



Research Paper

Geschlossen gegen Manipulation: Integriertes Modell zur Bewältigung ausländischer Einflussversuche (FIMI)

Lea Frühwirth

Juni 2025

Zentrale Befunde

- „FIMI“ – kurz für „Foreign Information Manipulation and Interference“ – beschreibt den Versuch von Staaten, die öffentliche Meinung in anderen Staaten zu manipulieren, um Gesellschaften zu destabilisieren. Es liegt daher im Kerninteresse demokratischer Staaten, ihre Bevölkerung bestmöglich vor solchen Manipulationsversuchen zu schützen.
- Um der Komplexität von FIMI-Risiken angemessen zu begegnen, reichen punktuelle und reaktive Ansätze nicht aus. Vielmehr muss zielgerichtet, systematisch und kombiniert vorgegangen werden, um alle verfügbaren Bewältigungspotenziale auszuschöpfen. Dazu braucht es ein fundiertes Problemverständnis, die Ableitung des passenden Lösungsraumes, eine breite Maßnahmenauswahl und die Kooperation aller zugehörigen Bewältigungs-Akteur:innen. Die Integration dieser Aspekte in ein gut abgestimmtes Umsetzungsmodell ist Voraussetzung für eine wirksame, effiziente und nachhaltige FIMI-Bewältigung.
- Die konkrete Ausgestaltung des Vorgehens muss neben der inhaltlichen Zielsetzung weitere strukturelle Anforderungen erfüllen, um wirksam und nachhaltig einsetzbar zu sein. Insbesondere der Prävention von potenzieller missbräuchlicher Nutzung muss von vornherein Sorge getragen werden.
- Während die perfekte, allumfassende Strategie bisher noch nicht entwickelt wurde, liegen vielfältige Beispiele einzelner Maßnahmen, Rahmenwerke, Institutionalisierungsformen und Prozessgestaltungen vor, die eine hilfreiche Abprungbasis für die Entwicklung eigener Konzepte bieten.
- CeMAS stellt mit dem integrierten Modell zur Bewältigung ausländischer Einflussversuche ein umfassendes Konzept vor, das einzelne Ansätze in ein großes Ganzes integriert. Angegriffene Werte werden frühzeitig geschützt und gestärkt. Akute Vorfälle werden zeitnah eindämmt und die Qualität und Anpassungsfähigkeit des Vorgehens wird kontinuierlich weiterentwickelt. Die systematische, fallbezogene Kombination von Bewältigungsansätzen in der Kooperation vielfältiger Bewältigungs-Akteur:innen bildet einen widerstandsfähigen und nachhaltigen Schutzschild um die Bevölkerung. Dieser Schutzschild ist dann der Entwicklungsgeschwindigkeit und Volatilität des Problemphänomens gewachsen.

Manipulation der öffentlichen Meinung zur Destabilisierung von Gesellschaften

Wenn Staaten versuchen, die öffentliche Meinung in anderen Staaten zu manipulieren, um eigene Ziele zu verfolgen, wird dies als „FIMI“ bezeichnet. Die englische Abkürzung steht für “Foreign Information Manipulation and Interference”. Typischerweise geht es dabei sowohl um die Vermittlung konkreter Narrative als auch um die Destabilisierung der anvisierten Gesellschaft, etwa durch Desinformationskampagnen oder irreführende Mehrheitssimulation (Deutsche Bundesregierung, 2025). Über Jahre hinweg soll auf diese Weise die öffentliche Meinung beispielsweise zum russischen Angriffskrieg gegen die Ukraine, aber auch gegenüber der deutschen Politik und Regierung, gegenüber der Integrität von Wahlen oder gegenüber Qualitätsmedien beeinflusst werden. Ängste und Unsicherheiten werden geschürt, Misstrauen gesät und Reizthemen instrumentalisiert, um die deutsche Gesellschaft zu destabilisieren. Die langfristige Verbreitung solcher Einflussversuche birgt das Risiko, den gesellschaftlichen Zusammenhalt, das grundlegende Vertrauen in Politik, Staat und demokratische Institutionen sowie in Qualitätsmedien auszuhöhlen (Frühwirth, 2023). FIMI soll Gesellschaften spalten und schwächen – und das möglichst unauffällig und schleichend. Es liegt daher im Kerninteresse demokratischer Staaten, ihre Bevölkerung bestmöglich vor solchen Manipulationsversuchen zu schützen.

Das vorliegende Research Paper zeigt, wie sich mittels systematischer Adressierung der Komplexität des Problems ein ganzheitliches Bewältigungsmodell entwickeln lässt, das Gesellschaften nachhaltig stärkt und schützt. Bewährte Konzepte und Praktiken finden Eingang in die Gestaltung und zeigen auf, was möglich ist.

Der ideelle Zielzustand als Kompass

Um der Komplexität und Wendigkeit des Problemphänomens gerecht zu werden, soll eine angemessene Bewältigungsstrategie systematisch hergeleitet werden. Dafür braucht es an erster Stelle den ideellen Zielzustand, auf dessen Erreichen Bewältigungsversuche ausgerichtet werden können:



Abbildung 1: Der Weg vom Ist- zum Sollzustand

FIMI wird dort zum Problem, wo die illegitimen Einflussversuche die Bevölkerung erfolgreich manipulieren, also Haltungen und letztlich Verhalten beeinflussen und verändern. So sei der anzustrebende Soll-Zustand an dieser Stelle wie folgt formuliert:

„Die Bevölkerung wird nicht durch FIMI beeinflusst.“

Es geht darum, die Manipulationswirkung so weit wie möglich einzudämmen, wobei realistischerweise eher von einer näherungsweisen Erfüllung als von einer vollständigen Erreichbarkeit dieses Zieles ausgegangen werden muss. Um sich diesem Soll-Zustand schrittweise anzunähern, müssen mehrere Aspekte geklärt werden. Zu Beginn steht die Frage nach der Problemdefinition. Was verstehen wir darunter, was gehört dazu und was nicht? Wie ist das Problem beschaffen und welche negativen Konsequenzen löst es aus, die wir verhindern wollen?

Daraus abgeleitet folgt die Definition des Lösungsverständnisses. Welche Bereiche werden zur Eindämmung des Problems als potenziell hilfreich bewertet? Wird FIMI beispielsweise in erster Linie als Informationsproblem verstanden, das dazu führt, dass Menschen falsche Dinge glauben, bietet sich der Lösungsraum Medienkompetenz und Informationsvermittlung an. Wird das Problem eher als Demokratiegefährdung betrachtet, ergeben sich Notwendigkeiten zur Stärkung angegriffener Werte.

Im nächsten Schritt kann aus dem Lösungsraum die Bandbreite verfügbarer Maßnahmen und zugehöriger Akteur:innen abgeleitet werden. Wo es um Medienkompetenz geht, könnten Aufklärungskampagnen oder Trainings von Bildungsträgern aufgeführt werden. Demokratiefördernde Maßnahmen könnten zum Vertrauensaufbau Transparenzinitiativen von Medienhäusern oder kommunale Partizipationsformate beinhalten.

Im letzten Schritt müssen die nun erarbeiteten Ansätze Eingang in ein Umsetzungsmodell finden, das aus der Theorie Praxis werden lässt. Welche Organisationsform eignet sich, um die benötigten Akteur:innen handlungsfähig zu machen? Welche Pläne, Rollen und Prozesse braucht es? Wie wird Qualität sichergestellt? Die Gestaltung des Umsetzungsmodells wird letztlich über die Wirksamkeit des Vorhabens entscheiden. Alles in allem bilden die Bereiche Problemverständnis, Lösungsraum, Maßnahmen und Bewältigungs-Akteur:innen sowie das Umsetzungsmodell die Antwort auf die Frage nach dem Weg vom Ist- zum Sollzustand.



Abbildung 2: Die Ausarbeitung konkreter Aspekte ebnet den Weg zum Sollzustand

Best Practices nutzen: Bestehende Konzepte zeigen, was möglich ist

Bereits bestehende Konzepte bieten wertvolle Impulse und Inspiration für die eigene Ausgestaltung. Im Folgenden sollen daher veranschaulichende Beispiele vorgestellt werden. Da die Bandbreite groß ist, wird kein Anspruch auf Vollständigkeit erhoben.

Problemverständnis

Die Definition des Problemverständnisses prägt maßgeblich die folgenden Lösungsbereiche und Maßnahmen. Ein zu eng gesteckter Problemrahmen birgt das Risiko, verfügbares Bewältigungspotenzial ungenutzt zu lassen. Desinformation, die Teil von FIMI-Aktivitäten sein kann, wird oft in erster Linie als Informationsproblem verstanden, dessen Risikopotential vor allem in der Vermittlung falscher Tatsachenbehauptungen fußt. CeMAS betrachtet Desinformation hingegen als komplexes Problem, das über den reinen Informationsaspekt hinausgeht. Das integrative Modell zum Umgang mit Desinformation macht neben der Informationsperspektive die Facetten Technologie, Sicherheit und Demokratie sichtbar, und betont die Notwendigkeit der sozialwissenschaftliche Perspektive als evidenzbasierte Handlungsgrundlage (Lamberty & Frühwirth, 2023). Nach dem integrativen Modell stellt Desinformation ein Problem dar, weil dadurch Menschen falsche Dinge glauben, die Sicherheit diskreditierter Gruppen beeinträchtigt wird und Demokratie zersetzende Impulse gestreut werden, die langfristig destabilisierend wirken können. Während jede einzelne Perspektive wichtig und relevant ist, würden Ansätze, die nur auf einer von ihnen basieren, zu kurz greifen. Die integrative Betrachtung ermöglicht, Desinformation in ihrer Komplexität in den Blick zu nehmen und eröffnet im nächsten Schritt einen breiteren Lösungsraum.

