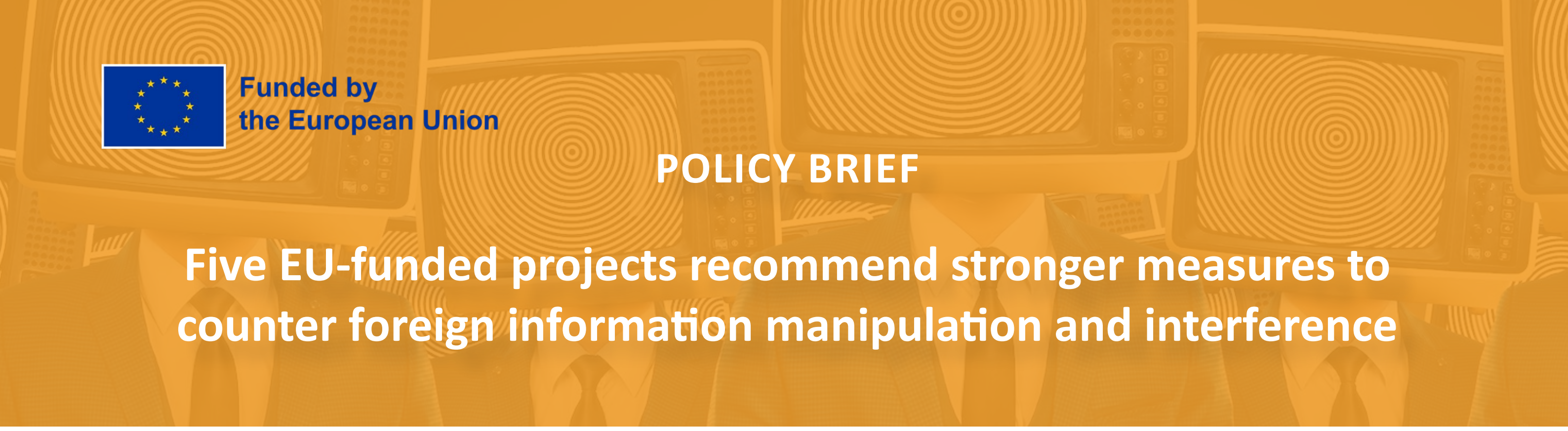


Funded by the European Union

POLICY BRIEF

Five EU-funded projects recommend stronger measures to counter foreign information manipulation and interference

Introduction

Foreign information manipulation and interference (FIMI) is a form of disinformation, with the emphasis on “foreign”. Some actors, e.g., fossil fuel companies, purvey disinformation too, which may be domestic information manipulation and interference (DIMI). Both types of disinformation are the scourge of our times, widely regarded as one of the most severe risks to democratic processes.[1]

This policy brief contains 10 recommendations for countering FIMI, especially inspired by Russia, which, in addition to its brutal war of aggression against Ukraine, is “escalating hybrid attacks, waging a battle of influence against Europe. The tactics used are reaching deep into the fabric of our societies, … they try to erode trust in democratic systems.”[2] As one response, the EC has said it would create a European Centre for Democratic Resilience to help the Union and Member States withstand these attacks that go beyond Ukraine.

As another response, five EU-funded projects[3] have joined forces to produce the 10 key recommendations to policymakers for countering FIMI[4] activities in Europe. They believe recommendations from five[5] projects will collectively carry more weight than just one project.

The coordinators of the five projects asked their partners to suggest one recommendation each based on their contribution to their project. The coordinators assembled these recommendations and analysed which appeared most frequently and/or which advanced the state of the art. They are sending this policy brief to policymakers and legislators at the EU and Member State levels and to urge adoption of the recommendations.

[1] World Economic Forum, 2024.

