CeMAS

Research Paper

United Against Manipulation: An Integrated FIMI Response Model

Lea Frühwirth

August 2025

Key Findings

- "FIMI" — short for "Foreign Information Manipulation and Interference" — describes states' attempts to manipulate public opinion in other states in order to destabilize them. It is thus in the core interest of democratic states to protect their populations from such manipulative attempts in the most effective way.
- Selective and reactive approaches are not enough to adequately counter the complex challenge that is FIMI. Instead, a targeted, systematic and combined approach is required to make full use of potential mitigation measures. This requires a sound understanding of the problem, the identification of the appropriate solution space, a broad selection of measures, and the cooperation of all relevant stakeholders. Integrating these elements into a well-coordinated implementation plan is a prerequisite for effective, efficient and sustainable FIMI mitigation.
- Additionally, the model must meet structural requirements to be effective and sustainable. In particular, the prevention of potential misuse must be considered from the outset.
- While the perfect, all-encompassing strategy has not yet been developed, there are many examples of individual measures, frameworks, institutional approaches and processes that provide a helpful starting point for developing an appropriate solution.
- With its integrated FIMI response model, CeMAS presents a comprehensive concept that integrates individual approaches into a holistic model. Values under attack from FIMI are protected and strengthened at an early stage. Emerging incidents are contained promptly, and the quality and appropriateness of the approach is continuously developed. The systematic, case-specific response approaches, undertaken in cooperation with a wide range of stakeholders, form a resilient and sustainable protective shield around the population. This enables the response system to adequately keep pace with the speed and volatility of the problem of FIMI.

Destabilizing Societies by Manipulating Public Opinion

"Foreign Information Manipulation and Interference," or FIMI, is the attempt of one state to manipulate public opinion in other states in order to pursue its own goals. Typically, this involves conveying specific narratives and destabilizing the targeted society. This may include disinformation campaigns or astroturfing (German Federal Government, 2025). These manipulation efforts can take place over multiple years, aiming to influence public opinion on topics such as the Russian war of aggression against Ukraine, German politics and government, the integrity of elections or the veracity of media sources. Fears and insecurities are stirred up, mistrust is sown, and controversial topics are exploited to destabilize society. The long-term spread of such attempts to exert influence carries the risk of undermining social cohesion, fundamental trust in politics, the state and democratic institutions as well as in reputable media sources (Frühwirth, 2023). FIMI is intended to divide and weaken societies — as inconspicuously and insidiously as possible. It is therefore in the core interest of democratic states to protect their populations from such manipulative attempts in the best possible way.

This research paper shows how systematically addressing the complexity of the problem can be used to develop a holistic FIMI response model that strengthens and protects societies in the long term. Proven concepts and practices are incorporated into the design and demonstrate what is possible.

Setting of Goals

To fully consider the complexity and agility of the problem an appropriate response strategy should be derived systematically. First and foremost, this requires the definition of an ideal desired state towards which mitigation attempts can be directed:

Figure 1 : The path from the actual state to the target state

FIMI becomes a problem where illegitimate attempts to exert influence successfully manipulate the population, i.e. influence and change the population's attitudes and ultimately behavior. At this point, the desired target state is:

"The population is not influenced by FIMI."

The aim is to limit the effects of manipulation as much as possible. However, realistically, it can be assumed that this goal will be partially achieved rather than fully achieved. To approach this target state, several aspects need to be clarified. First, there is the question of problem definition. What is considered relevant? Which elements are included, and which ones are not? What is the nature of the problem, and what negative consequences does it cause that we want to prevent?

Our understanding of the solution is derived from this definition. Which areas are potentially helpful in dealing with the problem? For example, if FIMI is primarily understood as an information problem that leads people to believe factually wrong things, the obvious choice for the solution is improving media literacy and communication. If the problem is seen instead as a threat to democracy, the apparent solution is to strengthen challenged democratic values.

In the next step, we define the range of available measures and actors involved in the response. Media literacy may be improved by measures such as awareness campaigns or educational programs. Democracy-promoting measures could include transparency initiatives by media companies or engaging local communities in political decision-making processes to build trust.

In the final step, the approaches that have been developed must be incorporated into an implementation model that turns theory into practice. What sort of organizational structures are required to enable the necessary participants to act? Which plans, roles, and processes are needed? How can quality be ensured? The design of the implementation model will ultimately determine its effectiveness. All in all, comprehending the problem, understanding the solution space, identifying the countermeasures and response actors as well as the implementation model provides a roadmap to move from the actual to the target state.

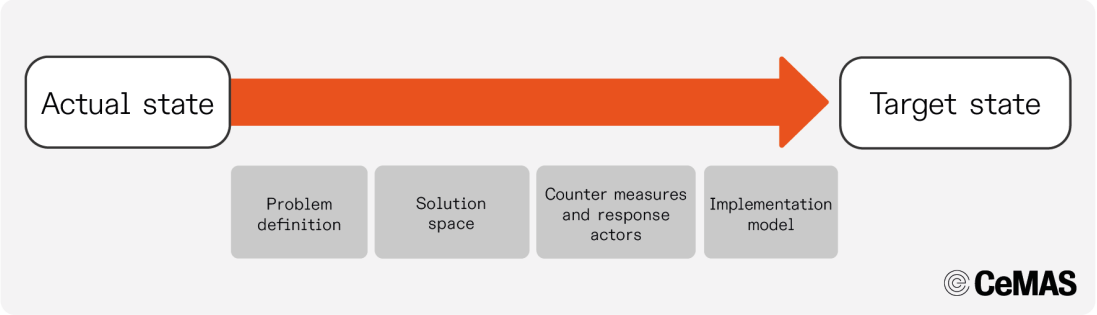

Figure 2: Developing the concrete aspects paves the way to the target state

Best Practices: Existing Concepts Demonstrate What is Possible

Existing concepts provide valuable inspiration and impetus for developing new solutions. Some illustrative examples are presented below. As the range is extensive, this list is not intended to be exhaustive.

Problem Definition

The definition of the problem significantly influences the subsequent solution areas and measures. If the problem scope is too narrowly defined, there is a risk that the available potential for overcoming it will not be fully utilized. Disinformation, which can be part of FIMI, is often viewed primarily as an information problem, with its risk potential rooted in the spread of false claims. CeMAS, on the other hand, views disinformation as a complex problem that goes beyond the mere information aspect. The integrative model for dealing with disinformation highlights the facets of technology, security and democracy alongside the information perspective and emphasizes the need for social science as an evidence-based foundation for action (Lamberty & Frühwirth, 2023). According to the integrative model, disinformation is a problem because it causes people to believe false claims, compromises the security of marginalized groups and spreads disruptive impulses that can destabilize democracy in the long term. While each individual perspective is important and relevant, approaches based on only one of them are bound to fall short. An integrative approach makes it possible to look at disinformation in all its complexity and opens a broader solution space in the next step.