Lösungsverständnis

Auf die Definition des Problemverständnisses folgt die Ableitung geeigneter Lösungsbereiche. Die OECD zeichnet das Idealbild einer Bewältigungsstrategie, die handlungsfähig, adaptiv, inklusiv und vernetzt handelt, um aufkommende Probleme präventiv zu adressieren oder zeitnah zu reagieren. Sie empfiehlt unter anderem Institutionalisierung, Transparenz, Reaktionsgeschwindigkeit, Prävention, Evidenzbasierung und gesamtgesellschaftliche Kooperation als Kernansätze (OECD, 2023). In länderübergreifenden Studien der Bertelsmann-Stiftung zu Regierungsmaßnahmen zeigten sich Schwerpunkte in den Bereichen Entschärfung falscher Information, Plattformregulierung, Transparenzförderung, staatliche Kommunikation, Medienpluralismus und Aufbau öffentlicher Einrichtungen (Keller et al., 2024). Die folgenden Beispiele geben einen Einblick in bestehende Lösungsverständnisse:

- Auf EU-Ebene geht es um Früherkennung und Eindämmung, Informationsbereitstellung, Befähigung und Resilienzsteigerung der Bevölkerung, Regulierung digitaler Dienste und den Schutz der Medien (European Commission. Directorate General for Communication, 2024; European Commission, 2018; European External Action Service, 2025b; European Commission, 2025b).
- Das „Framework to Counter Foreign State Information Manipulation“, das im Januar 2024 von den Vereinigten Staaten, dem Vereinigten Königreich und Kanada bekräftigt wurde, sieht die Bereiche „Nationale Strategien und Policies“, „Regierungsstrukturen und Institutionen“, „Menschliche und technische Fähigkeiten“, „Zivilgesellschaft, unabhängige Medien und Wissenschaft“ und „Multilaterales Engagement“ vor (Government of Canada, 2024).
- Schweden setzt auf das Prinzip der psychologischen Verteidigung, das auf der Förderung gesellschaftlicher Resilienz, der Früherkennung von Bedrohungen, der Abschreckung zugehöriger Akteur:innen und strategischer Kommunikation basiert (Pamment, 2024).
- Die niederländische regierungsweite Strategie zur effektiven Bekämpfung von Desinformation zielt auf die Stärkung des Debattenraums und soll den Einfluss von Desinformation reduzieren (Government of the Netherlands, 2022).
- Die taiwanesische Organisation Doublethink Lab benennt für Taiwan die zentrale Rolle zivilgesellschaftlicher Akteur:innen, die mit staatlichen und weiteren Akteur:innen an einem Strang ziehen, gestärkt durch ein geteiltes Zielverständnis (Doublethink Lab, 2024).
- Die Bayern-Allianz gegen Desinformation setzt auf öffentliche Angebote und Kooperation mit Plattformen, Medien, Politiker:innen und Zivilgesellschaft (Bayerisches Staatsministerium für Digitales, o. J.).

Gegenmaßnahmen und Akteur:innen

Die Bandbreite möglicher Einzelmaßnahmen im Lösungsraum ist groß. Zur Veranschaulichung der Ansatzpunkte verschiedener Maßnahmen soll die Verbreitung von FIMI als Kommunikationsprozess dargestellt werden, bei dem irreführende Kommunikation von einem Akteur erstellt wird, um Individuen zu erreichen und so letztlich Gesellschaften zu beeinflussen (Lamberty & Frühwirth, 2023):



Abbildung 3: Exemplarische Darstellung der Verbreitung von FIMI-Inhalten

Für die verschiedenen Prozessschritte kommen dabei unterschiedliche Gegenmaßnahmen infrage, die aus dem Repertoire bestimmter Bewältigungs-Akteur:innen

stammen. Diese müssen eingebunden werden, um die volle Handlungsbandbreite verfügbar zu machen: Es braucht den viel besprochenen gesamtgesellschaftlichen Ansatz, den „Whole-of-Society-Approach“. Im Folgenden werden exemplarische Maßnahmen vorgestellt, die pro Prozessschritt eingesetzt werden können. Hierbei handelt es sich um Optionen, deren Passung und Angemessenheit zum eigenen Kontext vor der Integration in den eigenen Werkzeugkoffer kritisch zu prüfen ist.¹

Akteursbezogene Maßnahmen

FIMI-Aktivitäten werden geschaffen, weil sie einem FIMI-Akteur dienlich sind. Entsprechend hilfreich sind fundierte Kenntnisse zu dessen Zielen. Wo es gelingt, den Akteurswillen zu FIMI-Handlungen zu senken, ist mit einer Problemreduktion zu rechnen.

Akteursbezogene Maßnahmen			
Maßnahme	Ziel	Akteur:innen	Beispiele
FIMI-Akteurskenntnis herstellen	Vertiefte Kenntnis zur Ableitung geeigneter Maßnahmen	Wissenschaftliche Forschung, Zivilgesellschaft, Nachrichtendienste	Forschung zu Weltbild und Zielen, ² historischem Verhalten ³ oder aktuellen Vorgehensweisen ⁴
Deterrence (Abschreckung)	Demotivation des Akteurs	Staat, Staatenbündnisse	Signalisieren von Awareness, ⁵ Blockade von Infrastruktur ⁶ oder Verhängen von Sanktionen ⁷

Abbildung 4: Beispiele für akteursbezogene Maßnahmen

¹ Für einen tieferen Einblick in die Bandbreite möglicher Maßnahmen vgl. Ziemer, 2023; Vilmer, 2021; Rød, 2025; sowie Humprecht et al., 2020.

² Einblicke in historische sowie Weltbildkonzepte wie das der „Russkij mir“ (dt. russische Welt) bieten hilfreichen Kontext zur Interpretation der Handlungen des Kremls (Zabirko, 2023; Marushevska, 2025).

³ Die Kenntnis historischer Verhaltensweisen und Instrumente von FIMI-Akteur:innen – etwa der sowjetischen „aktiven Maßnahmen“ im Kalten Krieg – ermöglicht die bessere Antizipation und Einordnung von Handlungen (Rid, 2021).

⁴ Analysen zur Kommunikationslandschaft und Funktionsweise von Einflussversuchen geben Aufschluss über Vorgehensweisen und Schwachstellen von FIMI-Akteur:innen (European External Action Service, 2025a; Smirnova, 2024).

⁵ Das öffentliche Bekanntgeben von Erkenntnissen zu FIMI-Aktivitäten sowie deren Verurteilung und Ablehnung senden ein Signal der Wachsamkeit an zugehörige FIMI-Akteur:innen (Europäisches Parlament, 2025).

⁶ Laut Eigenaussage hat das US-Militär zum Schutz der Zwischenwahlen 2018 vorübergehend den Internetzugang der russischen „Trollfabrik“ Internet Research Agency (IRA) blockiert (Nakashima, 2019).

⁷ Aufgrund des russischen Angriffskriegs gegen die Ukraine verabschiedete die Europäische Union Sanktionen gegen Russland. Diese betreffen explizit auch Urheber:innen von Desinformation (European Union, 2025).

Verbreitungsbezogene Maßnahmen

Manipulative Inhalte müssen Menschen erreichen, um ihre Wirkung entfalten zu können. Entsprechend ist die Reduktion bzw. Unterbindung der Erstellung und Verbreitung von manipulativen Inhalten ein potenzieller Hebel zu ihrer Eindämmung.

Verbreitungsbezogene Maßnahmen

Maßnahme	Ziel	Akteur:innen	Beispiele
Entziehen von Assets und Tools	Inhalte können nicht mehr oder nur mit erhöhtem Aufwand erstellt werden	Staat, Plattformen, Journalismus	Kontensperrungen durch plattforminterne Untersuchungen ⁸ oder nach Investigativrecherchen, ⁹ Beschlagnahmung von Webseiten ¹⁰
Plattformregulierung	Soziale Netzwerke setzen Contentmoderation zu FIMI-Inhalten konsequent um	Staat, Staatenbündnisse, Plattformen	Staatliche Intervention bei Plattformen, ¹¹ Freiwillige Selbstverpflichtung, ¹² Digital Services Act ¹³
Kriminalisierung	Reduktion von Verbreitung über die Herstellung von Strafbarkeit	Staat	Verabschiedung strafrechtlicher Gesetze zur Verfolgung von FIMI-Aktivitäten ¹⁴

Abbildung 5: Beispiele für verbreitungsbezogene Maßnahmen

Maßnahmen zur Stärkung von Individuen

Manipulative Inhalte sollen möglichst viele einzelne Menschen beeinflussen, um so letztlich die öffentliche Meinung zu verschieben. Schutz und Gegenmaßnahmen auf der individuellen Ebene können vor, während und nach der Exposition ansetzen:

⁸ Laut OpenAI wurden Aktivitäten von FIMI-Akteur:innen identifiziert und die Zugänge gesperrt (OpenAI, 2024).

⁹ Qurium und CORRECTIV hatten im Rahmen von Investigativrecherchen Dienstleister kontaktiert, deren Dienste von FIMI-Akteur:innen genutzt worden waren. Diese sperrten daraufhin Zugänge (Bernhard et al., 2024b).

¹⁰ Das US-Justizministerium gab 2024 die Beschlagnahmung von FIMI-Webseiten bekannt (Bernhard et al., 2024a).

¹¹ Nach einem Gespräch des Bundesinnenministeriums mit Telegram 2023 konnten vermehrte Sperrungen verschwörungsideologischer und rechtsextremer Kanäle und Gruppen verzeichnet werden (Holnburger, 2023).

¹² Der Code of Practice on Disinformation der EU setzt auf freiwillige Selbstverpflichtung und Plattformkooperation. Ab Juli 2025 soll daraus ein Code of Conduct nach dem DSA werden (European Commission, 2025a).

¹³ Der europäische Digital Services Act (DSA) dient der Plattformregulierung digitaler Dienste, etwa durch Verpflichtungen im Bereich Content-Moderation oder Risiko-Bewertungen (Europäische Kommission, 2024).

¹⁴ Entsprechende Gesetze existieren z. B. in Singapur, Taiwan und auf den Philippinen (Keller et al., 2024).