[2] European Commission and the High Representative of the Union for Foreign Affairs and Security Policy, ‘European Democracy Shield: Empowering Strong and Resilient Democracies’, 12 Nov 2025. https://commission.europa.eu/document/download/2539eb53-9485-4199-bfdc-97166893ff45_en?filename=JUST_template_comingsoon_standard_1.pdf

[3] The five projects are ATHENA (https://project-athena.eu/), EU-HYBNET (https://euhybnet.eu/), FERMI (https://fermi-project.eu/), SAUFEX (https://saufex.eu/) and VIGILANT (https://vigilantproject.eu/), two of which are ongoing while three finished earlier this year.

[4] The EC’s European Democracy Shield communication of 12 Nov 2025 defines FIMI as “a pattern of behaviour that threatens or has the potential to negatively impact values, procedures and political processes. Such activity is manipulative in character, conducted in an intentional and coordinated manner. Actors of such activity can be state or non-state actors, including their proxies inside and outside of their own territory.” https://commission.europa.eu/document/2539eb53-9485-4199-bfdc-97166893ff45_en

[5] ATHENA has 15 partners from 10 countries. EU-HYBNET had 25 partners from 13 countries. FERMI had 18 partners from 11 countries. SAUFEX has six partners from five countries. VIGILANT had 17 partners from 12 countries.

The 10 recommendations are as follows.

1. Member States should criminalise foreign interference activities, while still preserving freedom of speech.
2. Strengthen the EU's proactive response to FIMI through the European Centre for Democratic Resilience.
3. Strengthen cross-border information sharing and early warning.
4. Democratise and decentralise counter-FIMI decision-making processes.
5. Provide structured, role-specific training on countermeasures led by intelligence agencies.
6. National and EU authorities should enforce DSA requirements on platforms and search engines.
7. Develop technologies to expose deepfakes and other synthetic media in FIMI narratives.
8. Investigate who is funding FIMI, its main spreading channels and which societal groups are vulnerable.
9. Promote shared principles and interoperable frameworks across the EU.
10. Counter the loss of trust by protecting high quality journalism and independent media.

More detail

The following paragraphs provide more detail about each of the recommendations.

1. Member States should criminalise foreign interference activities.

FIMI activities are a threat to European and national security. Russia, China and other countries are actively engaged in undermining democracy and the security of Europe. Foreign interference is part of Putin's campaign of espionage, sabotage and assassinations[6] in Europe. Member States should adopt or expand laws criminalising FIMI activities. The UK offers a model. The UK's National Security Act 2023 sections 13 - 14 criminalises foreign interference, including "affecting the exercise by any person of their public functions… interfering with whether, or how, any person… participates in relevant political processes… or prejudicing the safety or interests of the United Kingdom". Prohibited conduct under the Act section 15 includes "misrepresentation that a reasonable person would consider to be false or misleading in a way material to the interference effect". The penalty includes a maximum term of 14 years and/or a fine.

2. Strengthen the EU's proactive response to FIMI through the European Centre for Democratic Resilience

On 12 November 2025, the EC announced that it will "set up a new European Centre for Democratic Resilience to withstand evolving common threats, such as disinformation and foreign interference in elections". While this initiative is welcome, a purely defensive or resilience-based approach is insufficient given the scale, persistence, and increasing sophistication of FIMI attacks targeting the EU.

[6] Such as Alexander Litvinenko or the attempted assassination of Sergei Skripal in the UK, former Chechen commander Zelimkhan Khangoshvili in Berlin, Russian helicopter pilot and defector Maxim Kuzminov in Spain, Bulgarian arms dealer Emilian Gebrev, etc.

Europe should not merely "withstand" threats. It should adopt a much more proactive, anticipatory, and deterrence-oriented approach towards FIMI actors, especially Russia, which accounts for the vast majority of FIMI attacks in Europe, as the European External Action Service (EEAS) has stated in its FIMI reports.[7] The EC should equip the Centre with monitoring, early-warning, and whistle-blower functions, especially during elections. It should extend partnerships to candidate countries to strengthen collective awareness of foreign influence operations. The EC should prioritise the deployment of countermeasures and resources against specific, dangerous narratives.

