
- Diskursverschiebungen,
- emotionalen Resonanzmustern sowie
- Bot- und Kampagnenaktivitäten bündelt.

Das K-LageZ bildet das operative Herz der kommunikativen Verteidigung. Es arbeitet ausschließlich mit offenen, rechtmäßig zugänglichen Informationsquellen (OSINT) und analysiert aggregierte Muster, nicht individuelle Inhalte oder Akteure.

Defence Skills Map (DSM)

Die Defence Skills Map übersetzt kommunikative Resilienz in konkrete sicherheitspolitische Fähigkeitsprofile. Neue Bedrohungen erfordern neue Rollen, Kompetenzen und Ausbildungswege – analog zu Cyber- oder Intelligence-Reformen.

Demzufolge erfordert Kommunikative Resilienz neue Kompetenzprofile:

- **Narrative Analysts** analysieren systematisch dominante, konkurrierende und feindliche Narrative im Informationsraum, identifizieren deren Ursprünge, Wirkmechanismen und Zielgruppen und liefern damit die analytische Grundlage für staatliche Reaktions- und Präventionsmaßnahmen.
- **Cognitive Defence Specialists** fokussieren auf die psychologischen und kognitiven Wirkdimensionen hybrider Bedrohungen. Sie entwickeln Schutz- und Resilienzstrategien gegen manipulative Einflussnahme, insbesondere im Kontext von Desinformation, emotionaler Polarisierung und KI-gestützter Beeinflussung.

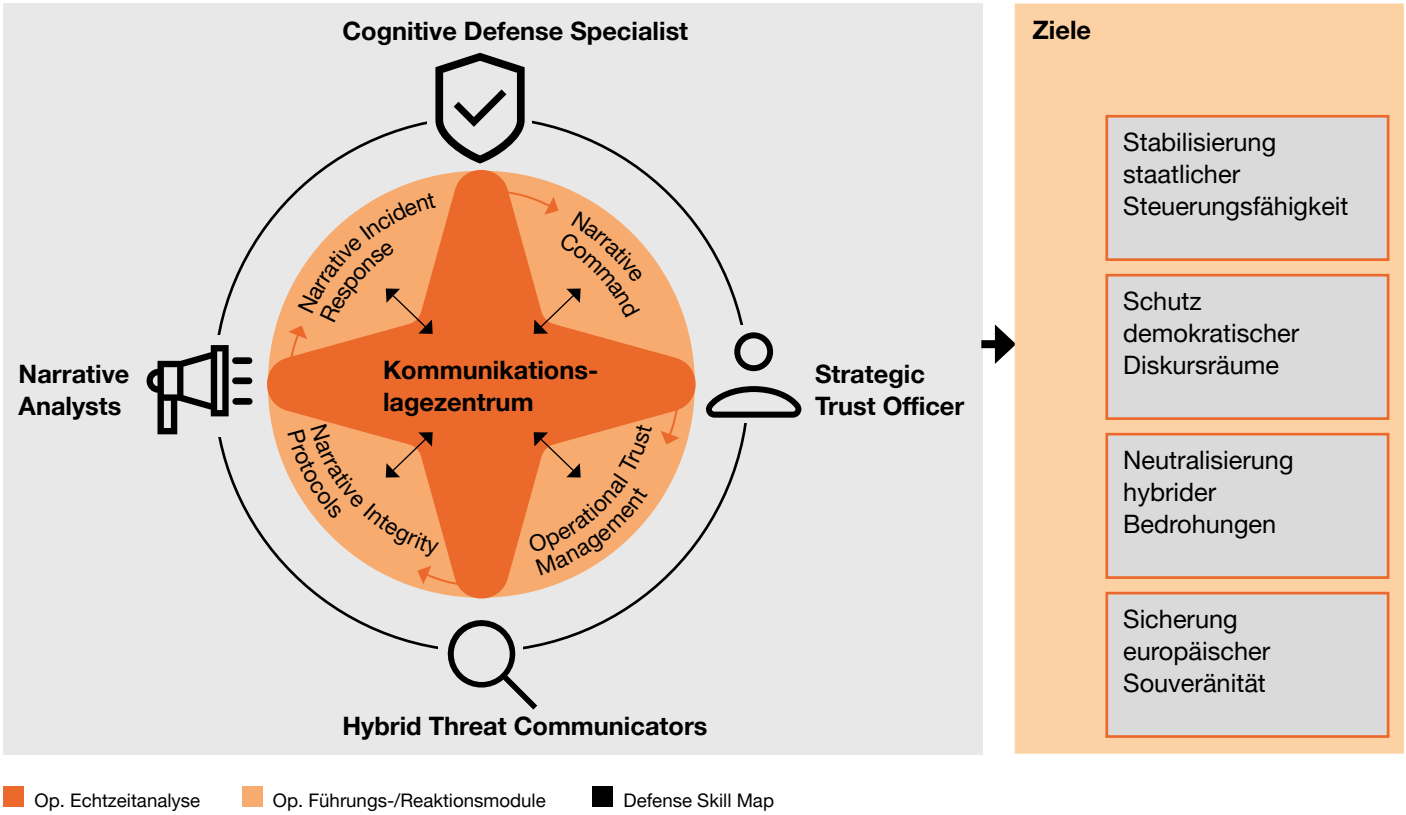
- **Hybrid Threat Communicators** gehen aktiv in die Kommunikation in Informationsräumen, die von hybriden Bedrohungen betroffen sind. Sie wirken damit effektiv FIMI-Operationen entgegen.
- **Strategic Trust Officers** sind für den strategischen Aufbau, die Pflege und den Schutz institutionellen Vertrauens verantwortlich. Sie bewerten die Auswirkungen staatlicher Kommunikation auf Legitimität, Glaubwürdigkeit und gesellschaftliche Kohäsion und koordinieren entsprechende Maßnahmen ressortübergreifend.