Maßnahmen zur Stärkung von Individuen

Maßnahme	Ziel	Akteur:innen	Beispiele
Öffentliche Sensibilisierungskampagne	Risikobewusstsein schaffen und Grundkompetenzen vermitteln	Staat, Medien, Zivilgesellschaft	Schwedische Sensibilisierungskampagne „Don't Be Fooled“; ¹⁵ sowie die niederländische Informationsseite "Isdatechtzo" ¹⁶
Zielgruppenspezifische Befähigung	Vermittlung von Grundkompetenzen an alle Altersgruppen	Zivilgesellschaft, Staat	Ansprechen von Erwachsenen über Angebote am Arbeitsplatz; ¹⁷ an Volkshochschulen ¹⁸ und über Einbindung von Vereinen; ¹⁹ Ansprache Jugendlicher abseits der Schule über freiwillige Jugendfeuerwehren ²⁰
Prebunking	Präventive „Immunisierung“ gegen Narrative und Taktiken	Zivilgesellschaft, Forschung, Plattformen, Medien	Google Prebunking-Kampagne auf YouTube ²¹
Gamifizierte Ansätze	Spielerische „Immunisierung“	Zivilgesellschaft, Forschung	Online-Lernspiele zur niedrigschwelligen Sensibilisierung ²²
Faktenchecks	Nachträgliches Entkräften von bereits gesehenen Falschbehauptungen	Journalismus, Zivilgesellschaft	Frei zugängliche, digitale Faktencheck-Angebote ²³
Gegenkommunikation	Nachträgliche Stellungnahmen zu bereits verbreiteten Falschbehauptungen	Staat, Medien	Taiwanesisches 2-2-2-Prinzip ²⁴
Transparenzinitiativen	Vertiefung der Nachvollziehbarkeit der Entstehung von Content	Technologie-Unternehmen, Zivilgesellschaft, Journalismus	Kontextualisierung von Inhalten durch Zertifikate, die Entstehung und Verarbeitung von beispielsweise Fotos nachvollziehbar machen ²⁵

Abbildung 6: Beispiele für Maßnahmen zur Stärkung von Individuen

¹⁵ Die Sensibilisierungskampagne vermittelt in Form von Postern, Flyern und Online-Inhalten grundlegende Umgangsmöglichkeiten zu Desinformation (Psychological Defence Agency, o. D.).

¹⁶ Die Webseite informiert über Funktionsweise und Erscheinungsformen von Desinformation und vermittelt Handlungsempfehlungen zum Selbstschutz (Isdatechtzo.nl (o. D.).

¹⁷ Die Initiative „Business Council for Democracy“ (BC4D) bietet zu den Themen Desinformation, Verschwörungserzählungen und Hassrede sensibilisierende Workshopformate am Arbeitsplatz an (Shiferaw & Laubenstein, 2022).

¹⁸ Im Rahmen des Projekts „faktenstark“ der Amadeu Antonio Stiftung und codetekt werden Kompaktkurse zu Desinformation an Volkshochschulen angeboten (Deutscher Volkshochschulverband, 2025).

¹⁹ Im Rahmen der Bayern-Allianz gegen Desinformation werden unter anderem Vereine eingebunden, um möglichst viele Menschen zu Desinformation zu sensibilisieren (Bayerisches Staatsministerium für Digitales, o. D.).

²⁰ Im Rahmen einer Kooperation zwischen CORRECTIV und der Deutschen Jugendfeuerwehr werden Medienkompetenztrainings für Jugendliche über die Vereinsstrukturen angeboten (CORRECTIV, 2025).

²¹ Sensibilisierende Werbeanzeigen wurden auf YouTube, Facebook und Instagram ausgespielt (Google, o. D.).

²² Online-Spiele wie "Bad News", "Go Viral" und "Harmony Square" sollen durch Gamification Nutzer:innen dazu einladen, sich spielerisch mit Desinformation auseinanderzusetzen (Cambridge Social Decision-Making Lab, o. D.).

²³ Faktencheck-Redaktionen prüfen Behauptungen auf ihren Wahrheitsgehalt, damit Nutzer:innen gesehene Behauptungen einordnen können (CORRECTIV, o. D.; Tagesschau.de, o. D.; BR24, o. D.).

²⁴ Das 2-2-2-Prinzip beschreibt die optimale Gestaltung von AdHoc-Kommunikation zu Desinformation, um möglichst viele Menschen zu erreichen. Die Kommunikation sollte demnach binnen zwei Stunden erfolgen, 200 Wörter enthalten und um zwei Grafiken ergänzt sein (Doublethink Lab, 2024).

²⁵ Beispielsweise könnte ein Foto auf einer Webseite um Informationen zum Entstehungsort und zu den Bearbeitungsschritten ergänzt werden (Coalition for Content Provenance and Authenticity, o. J.).

Maßnahmen zur Stärkung der Gesellschaft

FIMI zielt auf die Destabilisierung von Gesellschaften ab, indem sie systematisch Misstrauen in demokratische Institutionen, gegenüber Politiker:innen und Parteien sowie gegenüber Qualitätsmedien schürt und den gesellschaftlichen Zusammenhalt angreift. Schutzmaßnahmen werden also auch auf gesellschaftlicher Ebene benötigt. Sie sollten jene Werte stärken und schützen, die von FIMI-Aktivitäten bedroht werden.

Maßnahmen zur Stärkung der Gesellschaft

Maßnahme	Ziel	Akteur:innen	Beispiele
Stärkung des Informationsraums	Schutz der Medien, Sicherstellen der Verfügbarkeit seriöser Quellen	Staat, Medien	Niederländisches PersVeilig Protokoll zum Schutz von Journalist:innen ²⁶
Stärkung des Zusammengehörigkeitsempfindens	Perspektivenwechsel von Unterschieden zu Gemeinsamkeiten zur Stärkung des gesellschaftlichen Zusammenhalts	Staat, Zivilgesellschaft, Medien	Neuseeländische Kommunikationskampagne „Unite against COVID-19“ ²⁷
Partizipations- und Transparenzinitiativen in der Politik	Vertrauensförderung gegenüber Staat und Demokratie	Staat, Zivilgesellschaft	Partizipationsprojekt „Forum gegen Fakes“ ²⁸
Schwachstellenanalyse	Kenntnis aktueller möglicher Ansatzpunkte von FIMI-Aktivität, beispielsweise polarisierende Themen, Unzufriedenheiten oder Spannungen	Staat, Forschung, Zivilgesellschaft	Bevölkerungsbefragung zu Zustimmung zu russischer Propaganda ²⁹

Abbildung 7: Beispiele für Maßnahmen zur Stärkung der Gesellschaft

Umsetzungsmodell

Ein gut gefüllter Methodenkoffer ist eine wichtige Ressource zur Eindämmung eines Problems. Entscheidend ist jedoch der effektive und effiziente Einsatz der vielen möglichen Maßnahmen und die koordinierte, kooperative Arbeitsweise der zugehörigen Akteur:innen. Die Grundlage jeglicher nachhaltiger Bewältigungsbemühungen bildet die politische Priorisierung. Erst wo die Problemlösung als ausreichend wichtig erachtet wird, können wirksame Strukturen zur Bewältigung geschaffen werden, die den Weg vom Ist- zum Soll-Zustand ebnen. Ein geeignetes Modell schafft Klarheit zum Handlungsspielraum, zu den Prozessen, Rollen und Handlungsoptionen. In einer länderübergreifenden Untersuchung der Bertelsmann-Stiftung Ende 2024 zeigte sich,

²⁶ Die PersVeilig Initiative soll Journalist:innen vor Übergriffen schützen. Vereinbarung wurde u. a. das konsequente Anzeigen von Übergriffen sowie die priorisierte Bearbeitung solcher Anzeigen (PersVeilig, 2019).

²⁷ Die Kampagne zum Umgang mit der Pandemie betonte die gemeinsame Identität und Bedrohungsbewältigung der Bevölkerung, um Spaltung entgegenzuwirken (NZ Royal Commission COVID-19 Lessons Learned, o. D.).

²⁸ Das Projekt „Forum gegen Fakes“ der Bertelsmann Stiftung setzt auf Bürgerbeteiligung zur partizipativen Erarbeitung von Lösungsvorschlägen zum Umgang mit Desinformation (Bertelsmann Stiftung, 2024).

²⁹ Um festzustellen, inwiefern russische Propagandanarrative in der deutschen Bevölkerung verfangen konnten, wurden in repräsentativen Befragungen die Zustimmungswerte zu Kernnarrativen erhoben (Lamberty, 2024).

dass Staaten mit umfassenden, strategischen Bewältigungsstrategien zu FIMI-Aktivitäten noch die Ausnahme bilden (Freihse & Bochert, 2024). Die folgenden Beispiele bieten Einblick in ausgewählte Umsetzungskonzepte:

Ganzheitliche Modelle

- Die niederländische regierungsweite Strategie zur Bekämpfung von Desinformation definiert das Problemverständnis sowie den Lösungsraum und leitet Maßnahmen, Verantwortliche und Deadlines zur Umsetzung ab. Das Dokument beschreibt die Beiträge verschiedener Ministerien, inkludiert die Rolle wissenschaftlicher Forschung und benennt Kooperationsformen (Government of the Netherlands, 2022).
- Der lettische Ansatz fußt auf nationalen Werten und definiert als Ziele die staatliche und gesellschaftliche Resilienz gegenüber Einmischung in demokratische Prozesse sowie die Sicherstellung von Handlungsfähigkeit im Krisenfall. Dazu stehen die thematischen Schwerpunkte strategischer Kommunikation und der Absicherung des Informationsraums im Fokus. Bewältigungs-Akteur:innen kommen aus den Bereichen Staat, Kommunen, Zivilgesellschaft, Forschung und dem Privatsektor. Die Koordination der Zusammenarbeit übernimmt die Staatskanzlei (Cabinet of Ministers, Republic of Latvia, 2023).

Umsetzung einzelner Aspekte

- Die Institutionalisierung von Eindämmungsbemühungen kann verschiedene Formen annehmen. Verbreitet sind Koordinationseinheiten und Task Forces, wie beispielsweise die Zentrale Stelle zur Erkennung ausländischer Informationsmanipulation (ZEAM) in Deutschland. Die auf Initiative mehrerer Ministerien geschaffene Projektgruppe widmet sich der Erkennung und Analyse von FIMI-Aktivitäten zur Vorbereitung angemessener Reaktionen der Bundesregierung (Bundesministerium des Innern, o.D.). In Schweden wurde die Psychological Defence Agency und in Frankreich die Agentur VIGINUM geschaffen, die neben Aufdeckung und Analyse auch die ministerienübergreifende Koordination zur Bewältigung von FIMI-Aktivitäten steuern (Ferriol, 2022; Psychological Defence Agency, 2024; OECD, 2024).
- Beispiele für die Gestaltung von Teilprozessen zur Analyse und Reaktion auf entdeckte Aktivitäten finden sich beim Europäischen Auswärtigen Dienst (European External Action Service, 2024), dem britischen Government Communication Service (GSC) (Pamment, 2021) und im Kooperationsprojekt CORE (European Commission Joint Research Centre, 2023). Die Gestaltung von Reaktionsprozessen und Strukturen kann außerdem von langjährigen Erfahrungen aus den Bereichen Blaulichtorganisationen, Katastrophenschutz und Cybersecurity profitieren (Deutsches Rotes Kreuz, o. D.; Bundesamt für

Bevölkerungsschutz und Katastrophenhilfe, o. D.; Bundesamt für Sicherheit in der Informationstechnik, o. D.).