To be effective, the European Centre for Democratic Resilience should be equipped with operationally meaningful financial and operational resources, including:

- reliable, predictable and adequate funding streams;
- advanced monitoring and early warning functions, enabling the timely detection of emerging FIMI campaigns, especially in pre-election and election periods;
- secure whistle-blower and reporting mechanisms, allowing journalists, researchers, civil society actors, and platform employees to report suspected coordinated influence operations safely;
- analytical capacity to identify, prioritise, and attribute high-risk narratives, enabling EU institutions and Member States to focus resources on the most harmful and strategically significant threats.

The Centre should also play a stronger role in external cooperation, extending structured partnerships to EU candidate countries and neighbouring states. Recently, Moldova was subject to large-scale Russian disinformation efforts in the run-up to its parliamentary elections, which included mimicking actual websites and news sources to spread falsehoods aimed at driving a wedge between Moldova and Europe. Closer cooperation in situations like this would enhance collective situational awareness, reduce vulnerabilities in the EU's immediate neighbourhood, and help prevent influence operations from being tested or refined in less-protected information environments before being deployed within the Union.

We recommend that the EC:

- Adopt a more assertive and coordinated posture towards state and state-aligned actors engaged in systematic FIMI activities, moving beyond reactive measures to include anticipatory disruption and deterrence where legally and politically feasible.
- Mandate the Centre to support the prioritisation and deployment of countermeasures against specific, high-impact narratives and campaigns.
- Ensure close integration between the Centre, the European External Action Service (EEAS), national authorities, and trusted non-governmental partners, enabling rapid information sharing and coordinated responses during critical periods such as elections.

[7] In its first FIMI report in 2023, the EEAS said of 100 FIMI incidents it tracked, 88 came from Russia. https://www.eeas.europa.eu/eeas/1st-eeas-report-foreign-information-manipulation-and-interference-threats_en. EUvsDisinfo describes Russia as "the world's largest disinformation spreader". https://euvsdisinfo.eu/5-insidious-disinfo-narratives-spread-by-the-kremlin/. EUvsDisinfo, part of the European External Action Service's East StratCom Task Force, was created in 2015 to track, analyse, and debunk pro-Kremlin disinformation.

- Regularly assess the effectiveness of existing EU measures against FIMI, adapting tools, resources, and mandates in response to evolving threat actor behaviour.

3. Strengthen cross-border information sharing and early warning

FIMI involves highly coordinated and increasingly sophisticated actions operating seamlessly across borders. Effective countermeasures require equally coordinated, transnational responses, highlighting the importance of strengthening cooperation among stakeholders engaged in detecting and combating FIMI. Such cooperation should be underpinned by better access to, and harmonisation of, cross-border datasets as mandated by Art. 40 of the Digital Services Act (DSA), alongside the development of a common terminology and shared analytical criteria. This will improve interoperability and foster a more unified understanding of FIMI. Timely detection and joint analysis of emerging narratives are critical to prevent large-scale societal impacts.

Disinformation distortions and fabrications are part of a FIMI campaign and can travel by many different routes, reach many different audiences and generate many different effects in different contexts. Given the multifaceted, shapeshifting nature of disinformation, the EU and Member States should have a system and strategy in place that enables collaboration between different partners, from government authorities to non-governmental organisations (NGOs) as well as law enforcement authorities (LEAs). Collaborative sharing of trend analysis, forecasting, foresighting and information will improve detection and flagging of disinformation campaigns and actors.

We recommend that the EU

- Establish a rapid response coordination mechanism at EU level (which could be the EC's proposed European Centre for Democratic Resilience[8]), to facilitate immediate cross-border collaboration, especially, but not only, when disinformation campaigns show links to organised crime or terrorism.

- Strengthen collaboration among LEAs by implementing secure channels for sharing critical data, situational reports, and best practices related to disinformation and its links to criminal activity. This will foster a coordinated response and mutual understanding of challenges.

- Promote cooperation between LEAs and online platforms, including those outside the EU, where LEAs flag illegal content in line with the DSA and the platforms take timely and appropriate action to address illegal content and mitigate related harms.