Solution Space

The definition of the problem is followed by the identification of suitable solution spaces. The OECD draws the ideal picture of a mitigation strategy that is capable of action, adaptive, inclusive and interconnected to address emerging problems preventively and react promptly. Among other things, it recommends institutionalization, transparency, timeliness, prevention, evidence-based approaches and whole-of-society collaboration as core principles (OECD, 2023). Cross-national studies by the Bertelsmann Foundation have shown that government measures focused on mitigating the spread of false information, regulating platforms, promoting transparency, improving state communication, fostering media pluralism and building public institutions (Keller et al., 2024). The following examples provide an insight into existing solutions:

- At the EU level, programs focus on early detection and containment, providing information, empowering and increasing the resilience of the population, regulating digital services and protecting the media (European Commission. Directorate General for Communication, 2024; European Commission, 2018; European External Action Service, 2025b; European Commission, 2025b).
- The "Framework to Counter Foreign State Information Manipulation," which was endorsed by the United States, the United Kingdom and Canada in January 2024, establishes five action areas: national strategies and policies, government structures and institutions, human and technical capabilities, civil society, independent media and academia and multilateral engagement (Government of Canada, 2024).
- Sweden relies on the principle of psychological defense, which is based on the promotion of resilience, threat detection, deterrence and strategic communication (Pamment, 2024).
- The Dutch government's strategy to effectively combat disinformation aims to strengthen public discourse and reduce the influence of disinformation (Government of the Netherlands, 2022).
- The Taiwanese organization Doublethink Lab notes the central role of civil society actors in Taiwan, who work together with state and other actors and are strengthened by a shared vision (Doublethink Lab, 2024).
- The Bavarian Alliance against Disinformation relies on public services and cooperation with platforms, media, politicians and civil society (Bavarian State Ministry for Digital Affairs, n.d.).

Countermeasures and Response Actors

The range of possible individual countermeasures is vast. To demonstrate the starting points of different countermeasures, the spread of FIMI is presented as a communication process, in which misleading communication is created by an actor to reach individuals and ultimately influence societies (Lamberty & Frühwirth, 2023):

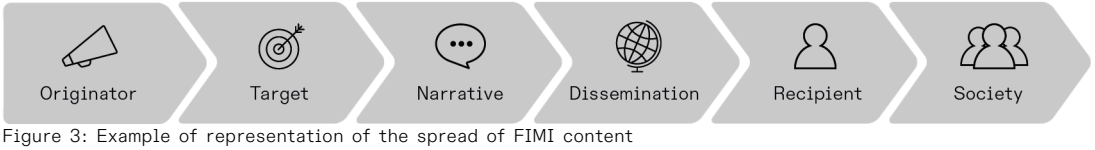

Figure 3: Example of representation of the spread of FIMI content

Each step of the process can be addressed by specific countermeasures, undertaken by the respective stakeholder. These actors must be jointly involved in the response to unlock the full range of mitigation measures: The much-discussed whole-of-society

approach is needed. Examples of measures that can be used for each process step are presented below. These options may or may not be suitable or appropriate depending on the context. Therefore, they should be thoroughly examined before implementation.[1]

Originator-related Measures

FIMI campaigns are created because they are useful to a FIMI actor, and as such, a sound knowledge of their objectives is helpful. Where it is possible to reduce the actor's willingness to engage in FIMI activities, a reduction in problems can be expected.

Originator-related Measures

Measure	Goal	Actors	Examples
Establishing knowledge of FIMI actors	In-depth knowledge to derive suitable measures	Scientific research, civil society, intelligence services	Research on world view and objectives,[2] historical behavior[3] or current practices[4]
Deterrence	Demotivation of the actor	State, alliances of states	Demonstrating awareness,[5] withdrawing infrastructure[6] or imposing sanctions[7]

Figure 4: Examples of originator-related measures

[1] For deeper insight into the range of possible measures, see Ziemer, 2023; Vilmer, 2021; Rød, 2025; and Humprecht et al., 2020.

[2] Insights into historical concepts and worldview such as the "Russkij mir" (Russian world) provide helpful context for interpreting the Kremlin's actions (Zabirko, 2023; Marushevska, 2025).

[3] Knowledge of historical behaviors and instruments of FIMI actors - such as Soviet "Active Measures" during the Cold War - enables better anticipation and assessment of actions (Rid, 2021).

[4] Analyses of the communication landscape and the functioning of influence attempts provide information on the typical approaches and weaknesses of FIMI actors (European External Action Service, 2025a; Smirnova, 2024).

[5] The public disclosure of findings on FIMI activities as well as their condemnation and rejection signals vigilance to FIMI actors (European Parliament, 2025).

[6] According to the US military, internet access of the Russian "troll factory" Internet Research Agency (IRA) had been temporarily blocked to protect the 2018 midterm elections (Nakashima, 2019).

[7] Due to the Russian war of aggression against Ukraine, the European Union adopted sanctions against Russia. These also explicitly affect originators of disinformation (European Union, 2025).

Dissemination-related measures

Manipulative content must reach people to be effective. Accordingly, reducing or preventing the creation and dissemination of manipulative content is a potential lever for curbing it.

Dissemination-related Measures

Measure	Goal	Actors	Examples
Withdrawal of assets and tools	Content can no longer be created or only with increased effort	State, platforms, journalism	Account blocking due to internal platform investigations[8] or investigative research,[9] confiscation of websites[10]
Platform regulation	Social networks consistently implement content moderation for FIMI content	State, alliances of states, platforms	State intervention in platforms,[11] voluntary commitment,[12] Digital Service Act[13]
Criminalization	Reduction of dissemination through the creation of criminal liability	State	Adoption of criminal laws to prosecute FIMI activities[14]

Figure 5: Examples of dissemination-related measures

Measures to Strengthen Recipients

Manipulative content is intended to influence as many individuals as possible in order to ultimately shift public opinion. Protection and countermeasures at an individual level can be taken before, during and after exposure:

[8] According to OpenAI, activities of FIMI actors were identified and access was blocked (OpenAI, 2024).

[9] As part of investigative research, Qurium and CORRECTIV contacted service providers whose services had been used by FIMI actors. They subsequently blocked access (Bernhard et al., 2024b).

[10] The US Department of Justice announced the seizure of FIMI websites in 2024 (Bernhard et al., 2024a).

[11] Following a conversation between the Federal Ministry of the Interior and Telegram in 2023, an increase in suspensions of conspiracist ideology and far-right channels and groups was observed (Holnburger, 2023).

[12] The EU's Code of Practice on Disinformation is based on voluntary self-commitment and platform cooperation. From July 2025, this is to become a Code of Conduct in accordance with the DSA (European Commission, 2025a).

[13] The European Digital Services Act (DSA) serves to regulate platforms for digital services, for example through obligations in content moderation or risk assessments (European Commission, 2024).