Die Defence Skills Map bildet diese Fähigkeiten systematisch ab und verankert sie in Rekrutierung, Ausbildung und Karrierewegen staatlicher und sicherheitsrelevanter Institutionen.

Gemeinsam formen diese Bausteine eine geschlossene Narrative Defence Architecture. Sie

- stabilisiert staatliche Steuerungsfähigkeit,
- schützt demokratische Diskursräume,
- neutralisiert hybride Destabilisierungsstrategien und
- sichert europäische Souveränität im Informationszeitalter ab.

Abbildung 2 – Operative Architektur Kommunikativer Resilienz



Damit liegt ein umsetzbarer Ansatz vor, der kommunikative Resilienz als rechtsstaatlich eingebettete und demokratiekonforme Kernfähigkeit operationalisiert. Im Schlusskapitel wird daraus abgeleitet, welche strategischen Konsequenzen sich für Europa ergeben – und welche nächsten Schritte für Aufbau, Institutionalisierung und Governance einer Verteidigungsarchitektur im Informationsraum prioritär sind.

06

Schluss

Was das für Europa bedeutet

Europa steht an einem sicherheitspolitischen Wendepunkt. Hybride Bedrohungen, FIMI, KI-basierte Einflussoperationen und der strukturelle Umbau des Informationsraums haben die Logik moderner Konfliktführung grundlegend verändert. Macht wird im 21. Jahrhundert nicht mehr primär über Territorium oder militärische Präsenz projiziert, sondern über Deutung, Wahrnehmung, Vertrauen und politische Handlungsfähigkeit.

Die vorliegende Studie zeigt: Die eigentliche strategische Schwäche Europas liegt nicht im Mangel an Analyse oder Regulierung, sondern in der fehlenden institutionellen und operativen Fähigkeit, den Informationsraum als sicherheitskritische Domäne systematisch zu verteidigen. Der Informationsraum ist zur neuen Verteidigungslinie demokratischer Souveränität geworden. Kommunikative Resilienz bildet die dafür notwendige strategische Kernfähigkeit moderner Sicherheitspolitik.