- Draw together the results of all relevant EU-funded projects from the past years (maybe as a new Call for Proposals, if no other solution can be identified). There are a plenty of solutions, but they are very fragmented in terms of LEAs that can use them, platform focus, country focus, technologies. We recommend the joint development of two technical solutions post-project (a key platform and a backup version) that combine the features that are tailored to all crucial end-users (including media outlets, CSOs, and government agencies) and were evaluated particularly positively.

[8] https://ec.europa.eu/commission/presscorner/api/files/document/print/en/ip_25_2660/IP_25_2660_EN.pdf

4. Democratise and decentralise counter-FIMI decision-making

The responsiveness of legislators and policymakers is key to foster societal resilience, understood as protecting and empowering civilians' basic needs as well as democratic institutions and procedures. To enhance responsiveness, we recommend democratising and decentralising FIMI decision-making processes to include non-governmental entities in deliberations regarding countermeasures. Societal input needs to be integrated into the processes on two complementary levels: "fact-speaking", which incorporates evidence-based contributions from experts, data, and scientific analysis, and "belief-speaking", which recognises the public's values, identities, concerns, and moral intuitions.[9] Effective democratic decision-making requires acknowledging both what is true (facts) and what matters to people (beliefs), because policies grounded solely in evidence may lack legitimacy, while those based only on values may lack accuracy or effectiveness. Integrating both forms of input ensures decisions that are informed, trusted, and socially sustainable.

We recommend that the EU:

- Support multi-level participation institutions (e.g., "Resilience Councils") that integrate academic institutions, civil society organisations (CSOs), and companies into detection, analysis and response processes based on proof ("fact-speaking"), building on emerging models such as those piloted in Poland.
- Establish structured channels for public participation, enabling the public to contribute to agenda-setting, oversight, and evaluation of FIMI responses based on critical reflection and democratic deliberation, informed by a balanced assessment of the societal discourse ("belief-speaking").
- Promote public engagement through education and skill-building, including media literacies, communication skills, and critical thinking capacities, informed by principles tested by the SAUFEX project (e.g., those from Interdemocracy[10] and Wisdom of Crowds[11]).
- Raise awareness of existing tools to which the public can have access to flag suspected FIMI activity and, if necessary, provide accessible plug-and-play tools.
- Ensure sustainable mixed funding models (EU start-up grants, complemented by local and private co-funding) to expand institutional responsiveness and maintain long-term societal involvement.

5. Provide structured, role-specific training on countermeasures led by intelligence agencies.

A thorough understanding of how humans produce, amplify or respond to manipulative information is essential for an effective societal response to FIMI. While FIMI threats are primarily detected and analysed by the intelligence community, countering their effects requires a multi-level, multi-actor response involving law enforcement agencies, CSOs, NGOs, fact-checkers, and platform providers. We also need to understand how FIMI actors exploit the Internet for their malign purposes through algorithmic amplification, i.e., how algorithms through virality exploit human behaviour.

[9] Lewandowsky, Stephan, et al., "The Debunking Handbook", University of Bristol, 2020. doi: 10.17910/b7.1182

[10] Hansen-Staszyński, Onno, Beata Staszyńska-Hansen and Tomasz Chłoń, Project SAUFEX on "societal resilience" and "whole-of-society approach": proposition for a citizen-oriented strategy as an integral part of the post-peace European defence strategy, SAUFEX, 2025. https://saufex.eu/

[11] Surowiecki, James, The Wisdom of Crowds: Why the Many Are Smarter Than the Few, Doubleday, New York, 2005.

Intelligence agencies and other qualified national authorities possess the expertise, threat awareness, and operational experience necessary to identify and respond to FIMI. Where legally permissible, these bodies should play a leading role in providing structured, role-appropriate training to other stakeholders. This would help build shared situational awareness and strengthen response capabilities across society, while respecting institutional mandates and legal constraints.