- Die deutsche Bund-Länder-offene Arbeitsgruppe Hybrid (BLoAG Hybrid) hat Empfehlungen für Landesministerien und Kommunen herausgegeben, um Schutzmaßnahmen auf diesen Ebenen zu unterstützen (Bundesministerium des Innern, 2023).
- Ein Beispiel für die systematische Integration von wissenschaftlicher Grundlagenforschung bietet Schweden (Psychological Defence Research Institute, o. D.). Auch die niederländische Strategie erwähnt den wichtigen Beitrag wissenschaftlicher Forschung (Government of the Netherlands, 2022).
- Auch im Bereich Qualitätssicherung liegen Beispiele vor, etwa in Form von Methoden zur Klassifizierung von Beobachtungen (DISARM Foundation, o. D.; Pamment, 2020), der zielorientierten Response-Auswahl (Serrano & Sessa, 2024), der Beurteilung von Auswirkungen und Relevanz (Nimmo, 2020; Pamment, 2021), der Attribution zu verantwortlichen Akteur:innen (Palmertz et al., 2025) sowie der transparenten Einordnung der Belastbarkeit der Erkenntnisse (Professional Head of Intelligence Assessment (PHIA), 2019).
- Reflektionsfragen zur fundierten Gestaltung von Response-Modellen helfen bei der Entwicklung eigener Konzepte (Palmertz et al., 2024) und Assessments ermöglichen die Überprüfung der allgemeinen Response-Struktur auf Wirksamkeit und Entwicklungsbedarfe (Pamment, 2022; Rød et al., 2025).
- Kooperative Ansätze stärken die Response-Community durch den Austausch von Beobachtungen und Wissen sowie durch aktive Zusammenarbeit, wie Modellprojekte aus den Bereichen Faktencheck (European Commission, 2024; European Fact-Checking Standards Network, o. D.), Detection (Alliance4Europe, o. D.) und Alerting zeigen (FIMI-ISAC, o.D.; European External Action Service, 2019).
- Standards zur Datenstrukturierung erleichtern die schnelle Verarbeitung und Weitergabe sowie die Vergleichbarkeit von Vorfällen (DISARM Foundation, o. D.; OASIS Cyber Threat Intelligence Technical Committee, o.D.).

Das integrierte Modell zur Bewältigung ausländischer Einflussversuche

Im Folgenden soll auf Basis der beschriebenen Herleitung und unter Berücksichtigung der aufgeführten Konzepte und Beispiele ein integriertes Modell zur Bewältigung ausländischer Einflussversuche (FIMI) entwickelt werden. Neben der Annäherung an den inhaltlichen Soll-Zustand „Die deutsche Gesellschaft wird nicht durch FIMI beeinflusst“ sind weitere Anforderungen zu erfüllen. So soll das Problem ganzheitlich und langfristig adressiert werden, indem sowohl präventive als auch reaktive Maßnahmen integriert werden. Um mit der Adaptivität des Problems mithalten zu können, muss die Bewältigung ressourceneffizient und anpassungsfähig sein. Die Modellgestaltung muss mit bewährten Vorgehensweisen auf nationaler und internationaler Ebene kompatibel sein, um eine praktische Anwendbarkeit herzustellen.

Die gesamtgesellschaftliche Kooperation muss kritische Aufgaben-Akteur:innen-Passungen beachten, um nicht selbst zur Quelle neuer Risiken zu werden. Beispielsweise sollten Faktenchecks nicht von staatlichen Akteur:innen erstellt werden. Auch muss die Organisationsgestaltung notwendige „Checks and Balances“ enthalten, um etwa im Falle eines autoritären Regierungswechsels Handlungsfähigkeit zu sichern, ohne unangemessene Instrumentalisierung zu ermöglichen. Es gilt, die Balance zu wahren: Ein handlungsstarker, kooperativer Bewältigungsansatz benötigt die treibende Kraft eines Staates, der das Problem ernst nimmt und Lösungsräume eröffnet, wo einzelne Response-Akteur:innen an die eigenen Ressourcen- und Kompetenzgrenzen stoßen. Gleichzeitig muss das entstehende Konstrukt so gestaltet sein, dass es nicht selbst zur Gefahr für die Bevölkerung wird und demokratische Freiheiten nicht zweckentfremdet werden können (Institute for Strategic Dialogue, 2024). Um nachhaltige Handlungsfähigkeit zum Schutz der Bevölkerung zu gewährleisten, muss die organisatorische Aufhängung langfristig verankert werden und sollte nicht mit jeder neuen Legislaturperiode Unsicherheiten zu ihrem Fortbestehen ausgesetzt werden.

Unter Berücksichtigung der genannten Anforderungen kann nun das Modell entwickelt werden. Hierzu wird der eingangs definierte Soll-Zustand herangezogen und in Rückwärtsschritten auf die jeweils benötigten Voraussetzungen überprüft. Mittels dieses „Backcasting“ wird ein Entwicklungsplan herausgearbeitet, der die Lücke zwischen Ist- und Sollzustand schließt.

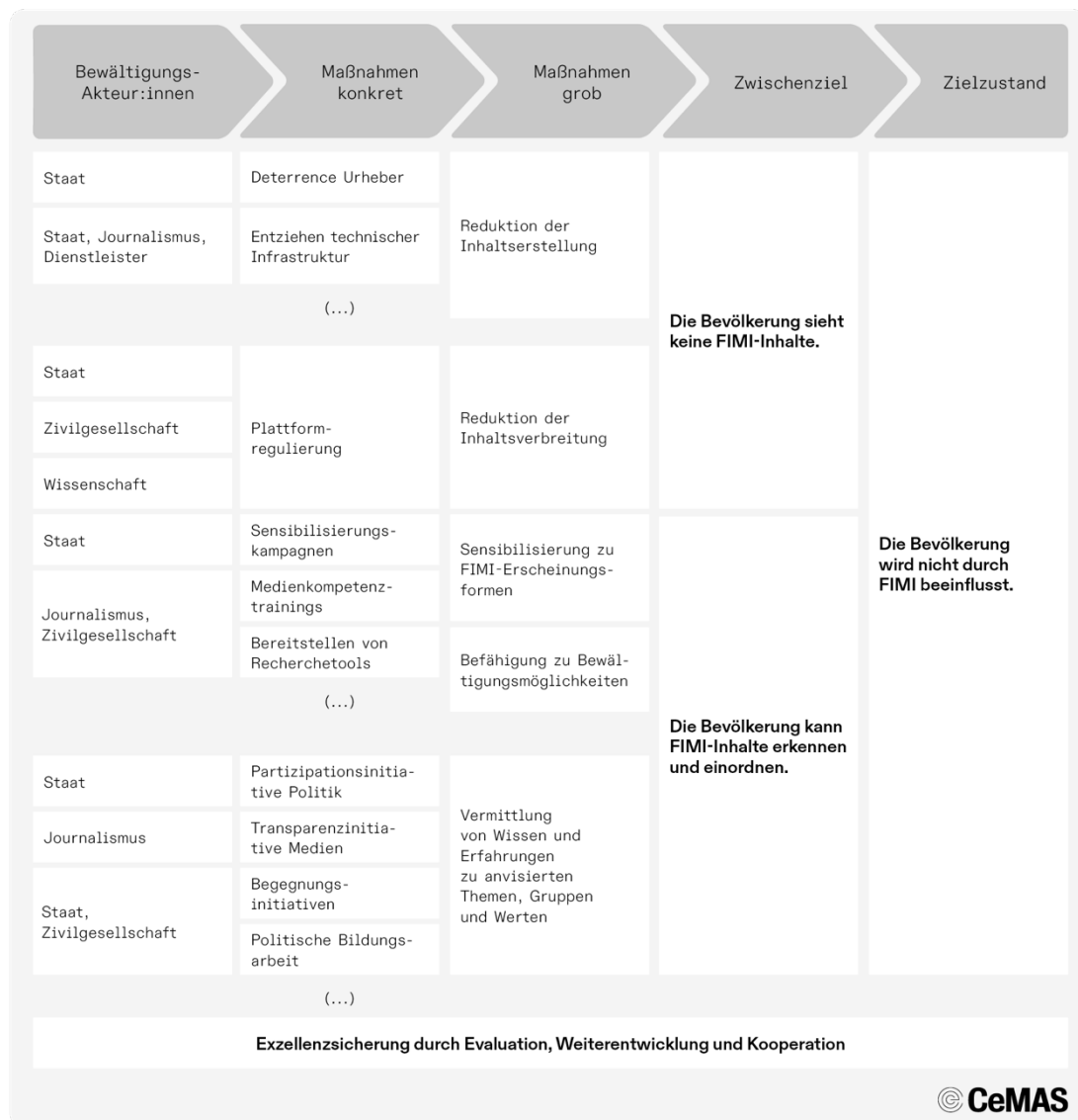


Abbildung 8: Vom Zielzustand (rechts) ausgehend lassen sich die jeweiligen Voraussetzungen ermitteln, um die Lücke zwischen Ist- und Sollzustand zu schließen

Vom Soll-Zustand ausgehend werden Zwischenziele identifiziert, die diesen fördern können. Um dafür zu sorgen, dass die Bevölkerung nicht durch FIMI beeinflusst wird, kann zum einen die Menge verfügbarer irreführender Inhalte reduziert werden. Denn: Was niemanden erreicht, kann niemanden beeinflussen.

Zum anderen kann die Befähigung der Bevölkerung dazu beitragen, dass Irreführendes erkannt und abgewehrt wird. So ergeben sich die Zwischenziele der Expositionsreduktion und der Steigerung der Manipulationsresilienz. Um diese Zwischenziele zu fördern, werden passende Maßnahmen ausgewählt. Beispielsweise könnten Maßnahmen zur Abschreckung und zur Plattformregulierung die Expositionsreduktion adressieren, während eine Kombination aus präventiver gesellschaftlicher Resilienzförderung, Medienkompetenz und Prebunking die Manipulationsresilienz der Bevölkerung stärkt. Diese exemplarische Auswahl von Maßnahmen macht schrittweise sichtbar, welche Akteur:innen in die Response-Bemühungen eingebunden werden müssen.