Solange diese Fähigkeit nicht systematisch aufgebaut, institutionell verankert und operativ geführt wird, bleibt Europas Sicherheitsarchitektur strukturell unvollständig – unabhängig von militärischer Stärke, wirtschaftlicher Leistungsfähigkeit oder technologischer Innovationskraft. Zugleich zeigt die Analyse internationaler Best Practices, dass dieser Paradigmenwechsel weder normativ problematisch noch demokratietheoretisch riskant ist. Demokratische Staaten können den Informationsraum wirksam verteidigen, ohne ihre eigenen Grundwerte zu unterminieren. Im Gegenteil: Der Schutz von Informationsräumen, Vertrauen und öffentlicher Deliberation ist die Voraussetzung dafür, dass Demokratie im digitalen Zeitalter überhaupt handlungsfähig bleibt.

Europa verfügt bereits über eine außerordentlich starke analytische Grundlage: die FIMI-Threat-Reports des EEAS, umfangreiche Hybridanalysen, technologische Frühwarnsysteme und zahlreiche nationale Best Practices. Was bislang fehlt, ist deren systematische Übersetzung in eine kohärente operative

Verteidigungsarchitektur.
Mit dieser Studie geben wir einen Impuls zur Entwicklung kommunikativer Resilienz als sicherheitspolitische Kernfähigkeit. Dafür definieren und integrieren wir:

- eine neue Verteidigungsdomäne: den Informationsraum,
- eine neue sicherheitspolitische Kernfähigkeit: kommunikative Resilienz,
- eine konkrete Verteidigungsarchitektur: die Narrative Defence Architecture,
- sowie ein umsetzbares Maßnahmenpaket: Narrative Command (N-CMD), Narrative Integrity Protocols (NIP), Kommunikationslagezentren (K-LageZ), Defence Skills Map, Operational Trust Management und Narrative Incident Response.

Kommunikative Resilienz ist kein kommunikationspolitisches Zusatzthema, sondern Ausdruck eines sicherheitspolitischen Fähigkeitswandels. Sie ist keine Einschränkung demokratischer Freiheit, sondern deren strukturelle Voraussetzung im digitalen Zeitalter. In Verbindung mit gesamtgesellschaftlichen Resilienzansätzen entsteht so ein kohärentes europäisches Sicherheitsmodell für das Informationszeitalter: von der strategischen Bedrohungsanalyse über die sicherheitspolitische Neudefinition bis hin zur operativen Implementierung.

Kommunikative Resilienz schützt nicht nur staatliche Steuerungsfähigkeit, sondern die offene Gesellschaft selbst. Sie ist keine Einschränkung demokratischer Freiheit, sondern ihre strukturelle Voraussetzung im digitalen Zeitalter.

Bibliografie

Brundage, M., Avin, S., Clark, J., et al. (2018). The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation. Oxford: Future of Humanity Institute.

Bundeskanzleramt Österreich (2025). Gesamtstaatliches Lagebild. Wien.

Bundesministerium des Innern (BMI)Bundesministerium des Inneren (BMI) (2023). Verfassungsschutzbericht 2023. Berlin.

Bundesregierung (2024). Integrierte Sicherheit für Deutschland. Nationale Sicherheitsstrategie. Berlin.

Bundesregierung Österreich (2024). Österreichische Sicherheitsstrategie. Wien.

Bundestag (2020). Desinformation mit Wahrheit und Transparenz begegnen. Drucksache 19/22870. Berlin.

Cybersecurity and Infrastructure Security Agency (CISA) (2021). Cybersecurity Incident & Vulnerability Response Playbooks. Washington, DC.

DisinfoLab EU (2025). Disinformation Landscape in Germany. Berlin / Brussels. https://www.disinfo.eu/publications/disinformation-landscape-in-germany/?post_type=publication&p=26967 (zuletzt aufgerufen: 20.01.2026).

European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE) (2022). Digitalization and hybrid threats: Assessing the vulnerabilities for European security. Helsinki.

European Commission (2016). Joint Framework on Countering Hybrid Threats. Brussels.

European Commission (2018a). Action Plan against Disinformation. Brussels.

European Commission (2018b). EU Code of Practice on Disinformation. Brussels.

European Commission (2019). EU-wide Risk Assessment on Disinformation. Brussels.

European Commission (2020). European Democracy Action Plan. Brussels.