Training on appropriate countermeasures provided by intelligence agencies will enable LEAs, CSOs, fact-checkers (including members of the European Fact-Checking Standards Network, EFCSN), and relevant platform teams to operate more effectively within their respective roles, and should cover:

- Threat typologies, channels, and content patterns associated with FIMI campaigns, tailored to the operational needs and legal remit of each audience;
- Practical guidance on technological tools for monitoring, analysis, and reporting, including clear frameworks on which tools are suitable for specific use cases to avoid fragmentation and inefficiency;
- Data access and data-sharing requirements, which are critical for effective monitoring and analysis. The establishment of a European information-sharing framework, comparable in function to the American Universal Crime Reporting Program, should be explored. Social media platform providers should be required to make relevant disinformation datasets available in a comprehensive, standardised, and interoperable form;
- Appropriate intervention and escalation mechanisms, enabling trained actors to prevent or mitigate harm while operating in compliance with national and EU-level legal and regulatory frameworks.

The European Commission should support and incentivise these training efforts by promoting structured cooperation between intelligence agencies, LEAs, a diverse set of CSOs, fact-checkers from across the political spectrum, and online platforms, including those headquartered outside the EU. This cooperation should focus on capacity-building, information exchange, and coordinated response, contributing to the timely identification, mitigation, and – where appropriate – removal of harmful and illegal content.

6. National and EU authorities should enforce DSA requirements on platforms and search engines.

Platforms must detect and disrupt coordinated disinformation campaigns, as required by law, without undermining freedom of expression, while regulations must balance accountability and innovation through harmonised, enforceable AI governance frameworks that prioritise democratic resilience over unchecked technological advancement.

Platforms should adopt privacy-by-design and telemetry systems that enable real-time detection of FIMI risks, e.g., disinformation amplification, emotional escalation, and radicalisation cues, in AI-generated or AI-amplified content. As a voluntary compliance accelerator under DSA Articles 34 and 35, these systems would allow platforms to generate anonymised, regulator-approved risk indicators – such as hashed trigger signatures and aggregated trends – without transmitting raw user data.

Very large online platforms (VLOPs) should vigorously implement the DSA provisions that enable civil society and researchers to access near-real-time platform data, especially in view of scepticism about their intentions. Attempts to evade or impede the implementation of European legislation must be resisted.

Social media data, even if available, vary greatly across platforms, which presents profound technical challenges. The development and availability of standardised high-quality multilingual social media datasets that include coherent information such as timestamps, engagement metrics, identifiers linking content across platforms etc. must be supported, as mandated by Art. 40 of the DSA.

Generative AI systems should fall under the DSA. Generative AI systems, including large language models (LLMs) and diffusion models, significantly amplify the risks of disinformation and FIMI by enabling the mass production of realistic, persuasive content at low cost, micro-targeted to specific groups. Systems are vulnerable to training data contamination, covert or deceptive alignment, and adversarial manipulation, which can embed lasting biases and distortions into their outputs. To mitigate these threats, EU policy should mandate rigorous provenance tracking and auditing of training data, transparent model alignment of declarations, standardised stress-testing against adversarial influence, and embedding of digital provenance markers in AI-generated content.

Platform accountability is essential to reduce adversarial manipulation. We recommend that the EC and Member States:

- Introduce public authenticity indicators (e.g., credibility scores, verification levels, bot probability ratings).
- Mandate transparency APIs providing real-time authenticity metrics to users and communities.
- Combine tools with grassroots media literacy programmes, open-source detection platforms, and systematic exposure of adversary tactics.
- Provide ways for research and auditing by making available real-world and large-scale data for research purposes in countering FIMI and periodic reports of identified content and campaigns.

The DSA should be amended to automatically allow companies, research centres and universities access to social media data for the conduct of publicly funded research (e.g., by consortia funded under Horizon Europe).

7. Develop technologies to expose deepfakes and other synthetic media.

As deepfake videos become more realistic and emotionally compelling, they are increasingly weaponised in sophisticated FIMI operations.[12] Their audiovisual nature makes them especially potent. Unlike text-based disinformation, deepfakes can simulate trusted figures with convincing gestures, voice patterns, and visual authenticity, undermining public trust and manipulating perception at scale. To counter this threat, we recommend investing in robust, explainable, multimodal, AI-based detection technologies that integrate both visual and audio analysis. Such technologies should fulfil the following strategic criteria:

[12] A parallel threat occurs when bad actors claim that real videos are deepfakes or modify real videos to make them fail deepfake analysis.