Insgesamt ermöglicht diese Form der Herleitung die zielorientierte Erstellung einer ganzheitlichen Bewältigungsstrategie, die sowohl die präventive als auch die reaktive Perspektive integriert und den Raum für eine kooperative FIMI-Bewältigung öffnet.

Die gewonnenen Erkenntnisse lassen sich nun in einer ganzheitlichen Handlungslandschaft darstellen, die in Domänen, Maßnahmen und Akteur:innen gegliedert ist und einen Schutzschild um die Bevölkerung bildet. Dieser ermöglicht sowohl die Reaktion auf neu aufkommende Aktivitäten als auch die konsequente präventive Arbeit an Langzeitfaktoren zugunsten des Bevölkerungsschutzes. Die ausführenden Domänen Prävention und Reaktion werden dabei von der Domäne Exzellenz gestärkt, die für Qualitätssicherung und kontinuierliche Weiterentwicklung sorgt.

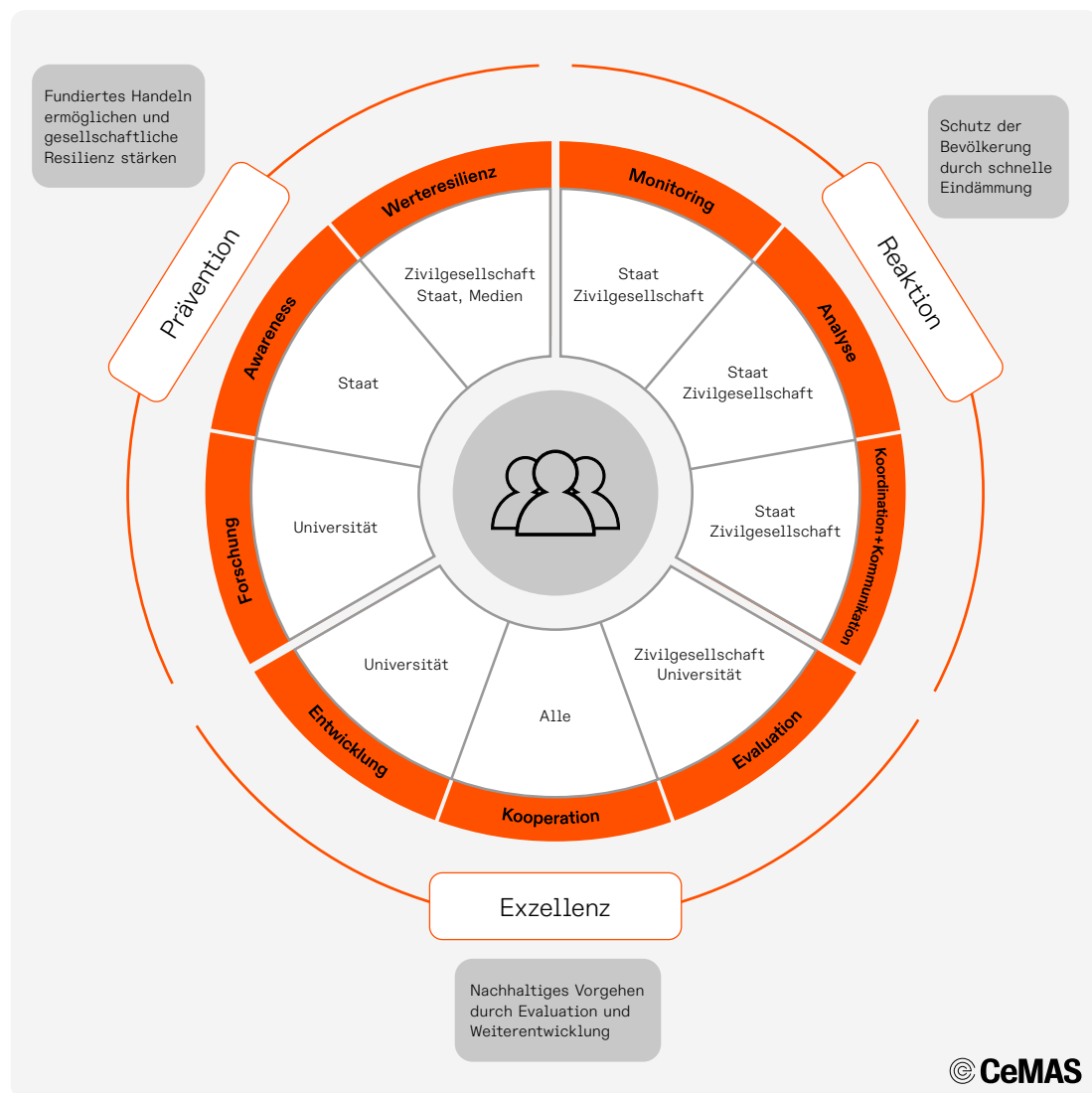


Abbildung 9: Die Handlungslandschaft des integrierten Response-Modells bildet einen Schutzschild um die Gesellschaft

Prävention

Die Präventionsdomäne widmet sich der langfristigen Stärkung von Individuen und Gesellschaft. Hierzu gehören sowohl grundlegende Forschungsarbeiten zu Problem, Lösung, Zielgruppe und Informationsraum als auch die Umsetzung von Förderungsmaßnahmen zur individuellen und gesellschaftlichen Manipulationsresilienz. Typische Akteur:innen dieser Domäne stammen aus den Bereichen wissenschaftlicher Forschung, Medien, Kommunikation und Zivilgesellschaft. Der Präventionsbereich schafft die evidenzbasierte Grundlage der Response und stärkt nachhaltig den Schutz von Individuen und Gesellschaft vor Manipulationsversuchen.

Reaktion

Der Reaktionsbereich kümmert sich um das Eindämmen von FIMI-Kampagnen. Dazu gehört ein kontinuierliches Monitoring zur Früherkennung, das sowohl bekannte Muster auf neue Aktivitäten überprüft (top-down), als auch die explorative Untersuchung potenzieller neuer Formen (bottom-up) abdeckt. Wo Aktivitäten festgestellt werden, werden diese durch Analyst:innen systematisch ausgewertet. Bei Bedarf wird von hier aus ein Eskalationsprozess gestartet, um notwendige Reaktionsmaßnahmen anzustoßen. Entsprechend müssen Kompetenzen und Befugnisse zur Koordination und Kommunikation vorhanden sein, um die Kooperation der benötigten Akteur:innen in der folgenden Bewältigung möglichst wirksam und effizient zu gestalten. Typische Akteur:innen dieser Domäne sind Staat und Zivilgesellschaft. Der Reaktionsbereich ermöglicht die fundierte und zeitnahe Antwort auf Bedrohungslagen.

Exzellenz

Die Exzellenzdomäne widmet sich der Qualitätssicherung sowie der kontinuierlichen Verbesserung des Vorgehens, etwa durch die systematische Evaluation aller durchgeführten Maßnahmen. Zur nachhaltigen Stärkung und Weiterentwicklung des Bewältigungssystems werden Entwicklungsmöglichkeiten ausgelotet, Kooperation und Wissensaustausch gefördert und die Entwicklung neuer Tools und Methoden vorangetrieben. Typische Akteur:innen dieses Bereichs stammen aus der Wissenschaft und der Zivilgesellschaft. Die Exzellenzdomäne sorgt für eine hohe Qualität der Arbeitsergebnisse und das Schritthalten mit der Entwicklungsgeschwindigkeit des Problemphänomens.

Die Handlungslandschaft stellt insgesamt jene Bereiche dar, die konstant am Schutz und an der Stärkung der gesellschaftlichen Bedrohungsbewältigung arbeiten. Neben den hier genannten Akteur:innen werden weitere bedarfsorientiert aktiv, beispielsweise während der Reaktion auf aufgedeckte Aktivitäten. Die Art und Weise der Arbeit entscheidet letztlich über Wirksamkeit und Effizienz: Es braucht ausreichende Ressourcen auf personeller wie finanzieller Ebene, schlanke Prozesse, klare Rollen,

produktive Schnittstellen und ein lernendes System mit gesunder Fehlerkultur und Veränderungsbereitschaft, um dem herausfordernden Problemfeld gerecht zu werden. Die Organisation sollte von einer veränderungsaffinen Arbeitskultur mit Mut zur Fehlerkultur geprägt sein, da die Bewältigung des dynamischen Problems nicht umhinkommen wird, Vorgehensweisen zu erproben, zu verwerfen und anzupassen. Statt Silo-Denken sollte das Handeln aller Beteiligten von einem klaren Fokus auf das gemeinsame, übergeordnete Ziel geprägt sein, der im Umgang mit dynamischen Entwicklungen Handlungssicherheit durch Orientierung und Priorisierung schafft.

Der ideale Ablauf im Akutfall

Während die Handlungslandschaft eine wichtige Übersicht zu den Domänen, Maßnahmen und Akteur:innen für ein handlungsleitendes Strategiekonzept darstellt, braucht es für den Schritt von der Theorie zur Praxis klar definierte Abläufe und Prozesse. Zwar werden sich verschiedene FIMI-Fälle selten vollständig gleichen, jedoch können grundlegende notwendige Prozessschritte für den Akutfall festgehalten werden:



Abbildung 10: Grundlegende Prozessschritte im Akutfall

Präventive Maßnahmen wirken bereits vor Auftreten eines neuen Akutfalles. Sie sind langfristig angelegt und bauen schrittweise schützende Faktoren auf, die im Akutfall stärkend wirken sollen. Der Aufbau eines **Echtzeit-Monitorings** ist eine zentrale Notwendigkeit für die Identifikation neuer FIMI-Aktivitäten. Wo sie auftreten, werden sie zeitnah und standardisiert dokumentiert, analysiert und bei ausreichender Relevanz als **Alert** an die Leitung des Krisenstabs eskaliert. Stimmt diese der Relevanzeinschätzung zu, beruft sie kurzfristig und hoch priorisiert den **Krisenstab** ein und bestimmt fallbezogen die benötigte Besetzung aus Bewältigungs-Akteur:innen. Im Krisenstab wird der Fall unter diesen besprochen und es werden passende **reaktive Maßnahmen** beschlossen. Es folgt deren zeitnahe Umsetzung, die erneute Überprüfung und bei zufriedenstellenden Ergebnissen der Abschluss des Falles. Im letzten Schritt werden Fall und Gegenmaßnahmen **evaluiert**, um Anpassungsnotwendigkeiten und Entwicklungspotenziale für zukünftige Fälle zu identifizieren und zur Umsetzung zu bringen. Im Folgenden soll die ideale Umsetzung anhand realistischer Szenarien verdeutlicht werden:

Szenario 1: Schnelle Eindämmung einer koordinierten Desinformationskampagne

Ausgangslage ist die Verbreitung einer Desinformationskampagne in sozialen Medien nach bekanntem Muster. Ab 8:00 Uhr morgens posten inauthentische koordinierte Accounts hundertfach scheinbare Meinungsäußerungen deutscher Bürger:innen. Sie verbreiten Aussagen gegen die Unterstützung der Ukraine, diskreditieren die deutsche Regierung und schüren Ängste vor wirtschaftlichem Abstieg. Die Beiträge enthalten Links zu gefälschten pro-russischen Nachrichtenartikeln, die die Optik deutscher Leitmedien imitieren. Die Originalbeiträge werden von weiteren Kampagnenaccounts vielfach weiter geteilt.