[14] Such laws exist, for example, in Singapore, Taiwan and the Philippines (Keller et al., 2024).

Measures to Strengthen Recipients

Measure	Goal	Actors	Examples
Public awareness campaign	Creating risk awareness and teaching basic knowledge	State, media, civil society	Swedish awareness campaign "Don't Be Fooled",[15] and Dutch information page "Isdatechtzo"[16]
Target group-specific empowerment	Teaching basic knowledge to all age groups	Civil society, state	Addressing adults with offerings at the workplace,[17] in adult education centers[18] and associations.[19] Addressing young people outside of schools in the German Youth Fire Brigade[20]
Prebunking	Inoculation against narratives and tactics	Civil society, research, platforms, media	Google Prebunking Campaign on YouTube[21]
Gamified approaches	Gamified inoculation	Civil society, research	Online educational games for low-threshold awareness raising[22]
Fact checks	Subsequent invalidation of false allegations that have already been seen	Journalism, civil society	Freely accessible, digital fact check offers[23]
Counter-communication	Subsequent statements on false allegations that have already been disseminated	State, media	Taiwanese 2-2-2 principle[24]
Transparency initiatives	Deepening the traceability of content creation	Technology companies, civil society, journalism	Contextualization of content through certificates[25]

Figure 6: Examples of measures to strengthen recipients

[15] The awareness campaign conveys basic ways of dealing with disinformation in the form of posters, flyers and online content (Psychological Defence Agency, n.d.).

[16] The website provides information on how disinformation works and manifests and gives recommendations for self-protection (Isdatechtzo.nl, n.d.).

[17] The Business Council for Democracy (BC4D) initiative offers awareness workshop formats in the workplace on the topics of disinformation, conspiracy narratives and hate speech (Shiferaw & Laubenstein, 2022).

[18] As part of the "faktenstark" project of the Amadeu Antonio Foundation and codetekt, compact courses on disinformation are offered at adult education centers (Deutscher Volkshochschulverband, 2025).

[19] As part of the Bavarian Alliance against Disinformation, associations, among others, are involved in order to raise awareness for disinformation (Bavarian State Ministry for Digital Affairs, n.d.).

[20] As part of a cooperation between CORRECTIV and the German Youth Fire Brigade, media skills training for young people is offered via the association structures (CORRECTIV, 2025).

[21] Awareness-raising ads were played on YouTube, Facebook and Instagram (Google, n.d.).

[22] Online games such as "Bad News", "Go Viral" and "Harmony Square" are intended to use gamification to educate about disinformation (Cambridge Social Decision-Making Lab, n.d.).

[23] Fact-checking editorial offices check claims for their truthfulness so that users can recognize false claims they have seen (CORRECTIV, n.d.; Tagesschau.de, n.d.; BR24, n.d.).

[24] The 2-2-2 principle describes the optimal design of ad hoc communication on disinformation in order to reach as many people as possible. According to this principle, communication should take place within two hours, contain 200 words and be supplemented by two graphics (Doublethink Lab, 2024).

[25] For example, a photo on a website could be supplemented with information on the place of origin and the processing steps (Coalition for Content Provenance and Authenticity, n.d.).

Measures to Strengthen Society

FIMI aims to destabilize societies by systematically fomenting mistrust in democratic institutions, politicians, political parties, and reputable media as well as attacking social cohesion. Protective measures are therefore also needed at a societal level. They should strengthen and protect the values that are threatened by FIMI.

Measures to Strengthen Society

Measure	Goal	Actors	Examples
Strengthening the information space	Protecting the media, ensuring the availability of reputable sources	State, media	Dutch PersVeilig protocol for the protection of journalists[26]
Strengthening the sense of cohesion	Change of perspective from differences to similarities to strengthen social cohesion	State, civil society, media	New Zealand communication campaign “Unite against COVID-19”[27]
Participation and transparency initiatives in politics	Promoting trust in the state and democracy	State, civil society	Participation project “Forum gegen Fakes”[28]
Vulnerability analysis	Knowledge of current possible starting points for FIMI activity, for example polarizing issues, dissatisfaction or tensions	State, research, civil society	Population survey on the approval of Russian propaganda[29]

Figure 7: Examples of measures to strengthen society

Implementation Model

A well-stocked toolbox is an important resource for addressing this problem. However, the effective and efficient use of the many possible measures and the coordinated, cooperative working methods of the relevant stakeholders are crucial. Political prioritization is a necessity for any sustainable mitigation efforts. Only where the solution to the problem is considered sufficiently important can effective structures be created to pave the way from the current to the target state. A suitable model provides clarity around the scope of action, processes and roles. A cross-national study conducted by the Bertelsmann Foundation at the end of 2024 showed that countries with comprehensive, strategic mitigation strategies for FIMI are still the exception (Freihse

[26] The PersVeilig initiative is intended to protect journalists from assaults. Among other things, it was agreed to consistently report assaults and prioritize the processing of such reports (PersVeilig, 2019).

[27] As part of response to the COVID-19 pandemic, the government of New Zealand conducted a campaign to emphasize the common identity and threat management of the population to bridge societal divisions (NZ Royal Commission COVID-19 Lessons Learned, n.d.).

[28] The Bertelsmann Stiftung's "Forum against Fakes" project relies on citizen participation to develop solutions for dealing with disinformation (Bertelsmann Stiftung, 2024).

[29] In order to determine the extent to which Russian propaganda narratives could catch on with the German population, approval ratings for core narratives were collected in representative surveys (Lamberty, 2024).

& Bochert, 2024). The following examples provide insights into selected implementation concepts:

Holistic Models

- The Dutch government's strategy to combat disinformation defines the problem and the scope of the solution as well as determining the measures, responsible parties and deadlines required for implementation. The document describes the contributions of various ministries, includes the role of scientific research and identifies forms of cooperation (Government of the Netherlands, 2022).
- The Latvian approach is based on national values. Its goals are defined as state and social resilience against interference in democratic processes and ensuring the ability to act in the event of a crisis. The program's focus is on strategic communication and safeguarding the information space. Stakeholders from the state, municipalities, civil society, research and the private sector are involved. Cooperation is coordinated by the State Chancellery (Cabinet of Ministers, Republic of Latvia, 2023).

Implementation of Individual Aspects

- The institutionalization of containment efforts can take various forms. Coordination units and task forces are widespread, such as the Central Office for the Detection of Foreign Information Manipulation (ZEAM) in Germany. This task force, created on the instructions of several ministries, is dedicated to identifying and analyzing FIMI activities in order to facilitate appropriate responses by the German government (Federal Ministry of the Interior, n.d.). In Sweden, the Psychological Defense Agency and in France the VIGINUM agency also manage cross-ministerial coordination to deal with FIMI, in addition to detection and analysis (Ferriol, 2022; Psychological Defence Agency, 2024; OECD, 2024).
- Examples of sub-process design for analyzing and responding to detected activities can be found at the European External Action Service (2024), the British Government Communication Service (GSC) (Pamment, 2021) and in the CORE cooperation project (European Commission Joint Research Centre, 2023). The design of response processes and structures can also benefit from long term experience in the areas of emergency response organizations, disaster control and cybersecurity (German Red Cross, n.d.; Federal Office of Civil Protection and Disaster Assistance, n.d.; Federal Office for Information Security, n.d.).
- The German Federal State Working Group on Hybrid Threats (BLoAG Hybrid) has issued recommendations for state ministries and local authorities to

support protective measures at the local level (Federal Ministry of the Interior, 2023).