- Multimodal capability: Combine visual, auditory, and temporal signals – such as facial movements, lip-sync accuracy, audio spectrum consistency, and timing discrepancies – to detect tampered content more reliably than unimodal systems.

- Explainability: Ensure that the technologies provide interpretable outputs (e.g., visual heatmaps, anomaly scoring, synchronisation metrics) to support human analysts, reinforce transparency, and enhance trust in automated detections.

- Resilience to manipulation: Train technologies to remain effective under real-world conditions, including compression, noise, re-encoding, and adversarial alterations often used to bypass detectors.

- Generalisation across contexts: Design technologies to detect a wide range of manipulations, including emerging deepfake techniques, by leveraging transfer learning and adaptive training approaches.

Such technologies will contribute to early detection and attribution, curbing the spread and persuasive power of falsified audiovisual material.

Although deepfakes can be more engaging than text-only messages, the latter is faster and easier to create with current Generative AI models. For instance, personalised messages to specific audiences can be created with high fluency and at scale, with the potential for being weaponised by FIMI campaigns. Investing in robust and explainable models for detecting and analysing AI-generated disinformation is, therefore, paramount to early detection of FIMI campaigns. In addition, FIMI campaigns may follow or spread specific narratives to enable engagement, mimic reliability and foster trust from citizens. Therefore, AI-based models that can analyse narratives from text, audio, image and videos are also important to counter FIMI disinformation. Such models should follow the same principle as for deepfakes.

As creating fake content has become very easy and often indistinguishable from reality, a systematic solution against disinformation through synthetic media is to strengthen the trustworthiness of authentic content at the point of capture. The EU should explore supporting and incentivising the adoption of proactive camera authentication systems that embed secure cryptographic signatures into photos and videos as they are recorded. If workable, this would allow users, journalists, and researchers to verify whether a piece of media is original or has been tampered with. An "authenticity by design" approach could provide a robust complement to forensic detection and increase resilience against FIMI campaigns. The EU should also mandate the VLOPs to do whatever is in their power to prevent deepfakes, AI-generated and known FIMI narratives from being spread on their platforms.

8. Investigate who is funding FIMI, its main spreading channels and which societal groups are vulnerable.

European and national financial institutions, intelligence agencies, LEAs, VLOPS and banks should work together to disrupt funding of FIMI campaigns. They should aim to disrupt and seize the financial transactions, including in cryptocurrencies, that fund FIMI campaigns. A focus on the financial dimension of FIMI is needed not only to expose hidden interests but also to foster accountability. Examples of such financial transactions include Russia's purchase of adverts on social media platforms without disclosing their origins.[13] Russia has recruited influence-for-hire firms to spread their FIMI.[14] It has paid for interviews with lawmakers in the European Parliament.[15] It has used shell companies and opaque NGOs to fund local organisations and events to produce and disseminate false videos.[16]

We recommend:

- Coordinated efforts by authorities to disrupt FIMI funding using the same model used to disrupt terrorist financing (dissuasive fines, sanctioned and removal of banking and other financial licences).
- Researchers should investigate the financial underpinnings of each FIMI case and assess whether existing policies or applicable local laws could be leveraged to limit or increase transparency around the financial flows.

In addition, FIMI's main spreading channels should be identified and analysed by researchers in order to understand its dynamics, creation and posting patterns. Once such channels are identified, VLOPs should act immediately to disrupt their activities in order to prevent further engagement. This can only be done via a coordinated effort of researchers, policymakers and VLOPs, which can be materialised through EU-funded projects.

Finally, identifying the most vulnerable societal groups is also paramount to understand FIMI's reach, propose counter campaigns and increase resilience in society. Research should focus on understanding the dynamics of FIMI and, given a potential event with high likelihood of interference (e.g., elections), identify groups that are most likely to be affected. Similarly to identifying spreading channels, joint effort is needed, involving multiple actors.