Unter Anwendung des integrierten Responsemodells sollte die Reaktion wie folgt aussehen:

Präventive Maßnahmen:

Umfassende Aufklärungskampagnen und Medienkompetenztrainings haben die breite Bevölkerung erreicht und für die Beschaffenheit von FIMI-Kampagnen sensibilisiert. Transparenzinitiativen der Presse sorgen dafür, dass Nutzer:innen bei seriösen Medien vertiefte Einblicke zur Entstehung von Inhalten finden, anhand derer sie besser zwischen authentischen und irreführenden Inhalten unterscheiden können. Auf operativer Ebene wurde frühzeitig festgelegt, dass im Akutfall eine Einberufung zum Krisenstab für angeforderte Bewältigungs-Akteur:innen höchste Priorität genießt. Ebenso wurden Befugnisse zu Kooperation und zum Informationsaustausch hergestellt.

Monitoring:

Aufgrund des bereits bekannten Kampagnenmusters wird die Aktivität im Monitoring umgehend registriert, dokumentiert und an den Analysebereich übergeben. Die weitere Entwicklung wird beobachtet.

Analyse:

Analyst:innen ordnen die Aktivität einem FIMI-Akteur zu, bewerten das Risikopotenzial, leiten Handlungsempfehlungen ab und teilen ihre Erkenntnisse in Form eines Alerts um 9:00 Uhr mit der Leitung des Krisenstabs.

Krisenstab:

Die Krisenstableitung prüft die Empfehlungen, stimmt der Relevanz des Falles zu und setzt für 12:00 Uhr ein Krisenstabstreffen an. Als notwendige Teilnehmende werden die zuständigen Analyst:innen, Vertreter:innen der betroffenen Plattform, des Außenministeriums, des Innenministeriums, des BSI, des Bundespresseamts, des Digital Services Coordinators sowie Faktencheck-Organisationen bestimmt. Im Stabstreffen wird die Sachlage vorgestellt, während die umgehende Entfernung der Inhalte und Konten als Maßnahmeziel vorgeschlagen wird, um unmittelbare Verbreitungsrisiken zu unterbinden. Nach intensivem Austausch der Bewältigungs-Akteur:innen wird dieser Vorschlag angenommen.

Reaktive Maßnahmen:

Der Krisenstab beschließt, dass die betroffene Plattform die Beiträge und Accounts nach interner Prüfung auf Basis der klaren Akteurs-Attribution, ihrer manipulativen Eigenschaft und des damit verbundenen Verstoßes gegen die Plattformrichtlinien entfernen soll. Das BSI überprüft die Beschaffenheit der Kampagnenwebseiten auf mögliche Ansatzpunkte für Gegenmaßnahmen. Die Faktencheck-Organisation erstellt Faktenchecks zu den vermittelten Kernnarrativen, sodass bereits erreichte Nutzer:innen Orientierung finden können. Eine aktive Gegenkommunikation wird vorerst nicht veranlasst, um die Kampagne nicht durch mehr Aufmerksamkeit zu verstärken. Der Alert wird in Netzwerken zur FIMI-Bewältigung geteilt, um Forschende, Faktenchecker:innen und andere staatliche Akteur:innen über die laufende Aktivität zu informieren. Für die Dauer des offenen Falles wird eine sichere digitale Kommunikationsform zum informellen Austausch der beteiligten Akteur:innen geöffnet. Nach Abschluss des Krisenstabmeetings um 13:00 Uhr setzen die Akteur:innen ihre Maßnahmen um und geben Updates. Um 16:00 Uhr kommt der Krisenstab erneut zusammen, um umgesetzte Maßnahmen zu besprechen und das Ergebnis zu sondieren. Die Plattform hat die Moderationshandlungen nach interner Prüfung umgesetzt, das BSI die Dienstleister der genutzten Webseiteninfrastruktur über die missbräuchliche Nutzung informiert. Der Fall wird seitens des Monitoringbereichs für eine weitere Woche bevorzugt beobachtet und bei beständiger Unauffälligkeit abgeschlossen, dokumentiert und zur Evaluation an den Exzellenzbereich übergeben.

Evaluation:

Im Rahmen der Evaluation werden Vorfall, Maßnahmen, Ergebnis und Wirksamkeit sowie Effizienz des Vorgehens analysiert und bewertet. Es entstehen Erkenntnisse dazu, inwiefern bestehende Vorgehensweisen beibehalten, angepasst oder weiterentwickelt werden sollen. Konkrete Handlungsempfehlungen werden zur Weiterentwicklung des Response-Systems genutzt.

Szenario 2: Eindämmung von Desinformation während einer Naturkatastrophe

In einer infrastrukturtechnisch schlecht zugänglichen Region führt Hochwasser zu Erdbeben und Überflutungen, es kommt zu Stromausfällen und Kommunikationsproblemen. Russische Staatsmedien und pro-russische Influencer:innen verbreiten online Falschbehauptungen zur kommunalen, Landes- und Bundespolitik: Es wird behauptet, die Behörden seien unvorbereitet, unfähig oder nicht willens, der Bevölkerung zu helfen oder würden Gelder lieber in die Unterstützung der Ukraine investieren. Es tauchen verschwörungsideologische Behauptungen auf, nach denen das Hochwasser auf den angeblichen Einsatz von Wetterwaffen zurückzuführen sei. Die Inhalte finden vor allem über Messenger-Dienste Verbreitung.

Das integrierte Responsemodell ermöglicht folgende Bewältigung:

Präventive Maßnahmen:

Im Vorfeld wurden Projekte zur gesellschaftlichen Resilienzstärkung durchgeführt, in denen Bürger:innen partizipativ in die Gestaltung von Gegebenheiten in ihren Kommunen eingebunden wurden, die Komplexität politischer Vorgänge erleben und ihre politischen Vertreter:innen kennen lernen konnten.

Transparenzprojekte im Medienbereich haben Lücken in der kommunalen medialen Abdeckung geschlossen und Einblicke in die Arbeit von Qualitätsmedien ermöglicht. Kooperative Projekte haben gesellschaftliche Gruppen zusammengebracht, um Verbesserungen im eigenen öffentlichen Umfeld anzustoßen, Selbstwirksamkeit zu fördern und Vorurteile abzubauen. Die für die Bewältigung von Naturkatastrophen zuständigen Behörden haben verstärkt in Kommunikation investiert, um für einen grundlegenden Wissensstand zu Risiken, Vorsorgemaßnahmen, Selbstschutz sowie zentralen Schritten im Akutfall zu sorgen, und um über erwartbare irreführende Falschbehauptungen aufzuklären. Kommunal wurden Bürger:innen proaktiv über lokale Gegebenheiten und krisenfeste Anlaufstellen für gesicherte Informationen informiert. Die Bevölkerung ist über die politischen Bemühungen der Katastrophenvorsorge und -bewältigung informiert, kennt die Risiken von Desinformation und weiß, wo gesicherte Informationen zu finden sind. Sicherheitsgefühl, Selbstwirksamkeitserwartung und Vertrauen in die zuständigen Behörden wurden gestärkt.

Monitoring und Analyse:

Bei Eintritt des Akutfalls wird eine Verbreitung der beschriebenen Desinformationsnarrative über Messenger-Dienste erst später auffallen, da bilaterale Messenger-Kommunikation im Gegensatz zu öffentlichen sozialen Netzwerken nicht gemonitort wird. Ab Kenntnis der Verbreitung der Narrative, etwa durch ein Sichtbarwerden im öffentlichen digitalen Diskurs, werden diese in den Bereichen Monitoring und Analyse behandelt wie in Szenario 1.

Krisenstab:

Analyst:innen und Krisenstabsleitung vergeben eine hohe Eskalationsstufe, da die Falschbehauptungen in der bestehenden Krisenlage geeignet sind, Menschen

zusätzlich zu gefährden. Die Besetzung des Krisenstabs umfasst die zuständigen Analyst:innen sowie Vertretungen der betroffenen Plattformen, des Außen- und Innenministeriums, Bundespresseamts, BKK, lokaler Blaulichtorganisationen sowie des Digital Service Coordinators.

Reaktive Maßnahmen:

Da von einer bereits erfolgten Verbreitung der FIMI-Inhalte in der Bevölkerung ausgegangen werden muss, ist Kommunikation gefragt. Diese muss korrekte Informationen vermitteln, Bürger:innen an bestehende Pläne und Abläufe erinnern und Handlungsorientierung bieten. Außerdem wird vor Falschbehauptungen und Gerüchten gewarnt und Umgangsmöglichkeiten empfohlen, ohne konkrete Behauptungen selbst zu wiederholen und damit zu verstärken. Unter Berücksichtigung möglicher technischer Ausfälle wird dafür gesorgt, dass alle betroffenen Bürger:innen Zugriff auf gesicherte Informationen haben und wissen, wo diese zu finden sind – etwa über einen Radiosender, eine Webseite oder über eigens eingerichtete Messengergruppen. Zur Unterstützung werden bestehende lokale Netzwerke wie Vereine und Freiwilligenorganisationen als Multiplikatoren eingebunden. Abseits der direkt betroffenen Zielgruppe setzt das Bundespresseamt proaktive Kommunikationsformate auf, um einer Instrumentalisierung der Hochwasserlage gegenüber der nicht direkt betroffenen Öffentlichkeit entgegenzuwirken.