- Sweden offers an example of the systematic integration of scientific research (Psychological Defense Research Institute, n.d.). The Dutch strategy also mentions the important contribution of scientific research (Government of the Netherlands, 2022).
- There are also examples of quality assurance, for instance in the form of methodology for observation classification (DISARM Foundation, n.d.; Pamment, 2020), target-oriented response selection (Serrano & Sessa, 2024), assessment of impact and relevance (Nimmo, 2020; Pamment, 2021), actor attribution (Palmertz et al., 2025) and transparent classification of result robustness (Professional Head of Intelligence Assessment (PHIA, 2019).
- Reflection questions to inform the design of response models help in developing new concepts (Palmertz et al., 2024) while assessments allow for the overall response to be checked for effectiveness and development needs (Pamment, 2022; Rød et al., 2025).
- Cooperative approaches strengthen the response community through the exchange of observations and knowledge, as well as through active collaboration, as shown by pilot projects in the areas of fact-checking (European Commission, 2024; European Fact-Checking Standards Network, n.d.), detection (Alliance4Europe, n.d.) and alerting (FIMI-ISAC, n.d.; European External Action Service, 2019).
- Standardizing data structures facilitates rapid processing and dissemination as well as the comparability of incidents (DISARM Foundation, n.d.; OASIS Cyber Threat Intelligence Technical Committee, n.d.).

Integrated FIMI Response Model

In the following section, an integrated model for mitigating foreign influence will be developed, taking into account the concepts and examples presented. In addition to approaching the target state of "The population is not influenced by FIMI," further requirements must be met. For example, the problem should be addressed holistically and in the long term by integrating both preventive and reactive measures. To keep pace with the adaptability of the problem, response efforts must be resource-efficient and flexible. The model design must be compatible with best practices at the national and international levels to ensure practical applicability.

Whole-of-society cooperation must consider the appropriateness for each stakeholder to each measure in order to avoid creating new risks. For example, fact checks should not be created by state actors. Organizational design must also include necessary checks and balances to safeguard the capability to act, for example, in the event of an authoritarian change of government without allowing inappropriate instrumentalization. It is thus important to maintain a balance: A strong, cooperative mitigation approach requires the driving force of a state that takes the problem seriously and opens spaces for solutions where individual actors reach the limits of their own resources and competencies. At the same time, the resulting construct must be designed in such a way that it does not itself become a potential threat to the population and its democratic freedoms (Institute for Strategic Dialogue, 2024). To ensure a sustainable ability to act, the organizational structure must be rooted from a long-term perspective and should not be subjected uncertainty regarding its continued existence with each new legislative period.

Taking these requirements into account, the model can now be developed. For this purpose, we define the desirable state and then work backward to identify the necessary steps to achieve this outcome. This backcasting is used to create a development plan that closes the gap between the actual and target state.

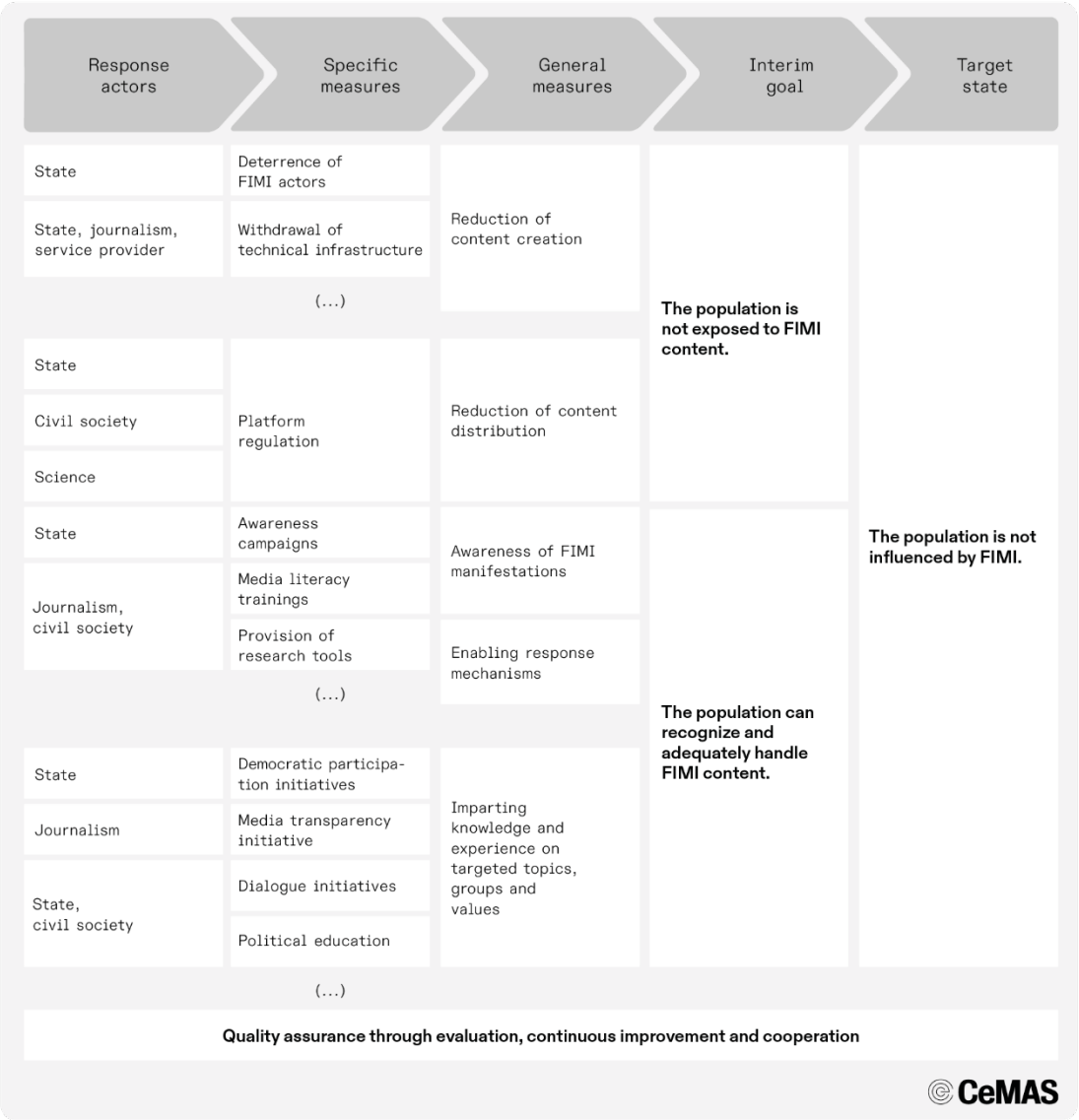

Figure 8: Starting from the target state (right), the respective prerequisites can be determined in order to close the gap between the actual and target state

Interim goals are identified that can promote the desired target state. To ensure that the population is not influenced by FIMI, the amount of misleading content available should be reduced. After all, misleading content can only influence its target audience if it achieves exposure.