9. Promote shared principles and interoperable frameworks across the EU.

The EU should promote shared principles, interoperable frameworks, and adaptive guidelines to support independent researchers and practitioners from across the political spectrum monitoring social media for illegal and/or harmful content linked to FIMI. The objective is to foster coherence and comparability across Member States while preserving the flexibility and innovation needed to respond to a rapidly evolving threat landscape.

Such guidance should aim to:

- support the effectiveness of social media monitoring in investigations of FIMI activities;
- ensure compliance with a common ethical, legal, and fundamental rights frameworks;
- allow methodological experimentation and the rapid integration of new tools and approaches.

[13] Cooney, Dan, 'A Russian Propaganda Group Purchased Ads on Facebook during the 2016 Election. Here's What That Means.', PBS News, 9 Sept 2017.

[14] Antoniuk, Daryna, 'Russian 'Influence-for-Hire' Firms Spread Propaganda in Latin America: US State Department', The Record, 8 Nov 2023.

[15] See Ch. 4.16 in Wright, David (ed.), Foreign Information Manipulation and Interference: Case Studies from the ATHENA project, Springer, Nov 2025.

[16] Becket, Stefan, and Melissa Quinn, 'U.S. Says Russia Funded Media Company That Paid Right-Wing Influencers Millions for Videos', CBS News, 5 Sept 2024.

Implementation of these principles and frameworks will benefit from collaboration between academia, policymakers, intelligence agencies, law enforcement authorities, CSOs, technical experts, and should be reflected in training and capacity-building activities for the LEA community.

Member States currently differ significantly in how EU-developed counter-FIMI tools and frameworks (e.g., DISARM, STIX, OpenCTI, ABCDE) are adopted, interpreted, and operationalised. To improve interoperability and shared situational awareness, the EU should:

- Support EU-funded, recurring capacity-building programmes on countering FIMI for governmental and non-governmental actors, offering modular learning paths that can be updated as threats evolve;
- Promote a shared, extensible terminology and taxonomy for describing FIMI incidents and responses, e.g., building on the DISARM Framework while allowing national or sector-specific extensions[17];
- Develop and maintain living good-practice manuals and response playbooks, validated across sectors, regularly updated, and aligned with EEAS methodologies, rather than fixed procedural standards;
- Facilitate the voluntary uptake of interoperable tools, for example, through the distribution of an OpenCTI starter pack including reference TTPs, example datasets, and reporting templates, designed to enhance data sharing and situational awareness while allowing local adaptation.
- Ensure concrete synergies with NATO's approach to disinformation in terms of procedures, because at national/governmental level in EU Member States, experts (especially MoDs and MFAs) should follow both NATO and EU guidance which might be confusing, repetitive, and time-consuming sometimes. NATO has a new exploratory concept now called NATO cognitive warfare which essentially places FIMI in a warfare-like environment. The threat is the same, but the instrumentalisation is different so this would be an area for congruence of concepts and procedures.

10. Counter the loss of trust by protecting high quality journalism and independent media.

Democratic states in Europe take pride in their pluralistic societies and the protection of fundamental rights such as freedom of expression. Yet these democratic principles also create openings for FIMI campaigns. A central challenge is to neutralise the harmful impacts of FIMI attacks while safeguarding the core achievements of democratic societies. We recommend an intervention that reinforces a key democratic asset: the protection and strengthening of high-quality, independent journalism and media.

High-quality media are those outlets that strive to produce work situated at the higher rungs of Erdmans' ladder.[18] This ladder ranges from statements to facts, to data, to evidence, and ultimately to proof. Facts are accurate statements about reality. Data consist of representative facts that are not selectively chosen. Evidence is data that are sufficiently conclusive to rule out alternative interpretations. Proof represents universal evidence: information that holds across all relevant contexts.