European Commission (2021). Strengthened Code of Practice on Disinformation. Brussels.

European Commission (2022). A Strategic Compass for Security and Defence. Brussels.

European Commission (2024). Strategic Compass Progress Report. Brussels.

European External Action Service (EEAS) (2023). First Report on Foreign Information Manipulation and Interference (FIMI). Brussels.

European External Action Service (EEAS) (2024). Second Report on Foreign Information Manipulation and Interference (FIMI). Brussels.

European External Action Service (EEAS) (2025). Third Report on Foreign Information Manipulation and Interference (FIMI). Brussels.

Government Accountability Office (GAO) (2023). Foreign Disinformation: Defining and Detecting Threats. Washington, DC.

Government of Lithuania (2021). National Security Strategy. Vilnius.

Kaljulaid, K. (2019). The Future of European Security. Munich Security Conference Speech.

Lithuanian Intelligence Services (2022). National Threat Assessment 2022 of the Republic of Lithuania. Vilnius.

Nabila, Mohammed Hafiz & Thompson, Matilda (2024). Countering Foreign Influence: The Role of Strategic Communications in National Security Policy Making in the United Stated. Johnson City/Ghana.

National Institute of Standards and Technology (NIST) (2023). Adversarial Machine Learning: A Taxonomy and Terminology of Attacks and Mitigations. Gaithersburg, MD.

Republic of Estonia Information System Authority (RIA) (2024). Cyber Security Strategy 2024–2030. Tallinn.

Republic of Estonia Information System Authority (RIA) (2025). Annual Cyber Security Review. Tallinn.

Swedish Civil Contingencies Agency (MSB) (2021). Strengthening civil preparedness. Karlstad.

Swedish Government (2022). Total Defence 2021–2025. Stockholm.

Swedish Psychological Defence Agency (2024). Psychological Defence: Concepts and principles for the 2020s. MPF Report Series. Stockholm.

Tsetsos, Dr. Konstantinos, Metis Institut für Strategie und Vorausschau (Metis Institute) (2021). Neue hybride Bedrohungen. Metis Studie Nr. 26. München.

Tsetsos, Dr. Konstantinos, Metis Institut für Strategie und Vorausschau (Metis Institute) (2023). Trends und Entwicklungen hybrider Bedrohungen. Metis Studie Nr. 35. München.

Abbildungsverzeichnis

Kontakt

Prof. Dr. Rainer Bernnat
Partner und Leiter Öffentlicher Sektor, PwC Deutschland
E-Mail: rainer.bernnat@pwc.com

Dr. Wolfgang Zink
Partner, PwC Deutschland
E-Mail: wolfgang.zink@pwc.com

Autor:innen

Marleen Naili
Senior Manager, PwC Deutschland
E-Mail: **marleen.naili@pwc.com**

Paul Malte Behne
Wissenschaftlicher Leiter DSI, Strategy& Deutschland
E-Mail: paul.malte.behne@pwc.com

Dr. Florian Andresen
Unabhängiger Wissenschaftler und fachlicher Experte
(Verteidigungsinnovation und Resilienz)

Über uns

Unsere Mandanten stehen tagtäglich vor vielfältigen Aufgaben, möchten neue Ideen umsetzen und suchen unseren Rat. Sie erwarten, dass wir sie ganzheitlich betreuen und praxisorientierte Lösungen mit größtmöglichem Nutzen entwickeln. Deshalb setzen wir für jeden Mandanten, ob Global Player, Familienunternehmen oder kommunaler Träger, unser gesamtes Potenzial ein: Erfahrung, Branchenkenntnis, Fachwissen, Qualitätsanspruch, Innovationskraft und die Ressourcen unseres Expert:innennetzwerks in 136 Ländern. Besonders wichtig ist uns die vertrauensvolle Zusammenarbeit mit unseren Mandanten, denn je besser wir sie kennen und verstehen, umso gezielter können wir sie unterstützen. PwC Deutschland. Mehr als 15.000 engagierte Menschen an 20 Standorten.

Rund 3,27 Mrd. Euro Gesamtleistung. Führende Wirtschaftsprüfungs- und Beratungsgesellschaft in Deutschland.