Evaluation:

Der Ablauf der Evaluation gestaltet sich grundsätzlich wie in Szenario 1. Aufgrund des erweiterten Kreises der Bewältigungs-Akteur:innen empfiehlt sich ergänzend die Überprüfung der Schnittstellenfunktionalität, beispielsweise zum THW oder zu lokalen Blaulichtorganisationen. Beide Bewältigungssysteme könnten in zukünftigen Krisenfällen von einer gut verschränkten Vorgehensweise zu FIMI-Vorfällen profitieren.

Die exemplarischen Szenarien verdeutlichen, wie die theoretische Handlungslandschaft des integrierten Modells in Aktion tritt, um die Bevölkerung über Expositionsreduktion und die Förderung von Manipulationsresilienz vor illegitimen Einflussversuchen zu schützen. Bereits die beiden Beispiele machen sichtbar, dass je nach Fall unterschiedliche Ansätze besonders wirksam sind, und sich entsprechend gegenseitig ergänzen sollten.

Fazit

In diesem Research Paper wurde die systematische Herleitung eines integrierten Modells zur Bewältigung ausländischer Einflussversuche vorgestellt. Es stellt bestehende Beispiele zur Definition von Problemvorstellung, Lösungsverständnis, Zielvorstellungen, Maßnahmen, Akteur:innen sowie Ansätze für die Prozessgestaltung vor und zeigt auf, welche Ressourcen verfügbar werden, wenn das Problem in seiner Komplexität angenommen und systematisch adressiert wird. Wo einzelne Ansätze nur Teilaspekte bearbeiten können, eröffnet ihre Integration in ein ganzheitliches Konzept das volle Bewältigungsspektrum. So wird die passgenaue Reaktion auf individuelle FIMI-Fälle ermöglicht. Insbesondere die Integration der langfristigen Präventionsperspektive sorgt für die nachhaltige Stärkung jener gesellschaftlichen Werte, die von FIMI-Aktivitäten angegriffen werden. Durch den systematisch kooperativen Ansatz und das explizite Augenmerk auf effiziente Handlungsstrukturen werden sowohl Ergebnisqualität als auch Reaktions- und Entwicklungsgeschwindigkeit gesteigert.

Ein wirksamer Schutz vor FIMI muss Komplexität annehmen und für sich nutzen. Dabei soll das skizzierte Modell keine starre Blaupause darstellen, sondern vielmehr Anstoß sein und gangbare Wege sowie bestehende Ressourcen aufzeigen, um die Entwicklung zu einem entsprechenden Vorgehen zu unterstützen. Auch sind längst nicht alle Fragen beantwortet, da insbesondere die konkrete Ausgestaltung interdisziplinär und gründlich erfolgen muss. Ihre finale Festschreibung sollte weder von einem einzelnen Response-Akteur stammen, noch würde ihr der begrenzte Rahmen eines Research Papers gerecht werden. Die Frage nach der konkreten Verankerung der beschriebenen Felder, Akteur:innen und Prozesse in einer Organisationsform ist keinesfalls trivial, da eine angemessene Antwort vielfältige Anforderungen erfüllen muss. Insbesondere die Prüfung auf Missbrauchspotenzial muss sorgfältig und interdisziplinär erfolgen. Trotz aller Herausforderungen bleibt die Erarbeitung eines integrierten Response-Modells dringend nötig, da FIMI-Akteur:innen Schwächen im Bewältigungssystem kontinuierlich nutzen, um die anvisierte Gesellschaft zu destabilisieren.

Die Herangehensweise sollte der Komplexität des Problems und den eigenen Werten gerecht werden, indem sie kooperativ erfolgt. Es braucht u. a. Expertise und Perspektiven aus staatlichen Organisationen, der Zivilgesellschaft, universitärer Forschung und den Medien, um ein schlagkräftiges Vorgehen zu entwickeln und Gestaltungsmacht verantwortungsvoll zu verteilen. Als treibende Kraft muss jedoch der Staat auftreten, da der Schutz der Bevölkerung vor FIMI-Einflüssen in seine Kernaufgaben fällt. Der Staat öffnet den Raum, in dem die vielfältigen Bewältigungs-Akteur:innen mit ihm zusammentreffen und Lösungen erarbeiten. Den Grundstein für die Umsetzbarkeit aller weiteren Schritte bildet die politische Priorisierung der Problemlösung. Das vorliegende Paper soll Grundlage und Anstoß für weiterführende Arbeiten zur integrierten Bewältigung ausländischer Einflussversuche sein.

Literaturverzeichnis

Alliance4Europe (o. D.). A4E Counter Disinformation Network (CDN). <https://alliance4europe.eu/cdn>

Bayerisches Staatsministerium für Digitales (o. D.). Bayern-Allianz gegen Desinformation. <https://www.stmd.bayern.de/themen/bayern-allianz-desinformation>

Bernhard, M., Hock, A. & Thust, S. (2024a, 3. September). Doppelgänger: USA beschlagnahmen Propaganda-Webseiten, die Deutschland im Visier hatten. <https://correctiv.org/faktencheck/russische-desinformation/2024/09/05/doppelgaenger-usa-beschlagnahmen-propaganda-webseiten-die-deutschland-im-visier-hatten>

Bernhard, M., Hock, A. & Thust, S. (2024b, 18. Juli). Nach CORRECTIV-Recherche: Russische Propaganda-Kampagne gerät ins Stocken. <https://correctiv.org/aktuelles/russland-ukraine-2/2024/07/18/nach-correctiv-recherche-russische-propaganda-kampagne-geraet-ins-stocken>

Bertelsmann Stiftung (2024). Forum gegen Fakes: Bürgergutachten zum Umgang mit Desinformation. <https://doi.org/10.11586/2024149>

BR24 (o. D.). #Faktenfuchs. <https://www.br.de/nachrichten/faktenfuchs-fakten-check,QzSlzI3>

Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (o. D.). Krisenmanagement. https://www.bbk.bund.de/DE/Themen/Krisenmanagement/krisenmanagement_node.html

Bundesamt für Sicherheit in der Informationstechnik (o. D.). Ich habe einen Vorfall – Checkliste Organisatorisches. <https://www.bsi.bund.de/dok/13282672>

Bundesministerium des Innern (2023). Sensibilisierung im Umgang mit hybriden Bedrohungen einschließlich Desinformation (BLoAG). <https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/heimat-integration/wehrhafte-demokratie/BMI24013.html>

Bundesministerium des Innern (o. D.). Zentrale Stelle zur Erkennung ausländischer Informationsmanipulation (ZEAM). <https://www.bmi.bund.de/SharedDocs/schwerpunkte/DE/desinformation-bei-bt-wahl/zeam-artikel.html>

Cambridge Social Decision-Making Lab (o. D.). Prebunking conspiratorial, electoral, and medical disinformation through online games. <https://inoculation.science/inoculation-games>

Coalition for Content Provenance and Authenticity (o. D.). An open technical standard providing publishers, creators, and consumers the ability to trace the origin of different types of media. <https://c2pa.org/>

CORRECTIV (2025). CORRECTIV und Deutsche Jugendfeuerwehr starten Kooperation. <https://correctiv.org/in-eigener-sache/2025/02/05/brandherd-desinformation-correctiv-und-deutsche-jugendfeuerwehr-starten-kooperation/>

CORRECTIV (o. D.). CORRECTIV.Faktencheck. <https://correctiv.org/faktencheck/>

Deutsche Bundesregierung. (2025). Was ist FIMI? <https://www.bundesregierung.de/breg-de/aktuelles/fimi-fake-news-international-2227610>

Deutscher Volkshochschulverband (2025). Kompaktkurse zum Thema Desinformation für Volkshochschulen in Kooperation mit faktenstark. <https://www.volkshochschule.de/meldungen/politische-jugendbildung-kooperation-mit-faktenstark.php>

Deutsches Rotes Kreuz (o. D.). Hilfeleistungssystem und Krisenmanagement im DRK. <https://www.drk.de/das-drk/auftrag-ziele-aufgaben-und-selbstverstaendnis-des-drk/hilfeleistungssystem-und-krisenmanagement/>

DISARM Foundation (o. D.) DISARM helps identify and respond to malign information influence operations. <https://www.disarm.foundation/>

Doublethink Lab (2024, 9. August). Taiwan POWER: A Model for Foreign Information Manipulation & Interference Resilience. <https://medium.com/doublethinklab/taiwan-power-a-model-for-resilience-to-foreign-information-manipulation-interference-70ea81f859b7>

Europäische Kommission (2024). Eine sicherere & fairere Online-Umgebung. <https://digital-strategy.ec.europa.eu/de/factpages/safer-fairer-online-environment>

Europäisches Parlament (2025, 23. Januar). Abgeordnete verurteilen Russlands Einsatz von Desinformation zur Rechtfertigung des Ukraine-Kriegs. <https://www.europarl.europa.eu/news/de/press-room/20250116IPR26330/abgeordnete-verurteilen-russlands-einsatz-von-desinformation-zum-ukraine-krieg>

European Commission (2018). Action plan against Disinformation. https://commission.europa.eu/document/download/b654235c-f5f1-452d-8a8c-367603af841_en?filename=eu-communication-disinformation-euco-05122018_en.pdf

European Commission (2024). European Digital Media Observatory (EDMO). <https://digital-strategy.ec.europa.eu/en/policies/european-digital-media-observatory>

European Commission (2025a). The 2022 Code of Practice on Disinformation. <https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation>

European Commission (2025b). The Code of Conduct on Disinformation. <https://digital-strategy.ec.europa.eu/en/library/code-conduct-disinformation>

European Commission Directorate General for Communication (2024). Tackling disinformation and information manipulation. Publications Office. <https://data.europa.eu/doi/10.2775/87640>

European Commission Joint Research Centre (2023). Hybrid threats: A Comprehensive Resilience Ecosystem. Publications Office. <https://data.europa.eu/doi/10.2760/37899>

European External Action Service (2019, März). Factsheet: Rapid Alert System. <https://www.eeas.europa.eu/node/59644>