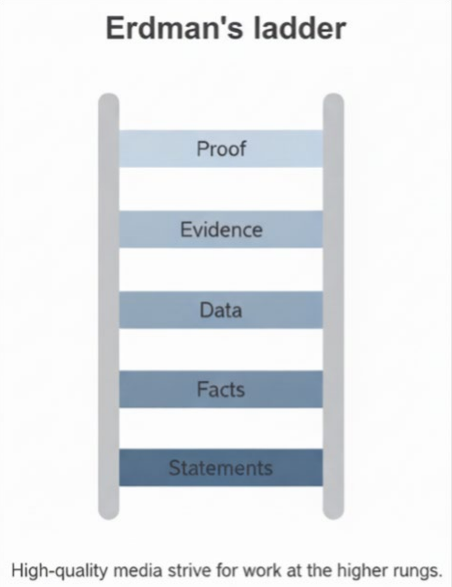
There is a well-established correlation between a robust media sector and the overall health of democratic societies. The erosion of trust in independent, professional and high-quality journalism has become a major

[17] See the structure for case studies adopted in the ATHENA project. Wright, David (ed.), Foreign Information Manipulation and Interference: Case studies from the ATHENA project, Springer Nature, Cham, Switzerland, 2025.

[18] Erdmans, Alex, May Contain Lies: How stories, statistics and studies exploit our biases - and what we can do about it, Penguin Random House, 2024.

driver of disinformation and FIMI. The decline in high-quality media is closely tied to the disruptive impact of social media, which has undermined traditional funding models based on advertising and print sales, particularly for local outlets. As revenues have collapsed, news organisations have drastically reduced their newsrooms, diminishing the quality, breadth and depth of their reporting, and in many cases forcing outlets to close altogether.

The European Media Freedom Act takes steps to protect news media from excessive concentration, undue political influence and unfair content restrictions imposed by online platforms. Two core problems need to be addressed: the huge share of the online advertising market controlled by Google and Meta[19] (and the problem that relying on "clicks" incentivises low-quality "clickbait") and, separately, the problem that, unlike music, audiovisual and e-/audiobooks, there is no possibility of easily paying for access to multiple publications via a one-stop-shop.



High-quality media strive for work at the higher rungs.

Canada and Australia provide examples of how high-quality journalism can be protected. Canada has implemented a comprehensive set of interventions to strengthen high-quality journalism, including the Journalism Labour Tax Credit, which offsets 25 per cent of newsroom salary costs; a Digital News Subscription Tax Credit that encourages the public to pay for trusted news; and the Local Journalism Initiative, which directly funds reporters in underserved communities. In addition, Canada's Online News Act requires major digital platforms to compensate news organisations for the use of their content, helping correct market imbalances and sustain professional reporting.

Australia has also taken strong steps to protect public-interest journalism, most notably through the News Media Bargaining Code, which compels Google and Meta to pay news publishers and has channelled substantial new funding into newsrooms. The government also supports regional and local news through programmes such as the Public Interest News Gathering (PING) fund and has long maintained stable public financing for the ABC and SBS networks to ensure wide access to independent reporting. Additional initiatives, such as the Regional and Small Publishers Innovation Fund, help smaller outlets adapt to digital disruption, collectively demonstrating a proactive national strategy to sustain high-quality journalism and democratic resilience.

In view of the above, we recommend:

- increased national funding (e.g., via licence fees) for local and national newspapers and other media whilst ensuring their independence and unbiased reporting;
- requiring VLOPs to pay for news content they harvest from news websites (as they are now required to do in Australia and Canada);
- protecting high quality independent media from SLAPP lawsuits and other legal means of silencing them.

[19] See https://peoplevsbig.tech/breaking-free-from-the-advertising-duopoly/

For more information about the five projects, see:

ATHENA: david.wright@trilateralresearch.com

EU HYBNET: paivi.mattila@turkuamk.fi

FERMI: sven-eric.fikenscher@pol.hfoed.bayern.de

SAUFEX: tomasz.chlon@port.lukasiewicz.gov.pl

VIGILANT: brendan.spillane@ucd.ie

Funded by
the European Union