On the other hand, building capacity among the population can help to ensure misleading information is recognized and refuted, achieving the interim goals of reducing exposure and increasing resilience to manipulation. Appropriate measures are selected to attain these interim goals. Measures for deterrence and platform regulation could address exposure reduction, while a combination of preventive social resilience programs, promotion of media literacy and prebunking strengthens the population's resilience to manipulation. This example selection of measures reveals step by step which actors need to be involved in the response efforts.

Overall, this process of development enables a goal-oriented creation of a holistic response strategy that integrates both the preventive and the reactive perspective and opens a space for cooperative FIMI mitigation.

The insights gained can now be presented as a holistic scope of actions comprised of domains, measures and actors. These actions form a protective shield around the population. This enables both a short-term, timely response to emerging threats and consistent preventive work on long-term factors to ensure civil protection. The executive domains of prevention and reaction are strengthened by the domain of excellence, which ensures quality and continuous improvement.

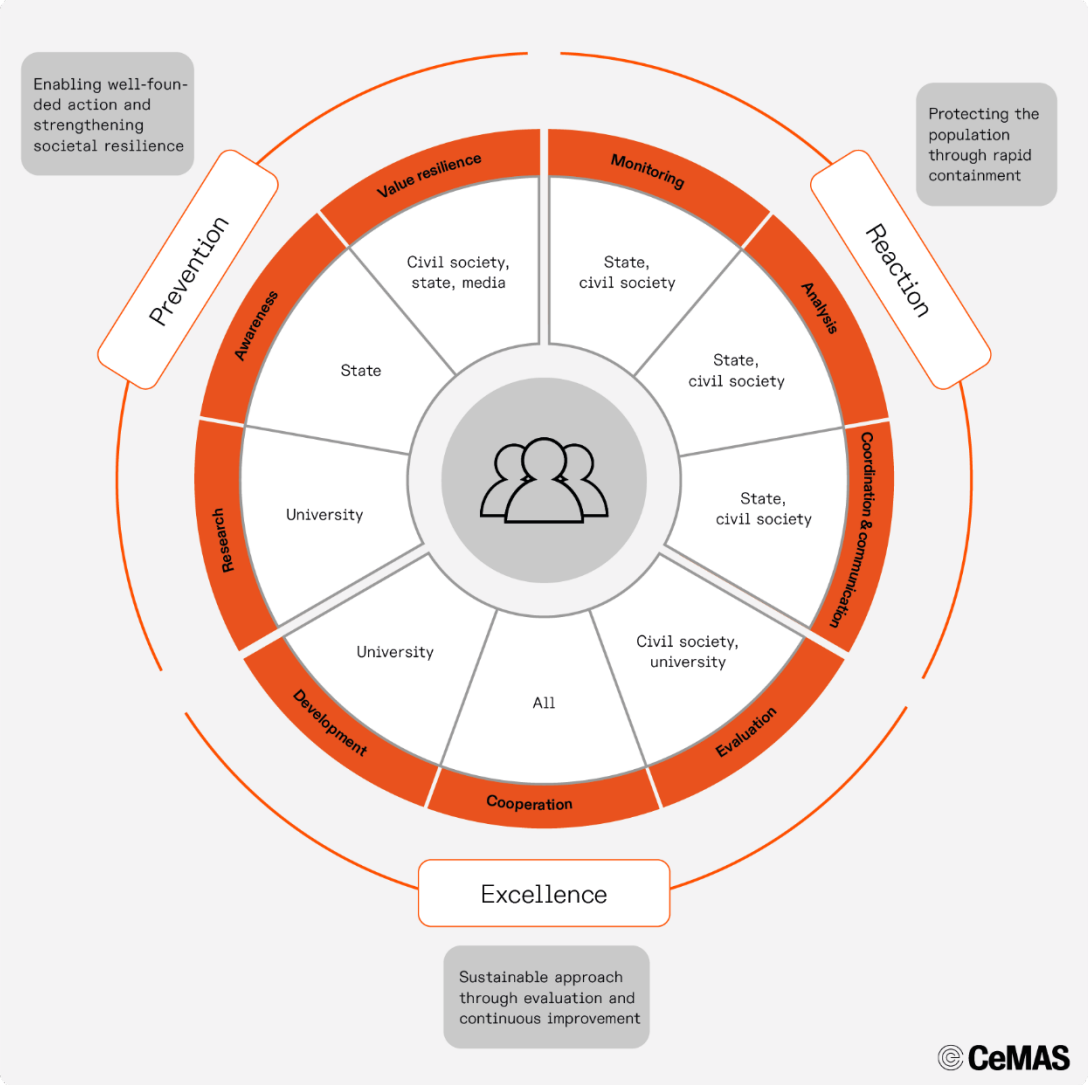

Figure 9: The scope of actions of the integrated response model forms a protective shield around society

Prevention

The prevention domain is dedicated to strengthening individuals and society in the long term. This includes fundamental research of the problem, solution, target group and information space, as well as the implementation of support measures to improve individual and societal resilience to manipulation. Typical actors in this domain come from the fields of scientific research, media, communication and civil society. The prevention area creates the evidence-based foundation for response efforts and sustainably strengthens individuals and society against manipulation attempts.

Reaction

The reaction domain deals with the containment of FIMI campaigns. This includes continuous monitoring for early detection, which checks known patterns of behavior for new activities (top-down) as well as the exploratory investigation of potential new forms (bottom-up). When activities are identified, they are systematically assessed by analysts. If necessary, an escalation process is triggered to initiate response measures. Accordingly, competencies and authorizations for coordination and communication must be available to facilitate stakeholder cooperation. Typical actors in this domain come from the government and civil society. The reaction domain provides a well-founded and timely response to threat scenarios.

Excellence

The domain of excellence is dedicated to assuring quality and continuous improvement, for example through the systematic evaluation of all measures implemented. To sustainably strengthen and further develop the mitigation strategy, development opportunities are explored, cooperation and knowledge exchange are promoted and new tools and methods are developed. Typical actors in this domain come from academia and civil society. The domain of excellence ensures that response efforts yield high-quality results and can keep pace with the evolving threat landscape.