European External Action Service (2024, 23. Januar). 2nd EEAS Report on Foreign Information Manipulation and Interference Threats. <https://www.eeas.europa.eu/eeas/2nd-eeas-report-foreign-information-manipulation-and-interference-threats>

European External Action Service (2025a, 19. März). 3rd EEAS Report on Foreign Information Manipulation and Interference Threats. <https://www.eeas.europa.eu/eeas/3rd-eeas-report-foreign-information-manipulation-and-interference-threats-0>

European External Action Service. (2025b). Information Integrity and Countering Foreign Information Manipulation & Interference (FIMI). https://www.eeas.europa.eu/eeas/information-integrity-and-countering-foreign-information-manipulation-interference-fimi_en

European Fact-Checking Standards Network (o. D.). <https://efcsn.com>

European Union (2025, April). EU sanctions against Russia following the invasion of Ukraine. https://ec.europa.eu/commission/presscorner/api/files/attachment/881067/Factsheet_EU_Sanctions_against_Russia_EN.pdf

Ferriol, G. (2022, 2. November). VIGINUM Year #1. <https://www.sgdsn.gouv.fr/publications/viginum-annee1>

FIMI-ISAC (o. D.). Foreign Information Manipulation and Interference – Information Sharing and Analysis Centre. <https://fimi-isac.org/index.html>

Freihse, C., & Bochert, F. (2024). Up to the challenge? Strategies to counter disinformation in the EU, UK and US. <https://doi.org/10.11586/2024161>

Frühwirth, L. (2023, 10. August). Koordinierter Vertrauensverlust. cemas.io. <https://cemas.io/blog/desinformation-demokratiegefaehrung/>

Google (o. D.). Prebunking ist eine Technik, um Manipulationen im Internet vorzubeugen. <https://prebunking.withgoogle.com>

Government of Canada (2024, 18. Januar). The Framework to Counter Foreign State Information Manipulation. GAC. <https://www.international.gc.ca/transparency-transparence/rapid-response-mechanism-mecanisme-reponse-rapide/manipulation.aspx>

Cabinet of Ministers, Republic of Latvia (2023, 20. März). The National Concept on Strategic Communication and Security of the Information Space 2023-2027.

<https://www.mk.gov.lv/en/valsts-strategiskas-komunikacijas-un-informativas-telpas-drosibas-koncepcija>

Government of the Netherlands (2022). Government-wide strategy for effectively tackling disinformation. <https://www.government.nl/documents/parliamentary-documents/2022/12/23/government-wide-strategy-for-effectively-tackling-disinformation>

Holnburger, J. (2023, 29. März). Chronologie einer Radikalisierung. Wie Telegram zur wichtigsten Plattform für Verschwörungsideologien und Rechtsextremismus wurde. <https://cemas.io/publikationen/telegram-chronologie-einer-radikalisierung>

Humprecht, E., Esser, F. & Van Aelst, P. (2020, Januar). Resilience to Online Disinformation: A Framework for Cross-National Comparative Research. <http://dx.doi.org/10.1177/1940161219900126>

Institute for Strategic Dialogue (2024, April 19). 25 Vorschläge für eine effektive Strategie zum Umgang mit Informationsmanipulation. <https://isdgermany.org/25-vorschlaege-fuer-eine-effektive-strategie-zum-umgang-mit-informationsmanipulation>

Isdatechtzo.nl (o. D.) <https://www.isdatechtzo.nl>

Keller, C. I., Freihse, C., & Berger, C. (2024). Staatliche Maßnahmen gegen Desinformation. <https://doi.org/10.11586/2024065>

Lamberty, P. (2024). Jahrestag des russischen Angriffskriegs auf die Ukraine: Glaube an Propaganda- und Verschwörungserzählungen. <https://cemas.io/blog/prorussische-verschwörungserzaehlungen/>

Lamberty, P., & Frühwirth, L. (2023). Informationsmanipulation als komplexe Herausforderung. Integratives Modell zum Umgang mit Desinformation. <https://cemas.io/publikationen/integratives-modell-desinformation/>

Marushevskaya, A. (2025). Five historical pillars of Russian imperial propaganda. <https://euvsdisinfo.eu/five-historical-pillars-of-russian-imperial-propaganda>

Nakashima, E. (2019, 27. Februar). U.S. Cyber Command operation disrupted Internet access of Russian troll factory on day of 2018 midterms. The Washington Post. https://www.washingtonpost.com/world/national-security/us-cyber-command-operation-disrupted-internet-access-of-russian-troll-factory-on-day-of-2018-midterms/2019/02/26/1827fc9e-36d6-11e9-af5b-b51b7ff322e9_story.html

Nimmo, B. (2020). The breakout scale: Measuring the impact of influence operations. <https://www.brookings.edu/articles/the-breakout-scale-measuring-the-impact-of-influence-operations/>

NZ Royal Commission COVID-19 Lessons Learned (o. D.). 2.5 What Happened: public information and communication. Main Report. <https://www.covid19lessons.royal-commission.nz/reports-lessons-learned/main-report/part-two/2-5-what-happened-public-information-and-communication/>

OASIS Cyber Threat Intelligence Technical Committee (o. D.). Introduction to STIX. <https://oasis-open.github.io/cti-documentation/stix/intro>

OECD (2021). OECD Report on Public Communication: The Global Context and the Way Forward. OECD. <https://doi.org/10.1787/22f8031c-en>

OECD (2023). Good practice principles for public communication responses to mis- and disinformation. OECD Public Governance Policy Papers, Bd. 30. <https://doi.org/10.1787/6d141b44-en>

OECD (2024). Facts not Fakes: Tackling Disinformation, Strengthening Information Integrity. OECD. <https://doi.org/10.1787/d909ff7a-en>

OpenAI (2024, 30. Mai). Disrupting deceptive uses of AI by covert influence operations. Archivierte Version: <https://web.archive.org/web/20240530173817/https://openai.com/index/disrupting-deceptive-uses-of-AI-by-covert-influence-operations/>

Palmertz, B., Isaksson, E., & Pamment, J. (2025, Januar). A Framework for Attribution of Information Influence Operations. <https://adacio.eu/a-framework-for-attribution-of-information-influence-operations>

Palmertz, B., Weissmann, M., Nilsson, N., & Engvall, J. (2024). Building Resilience and Psychological Defence – An analytical framework for countering hybrid threats and foreign influence and interference. <https://mpf.se/psychological-defence-agency/publications/archive/2024-03-25-building-resilience-and-psychological-defence---an-analytical-framework-for-countering-hybrid---threats-and-foreign-influence-and-interference>

Pamment, J. (2020). The EU's Role in Fighting Disinformation: Crafting A Disinformation Framework. https://carnegieendowment.org/files/Pamment_-_Crafting_Disinformation_1.pdf

Pamment, J. (2021). RESIST 2 Counter-disinformation toolkit. <https://gcs.civilservice.gov.uk/publications/resist-2-counter-disinformation-toolkit/>

Pamment, J. (2022, November). A Capability definition and assessment framework for countering disinformation, influence, and foreign interference. <https://stratcom-coe.org/pdfs/?file=/publications/download/Defining-Capabilities-DIGITAL.pdf>

Pamment, J. (2024). Psychological defence: Concepts and principles for the 2020s. Psychological Defence Agency. <https://mpf.se/psychological-defence->

[agency/publications/archive/2024-10-28-psychological-defence-concepts-and-principles-for-the-2020s](#)

PersVeilig (2019, Oktober). Press Safety Protocol. https://persveilig.nl/as-sets/f/285119/x/1c6e153d94/050923_persveilig-protocol-a4-eng.pdf

Professional Head of Intelligence Assessment (PHIA) (2019, Januar). Professional Development Framework for all-source intelligence assessment.

Psychological Defence Agency (2024, 3. April). Our mission. <https://mpf.se/psychological-defence-agency/about-us/our-mission>

Psychological Defence Agency (o. D.). Get the tools! <https://bliintelurad.se/en>

Psychological Defence Research Institute (o. D.). Leading Research in psychological defence. <https://www.psychologicaldefence.lu.se/>

Rid, T. (2021). Active Measures—The Secret History of Disinformation and Political Warfare. Profile Books.

Rød, B., Pursiainen, C., & Eklund, N. (2025). Combatting Disinformation – How Do We Create Resilient Societies? Literature Review and Analytical Framework. European Journal for Security Research. <https://doi.org/10.1007/s41125-025-00105-4>

Serrano, R. M., & Sessa, M. G. (2024, 29. November). Beyond Disinformation Countermeasures: Building a Response-Impact Framework. EU DisinfoLab. <https://www.disinfo.eu/publications/beyond-disinformation-countermeasures-building-a-response-impact-framework/>

Shiferaw, S. & Laubenstein, S. (2022, April). Der Business Council for Democracy. Info-Paket via <https://www.bc4d.org>

Smirnova, J. (2024, 29. Oktober). SDA-Dokumente: Einblicke in Russlands digitale Desinformationsstrategie. <https://cemas.io/blog/sda-dokumente-russlands-desinformationsstrategie/>

Tagesschau.de (o.D.). ARD-Faktenfinder. <https://www.tagesschau.de/faktenfinder>

Vilmer, J.-B. J. (2021, Juli). Information Defense: Policy Measures taken against Foreign Information Manipulation. <https://www.atlanticcouncil.org/wp-content/uploads/2021/07/Information-Defense-07.2021.pdf>

Zabirko, O. (2023, 15. Juni). Russkij mir. bpb.de. <https://www.bpb.de/themen/europa/russland/522375/russkij-mir/>

Ziemer, C.-T. (2023, 17. April). Psychologische Interventionen gegen Desinformation. <https://cemas.io/blog/psychologische-intervention/>

Redaktion:
Julia Smirnova
Simone Rafael

Kontakt:
info@cemas.io
25. Juni 2025

Angaben gemäß § 5 TMG
CeMAS – Center für Monitoring,
Analyse und Strategie gGmbH
Konstanzer Straße 15A, D-10707 Berlin

CeMAS, das Center für Monitoring, Analyse und
Strategie, bündelt interdisziplinäre Expertise
zu Verschwörungsideologien, Desinformation,
Antisemitismus & Rechtsextremismus.

Handelsregister: HRB 226823 B
Registergericht: Berlin
USt-ID-Nummer: DE 340877977

Vertreten durch:
Josef Holnburger und Gregor Bauer

Redaktionell verantwortlich:
Josef Holnburger