Overall, the scope of actions represents the sectors that are constantly working to protect and strengthen society in the face of FIMI threats. In addition to the specific actors mentioned here, other stakeholders may become active as needed, for example, in response to specific threats. The effectiveness and efficiency of the work ultimately depends on the way it is carried out: sufficient resources at both a human and financial level, streamlined processes, clear roles, productive collaboration and a system of improvement with a healthy error culture and willingness to change are required to address this challenging problem. The organization should be characterized by a work culture with an affinity for change and the courage to make mistakes, as overcoming this dynamic problem will require testing, discarding and adapting procedures. Instead of engaging in siloed mentalities, stakeholders should focus on the

common, overarching goal, thus creating certainty of action through alignment and prioritization when dealing with dynamic developments.

The Ideal Response

While the scope of actions provides an important overview of the domains, measures and actors for a strategic concept, clearly defined procedures and processes are required to move from theory to practice. Although FIMI cases will rarely be identical, the basic response steps required for acute incidents can be defined:

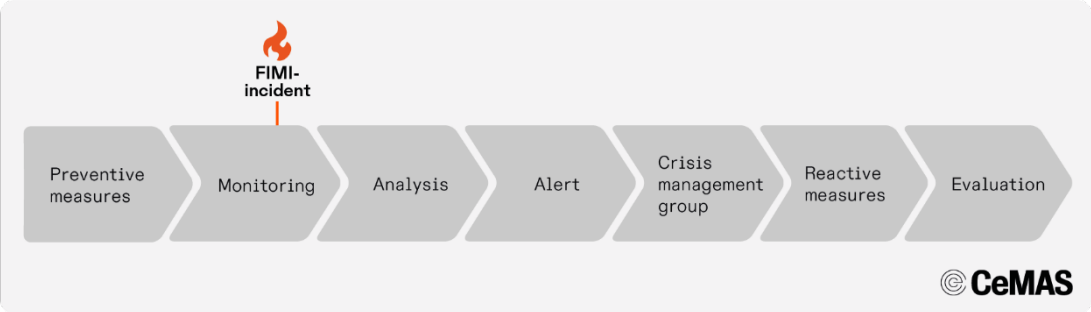

Figure 10: Basic steps in an acute case

Preventive measures are put in place before a new acute case occurs. They are designed for the long term and gradually build up protective elements that should have a strengthening effect in an acute case. The establishment of **real-time monitoring** is a central necessity for the identification of new FIMI activities. When they occur, they are documented in a timely and standardized manner, analyzed and, if sufficiently relevant, escalated as an **alert** to the crisis management group leadership. If the latter agrees with the relevance assessment, it convenes the **crisis management group** at short notice with high priority and determines on a case-by-case basis which stakeholders are required for the response. The crisis management group discusses the case and decides on appropriate **reactive measures**. These are then promptly implemented and reviewed. If the results are satisfactory, the case is closed. In the final step, the case and countermeasures are **evaluated** to identify the need for adjustments and the potential for development for use in future cases. The ideal implementation is illustrated below using realistic scenarios:

Scenario 1: Rapid Containment of a Coordinated Disinformation Campaign

The starting point is a disinformation campaign on social media that follows a familiar pattern. Starting at 8:00 a.m., inauthentic coordinated accounts post hundreds of statements that present as German citizens expressing their opinions. They spread statements against support for Ukraine, discredit the German government and stir up fears of economic decline. The posts contain links to fake pro-Russian news articles that mimic the look of leading German media sources. The original posts are widely shared by other campaign accounts.

Using the integrated response model, the reaction should be as follows:

Preventive Measures:

Comprehensive public awareness campaigns and media literacy training have reached the public and informed them of the nature of FIMI campaigns. Transparency initiatives by the press ensure that users can find in-depth insights into the creation of content by reputable media outlets, enabling them to better distinguish between authentic and misleading content. At an operational level, it was determined early on that, in an acute case, the highest priority would be to convene a crisis management group with the necessary stakeholders for the response. Authority and permission to cooperate and exchange information were also established.

Monitoring:

Based on the familiar campaign pattern, the activity is immediately registered in monitoring. It is documented and transferred to the analysis step. Further developments continue to be monitored.

Analysis:

Analysts determine the FIMI actor behind the campaign, assess potential risk, determine recommendations for action and share their findings with the head of the crisis management group in the form of an alert by 9:00 am.

Crisis Management Group:

The leadership of the crisis management group reviews the recommendations, agrees on the relevance of the case and schedules a crisis management group meeting for 12:00 pm. The necessary participants are the relevant analysts, representatives of the affected platform, the Ministry of Foreign Affairs, the Ministry of the Interior, the Federal Office for Information Security, the Federal Press Office, the Digital Services Coordinator and fact-checking organizations. At this meeting, the situation is presented and the immediate removal of content and accounts is proposed as a measure to mitigate immediate dissemination risks. This proposal is accepted after thorough discussion among the stakeholders involved.

Reactive Measures:

The crisis management group decides that the affected platform should remove posts and accounts after an internal review, based on the clear identification of the actor, their manipulative nature and the associated violation of platform guidelines. The Federal Office for Information Security investigates the digital origin points of the campaign for possible starting points for countermeasures. The fact-checking organization provides fact checks about core narratives so that citizens who have already come into contact with manipulative content can find guidance. Active counter-messaging is not initiated for the time being, so as not to reinforce the campaign by attracting more attention. The alert will be shared in FIMI response networks to inform researchers, fact checkers, and other state actors about the ongoing activity. For the duration of the open case, a secure form of communication is established for informal exchange between the response actors involved. At the end of the crisis team meeting at 1:00 pm, the stakeholders implement their measures and provide updates. The crisis management group meets again at 4:00 pm to discuss the implemented measures and to review the outcome. At this point, the platform has implemented moderation measures following an internal review, and the Federal Office for Information Security has informed the service providers of the website infrastructure used about the misuse. The monitoring department will keep the case under observation for another week, and, if activity has subsided, will close, document and hand over the case to the excellence department for evaluation.

Evaluation:

As part of the evaluation, the incident, implemented measures, outcomes as well as effectiveness and efficiency of the procedure are analyzed and assessed. Through this process, the crisis management group gains insights into which existing procedures should be retained, adapted or further developed. Specific recommendations for action are used to further develop the response system.

Scenario 2: Containment of disinformation during a natural disaster

In a remote region with limited accessibility, high water leads to landslides, flooding, power outages, and communication problems. Russian state media and pro-Russian influencers spread false claims online about local, state, and federal policy. They claim that authorities are unprepared, unable, or unwilling to help the population or would rather invest money in supporting Ukraine. Conspiracy theories emerge, claiming that the floods were caused by the alleged use of weather weapons. The content is mainly spread via messenger services.

The integrated model enables the following response:

Preventive Measures:

Prior to these events, programs were carried out to strengthen social resilience. These projects engaged citizens in participatory ways of shaping the conditions in their communities, giving them the opportunity to experience the complexity of political processes first-hand and to get to know their political representatives.

Transparency projects in the media sector have closed gaps in local media coverage and provided insights into how reputable media sources carry out their work. Cooperative projects have brought social groups together to initiate improvements in their own areas, promote self-efficacy and reduce prejudices. The authorities responsible for dealing with natural disasters have increased communication efforts to ensure a basic level of public knowledge about risks, precautionary measures, self-protection, and key steps to take in the event of an emergency as well as to educate people about likely misleading claims. At the local level, citizens were proactively informed about local conditions and crisis-proof contact points for reliable information. The population is informed about the political efforts of disaster prevention and management, is aware of the risks of disinformation and knows where to find reliable information. A sense of security, confidence and trust in the responsible authorities have been strengthened.

Monitoring and Analysis:

The spread of the disinformation narratives described above via messenger services will only become apparent at a later stage, as private messaging services can't be monitored, unlike public data from social media platforms. Once the spread of the narratives becomes known, for example by becoming visible in public digital discourse, they are treated using the same processes of monitoring and analysis as in Scenario 1.

Crisis Management Group:

Analysts and the leadership of the crisis management group assign a high escalation level, as the false allegations are likely to put people at additional risk. The members of the crisis management group include the relevant analysts, as well as representatives of the affected platforms, the Foreign and Interior Ministries, the Federal Press Office, Federal Office of Civil Protection and Disaster Assistance, local emergency services and the Digital Service Coordinator.

Reactive Measures:

As it must be assumed that the FIMI content has already been disseminated among the population, communication is key. This messaging must convey accurate information, remind citizens of existing plans and procedures, and provide guidance for action. It should also warn against false claims and rumors, as well as recommending ways of responding to them without repeating, and thus reinforcing, specific claims. Accounting for possible technical failures, care is taken to ensure that all affected citizens have access to secure information and know where to find it — for example via a radio station, a website or specially set up messenger groups. Existing local networks, such as clubs and volunteer organizations are involved in providing further support in spreading the messaging. Beyond the directly affected group, the Federal Press Office is setting up proactive communication to counteract the instrumentalization of the flood situation among the public who are not directly affected.

Evaluation:

The evaluation process is similar to Scenario 1. Due to the increased number of stakeholders involved in the response, it is advisable to review the cross-organization collaboration capabilities, for example with the Federal Agency for Technical Relief (THW) or local emergency services. Both response systems could benefit from a collaborative approach to FIMI incidents in future crises.

The example scenarios demonstrate how the integrated model's theoretical scope of actions comes to life, protecting the population from illegitimate influence attempts by reducing exposure and promoting resilience. These two examples alone make it clear that different approaches are effective in different cases and should be tailored accordingly.

Conclusion

This research paper presents the systematic design of an integrated FIMI response model. It presents existing examples of problem definitions, solution concepts, objectives, measures, response actors and approaches for process design as well as showing which resources should become available when the problem is acknowledged in its complexity and is systematically addressed. While individual approaches can deal with certain aspects of the problem in isolation, their integration into a holistic concept opens the full spectrum of solutions. This enables a tailor-made response to individual FIMI cases. In particular, the integration of long-term prevention efforts ensures that societal values that are systematically targeted by FIMI are sustainably strengthened. The ingrained cooperative approach and the explicit focus on efficient action structures increase both the quality of results and the speed of response and further development of response processes.

Effective protection against FIMI must embrace complexity and use it to its advantage. The model outlined here is not intended to be a rigid blueprint, but rather to provide a foundation and to highlight viable paths and existing resources in order to support the development of an appropriate approach. Nor have all the questions been answered, as the concrete design must be created with an interdisciplinary and thorough process. Moreover, its ultimate form should not come from a single stakeholder and the limited scope of a research paper cannot do it justice. The question of the concrete manifestation of the described fields, actors and processes in an organizational form is by no means trivial, as an appropriate response must meet a variety of requirements. In particular, the potential for abuse must be considered carefully and in an interdisciplinary manner. Despite all these challenges, the development of an integrated response model remains urgently necessary, as FIMI actors continuously exploit vulnerabilities in the current mitigation system to destabilize targeted societies.

The strategy should reflect the complexity of the problem and stakeholders' own values by taking a cooperative approach. It requires expertise and perspectives from government organizations, civil society, academic researchers and the media, among others, to develop an effective approach and distribute power responsibly. However, the state must act as the driving force, as protecting the population from FIMI influences is one of its core responsibilities. The state creates a space in which various stakeholders can meet and develop solutions. The cornerstone for the feasibility of all further steps is the political prioritization of the problem and of mitigation efforts. This paper is intended to provide the basis and impetus for further work on an integrated response to FIMI.

Bibliography

Alliance4Europe. (n.d.). *A4E Counter Disinformation Network (CDN).* https://alliance4europe.eu/cdn

Bavarian State Ministry for Digital Affairs. (n.d.). *Bavarian alliance against disinformation.* https://www.stmd.bayern.de/themen/bayern-allianz-desinformation

Bernhard, M., Hock, A., & Thust, S. (2024a, September 3). *USA confiscates propaganda websites that targeted Germany.* CORRECTIV. https://correctiv.org/faktencheck/russian-disinformation/2024/09/05/doppelgaenger-usa-beschlagnahmen-propaganda-webseiten-die-deutschland-im-visier-hatten

Bernhard, M., Hock, A., & Thust, S. (2024b, July 18). *According to CORRECTIV research: Russian propaganda campaign comes to a standstill.* https://correctiv.org/aktuelles/russland-ukraine-2/2024/07/18/nach-correctiv-recherche-russische-propaganda-kampagne-geraet-ins-stocken

Bertelsmann Foundation. (2024). *Forum against fakes: Citizens' report on dealing with disinformation.* https://doi.org/10.11586/2024149

BR24. (n.d.). *#Faktenfuchs.* https://www.br.de/nachrichten/faktenfuchs-faktencheck,QzSIzl3

Federal Office of Civil Protection and Disaster Assistance. (n.d.). *Crisis management.* https://www.bbk.bund.de/DE/Themen/Krisenmanagement/krisenmanagement_node.html

Federal Office for Information Security. (n.d.). *I have an incident – Organizational checklist.* https://www.bsi.bund.de/dok/13282672

Federal Ministry of the Interior. (2023). *Raising awareness in dealing with hybrid threats including disinformation (BLoAG).* https://www.bmi.bund.de/SharedDocs/downloads/DE/publikationen/themen/heimat-integration/wehrhafte-demokratie/BMI24013.html

Federal Ministry of the Interior. (n.d.). *Central Office for the Detection of Foreign Information Manipulation (ZEAM).* https://www.bmi.bund.de/SharedDocs/schwerpunkte/DE/desinformation-bei-bt-wahl/zeam-artikel.html

Cambridge Social Decision-Making Lab. (n.d.). *Prebunking conspiratorial, electoral, and medical disinformation through online games.* https://inoculation.science/inoculation-games

Coalition for Content Provenance and Authenticity. (n.d.). *An open technical standard for tracing the origin of media.* https://c2pa.org/

CORRECTIV. (2025). *CORRECTIV and the German Youth Fire Brigade launch cooperation.* https://correctiv.org/in-eigener-sache/2025/02/05/brandherd-desinformation-correctiv-und-deutsche-jugendfeuerwehr-starten-kooperation/

CORRECTIV. (n.d.). *CORRECTIV.factcheck.* https://correctiv.org/faktencheck/

German Federal Government. (2025). *What is FIMI?* https://www.bundesregierung.de/breg-de/aktuelles/fimi-fake-news-international-2227610

German Adult Education Association. (2025). *Compact courses on disinformation for adult education centers in cooperation with faktenstark.* https://www.volkshochschule.de/meldungen/politische-jugendbildung-kooperation-mit-faktenstark.php

German Red Cross. (n.d.). *Assistance system and crisis management in the German Red Cross.* https://www.drk.de/das-drk/auftrag-ziele-aufgaben-und-selbstverstaendnis-des-drk/hilfeleistungssystem-und-krisenmanagement/

DISARM Foundation. (n.d.). *DISARM helps identify and respond to malign information influence operations.* https://www.disarm.foundation/

Doublethink Lab. (2024, August 9). *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

European Commission. (2018). *Action plan against disinformation.* https://commission.europa.eu/document/download/b654235c-f5f1-452d-8a8c-367603af841_en

European Commission. (2024). *A safer & fairer online environment.* https://digital-strategy.ec.europa.eu/de/factpages/safer-fairer-online-environment

European Commission. (2024). *European Digital Media Observatory.* 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.* https://data.europa.eu/doi/10.2775/87640

European Commission Joint Research Center. (2023). *Hybrid threats: A comprehensive resilience ecosystem.* https://data.europa.eu/doi/10.2760/37899

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

European External Action Service. (2024, January 23). *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, March 19). *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. (n.d.). https://efcsn.com

European Parliament. (2025, January 23). *MEPs condemn Russia's use of disinformation to justify the war in Ukraine.* https://www.europarl.europa.eu/news/de/press-room/20250116IPR26330

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

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

FIMI-ISAC. (n.d.). *Foreign Information Manipulation and Interference – Information Sharing and Analysis Center.* 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, August 10). *Coordinated loss of trust.* https://cemas.io/blog/desinformation-demokratiegefaehrdung/

Google. (n.d.). *Prebunking is a technique to prevent manipulation on the Internet.* https://prebunking.withgoogle.com

Government of Canada. (2024, January 18). *The framework to counter foreign state information manipulation.* https://www.international.gc.ca/transparency-transparence/rapid-response-mechanism-mecanisme-reponse-rapide/manipulation.aspx

Cabinet of Ministers, Republic of Latvia. (2023, March 20). *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, March 29). *Chronology of radicalization: How Telegram became the most important platform for conspiracy ideologies and right-wing extremism.* https://cemas.io/publikationen/telegram-chronologie-einer-radikalisierung

Humprecht, E., Esser, F., & Van Aelst, P. (2020, January). *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 suggestions for an effective strategy to deal with information manipulation.* https://isdgermany.org/25-vorschlaege-fuer-eine-effektive-strategie-zum-umgang-mit-informationsmanipulation

Isdatechtzo.nl. (n.d.). https://www.isdatechtzo.nl

Keller, C. I., Freihse, C., & Berger, C. (2024). *State measures against disinformation.* https://doi.org/10.11586/2024065

Lamberty, P. (2024). *Anniversary of the Russian war of aggression on Ukraine: Belief in propaganda and conspiracy narratives.* https://cemas.io/blog/prorussische-verschwoerungserzaehlungen/

Lamberty, P., & Frühwirth, L. (2023). *Information manipulation as a complex challenge: Integrative model for dealing with disinformation.* https://cemas.io/publikationen/integratives-modell-desinformation/

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

Nakashima, E. (2019, February 27). *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. (n.d.). *2.5 What happened: Public information and communication (Main report).* https://www.covid19lessons.royalcommission.nz/reports-lessons-learned/main-report/part-two/2-5-what-happened-pbulic-information-and-communication/

OASIS Cyber Threat Intelligence Technical Committee. (n.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.* 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, No. 30). https://doi.org/10.1787/6d141b44-en

OECD. (2024). *Facts not fakes: Tackling disinformation, strengthening information integrity.* https://doi.org/10.1787/d909ff7a-en

OpenAI. (2024, May 30). *Disrupting deceptive uses of AI by covert influence operations.* Archived 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, January). *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 defense: 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/pdfjs/?file=/publications/download/Defining-Capabilities-DIGITAL.pdf

Pamment, J. (2024). *Psychological defense: Concepts and principles for the 2020s.* Psychological Defense Agency. https://mpf.se/psychological-defence-agency/publications/archive/2024-10-28-psychological-defence-concepts-and-principles-for-the-2020s

PersVeilig. (2019, October). *Press safety protocol.* https://persveilig.nl/_assets/f/285119/x/1c6e153d94/050923_persveilig-protocol-a4-eng.pdf

Professional Head of Intelligence Assessment (PHIA). (2019, January). *Professional development framework for all-source intelligence assessment.*

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

Psychological Defense Agency. (n.d.). *Get the tools!* https://bliintelurad.se/en

Psychological Defense Research Institute. (n.d.). *Leading research in psychological defense.* 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, November 29). *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). *The Business Council for Democracy.* Info package: https://www.bc4d.org

Smirnova, J. (2024, October 29). *SDA documents: Insights into Russia's digital disinformation strategy.* https://cemas.io/blog/sda-dokumente-russlands-desinformationsstrategie/

Tagesschau.de. (n.d.). *ARD fact finder.* https://www.tagesschau.de/faktenfinder

Vilmer, J.-B. J. (2021, July). *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, June 15). *Russkij mir.* bpb.de. https://www.bpb.de/themen/europa/russland/522375/russkij-mir/

Ziemer, C.-T. (2023, April 17). *Psychological interventions against disinformation.* https://cemas.io/blog/psychologische-intervention/

Editorial office:
Julia Smirnova
Simone Rafael
Jessa Mellea

Contact:
info@cemas.io

August 14, 2025

Information according to § 5 TMG
CeMAS - Center for Monitoring,
Analysis and Strategy gGmbH
Lietzenburger Str. 107, D-10707 Berlin

CeMAS, the Center for Monitoring, Analysis and Strategy, brings together interdisciplinary expertise on conspiracy ideologies, disinformation, anti-Semitism and the far right.

Commercial register: HRB 226823 B
Register court: Berlin
VAT ID number: DE 340877977

Represented by:
Josef Holnburger and Gregor Bauer

Editorial responsibility:
Josef Holnburger