Funded by the European Union

POLICY BRIEF

Shields Up: Recommendations to Strengthen the European Centre for Democratic Resilience's Response to FIMI

by Pedro Peres Cavalcante and Ian Slesinger, Trilateral Research

April 2026

Introduction

Foreign Information Manipulation and Interference (FIMI) has emerged as one of the most pressing threats to democratic stability in the European Union. Through targeted disinformation, influence operations, and technologically enhanced manipulation tactics, authoritarian regimes and hostile actors aim to erode public trust, polarise societies, distort electoral competition, and weaken the foundations of EU democracy. Effectively countering FIMI is not merely a security priority — it is essential to safeguarding democratic institutions, electoral integrity, independent media, and an informed and engaged citizenry.

The new European Centre for Democratic Resilience (ECDR) is to be a centrepiece in the new strategic pack of measures recently announced by the European Commission and the High Representative. Indeed, the Joint Communication on the European Democracy Shield explicitly identifies the Centre as a dedicated operational hub to anticipate, detect and respond to FIMI and disinformation, tasked with developing an EU Blueprint to counter FIMI and tools to protect the integrity of electoral processes across Member States. As a central hub that relies on the voluntary participation of Member States, it is important that the Centre begins its work by prioritising measures set to ensure the engagement of national public stakeholders and strengthen their individual capacity to combat threats against democracy.

This policy brief outlines how FIMI-specific findings and recommendations from the Horizon Europe ATHENA Project, and other European-funded research, can support the European Commission's new European Democracy Shield (EDS) initiative to reinforce democratic resilience across the EU. It also provides recommendations to maximise impact across EU institutions, Member States, civil society and digital ecosystems.

Recommendations

1. Capacity building at the national level

As FIMI and disinformation contents become increasingly localised and personalised, attention must be paid to the specific local contexts in which FIMI and disinformation are targeted and consumed, including the social, cultural and linguistic dimensions in which they manifest.

The Democracy Shield already explicitly recognises the relevance of linguistic and cultural diversity in its provisions on public financing of public service media and, indirectly, through support for media pluralism. As actors working in the forefront against FIMI and disinformation, national and local actors of each Member State must be well-equipped to anticipate and detect threats in their own languages and local contexts across Europe.

To facilitate this, **we recommend that the Centre**:

- **Prioritises capacity building at the Member State level through training for state agencies and civil society actors working to combat FIMI and disinformation.**

  To support the Centre's goal to increase responsiveness to FIMI and disinformation throughout Europe, the Centre should develop and deploy training activities to ensure public entities stay on track with the latest developments in technology and FIMI and disinformation trends. As revealed by the ATHENA mini-Delphi study on the impact of emerging technologies to FIMI and disinformation, staying on top with the latest technological advancements is key for the skillset of professionals working in the anticipation, detection and analysis of these threats.

- **Leverages research findings and innovation developed in EU projects on FIMI and disinformation.**

  As a coordination and cooperation platform, the ECDR will benefit from continuously mapping research insights, methodological innovations and technological tools from EU-funded research that can be incorporated across Member States to increase democratic resilience. ATHENA, vera.ai and FERMI are some examples of relevant Horizon projects.

  The Centre should proactively evaluate barriers to uptake for these technological tools in Member States and take steps to mitigate them. The ECDR can also play a role in allocating funding for research and innovation and technology acceleration for enabling democratic resilience – including tools for detecting and countering FIMI. The ECDR should also scale-up existing and new tools from HORIZON projects for usability, accessibility and integration, serving as a platform for distributing these tools and training local actors to use them effectively.

ATHENA Tech Tools

The ATHENA project is developing a data collection platform and data set (of more than 500 channels carrying FIMI), a FIMI toolbox of at least five tools for use in combating disinformation; and a dashboard showing users how to navigate the data set and toolbox. Our upcoming platform for combating disinformation helps intelligence analysts by increasing their agility in uncovering FIMI operations and by providing a standardized resource to streamline threat recognition across Member States.

Our platform features:

- A dashboard with tools for filtering data and monitoring ongoing FIMI campaigns as they emerge;
- A FIMI toolbox with tools that can provide reliability scores for articles with probabilities for an image or video to be a deep fake;
- Network analysis + deepfake tools (currently under development).

2. Intelligence and best practices sharing

The Centre should facilitate a permanent and continuous exchange between the stakeholders who contribute to it. To fulfil its cooperative scope, the ECDR should foster a virtuous cycle of exchange of intelligence and best practice sharing.

We recommend that the Centre:

- **Introduce a mechanism for the collection of data gathered by relevant Member State agencies monitoring FIMI and disinformation.**

  Government agencies can submit their intelligence data and analysis performed at the local level to the Centre, so that FIMI techniques, incidents, patterns and trends can be monitored in near real-time. This allows stakeholders to identify new attacks, campaigns and methods as they emerge and trigger rapid and appropriate responses. Alongside the data and research from civil society and other non-government stakeholders collected via the Stakeholder Platform, the ECDR hub can identify cross-cutting patterns and themes in intelligence gathering and share analyses with Member States.

Case study: Russian FIMI campaign targeting the 2024 Romanian election

Romania's 2024 presidential election has become a key reference point for how Russian FIMI can distort an EU Member State's electoral process and trigger Union-level responses. The first electoral round produced an unexpected surge for ultranationalist candidate Călin Georgescu, whose visibility was driven by TikTok and Telegram rather than traditional campaigning.

Subsequent declassification of national security assessments by the Supreme Council for National Defence (CSAT) revealed coordinated hybrid activities attributed to Russia, including cyber operations against electoral IT systems and a large-scale online influence effort that used bots, fake or impersonated institutional accounts, and covertly financed TikTok promotion far beyond declared campaign spending.[1] Consequently, the Romanian Constitutional Court annulled the first round, explicitly linking its decision to foreign interference that had undermined the integrity of the vote. Romanian authorities thus played a central role: intelligence services detected and documented the operation; CSAT framed it as a national security threat; the president authorised exceptional declassification; and judicial authorities translated this into concrete constitutional remedies.

At EU level, the case has been used to illustrate Russia's broader "hybrid offensive" against European democracies and the specific risks arising from very large online platforms. The European Commission intensified its supervisory actions under the DSA (making data retention orders, for instance) and stepped up monitoring of TikTok's systemic risks, while the signatories of the then Code of Practice on Disinformation activated its Rapid Response mechanism.

The Romanian campaign shows that EU level tools rely heavily on timely inputs from local actors - security services, electoral bodies, courts, independent media and civil society - who are often the first to detect, document and publicly substantiate complex FIMI operations.

1 AGERPRES, "Declassified documents from CSAT/Romania – target of Russian hybrid actions, Georgescu's campaign – financed", AGERPRES, 4 Dec. 2024. https://agerpres.ro/2024/12/04/declassified-documents-from-csat-romania---target-of-russian-hybrid-actions-georgescu-s-campaign---f--1398576

- **Provide advisory services and resource sharing for identifying and gathering intelligence on FIMI and best practices for mitigating its proliferation and impact at the local scale within Member States.**

These advisory services should support state agencies, civil society organisations, journalists and press organisations, and potentially affected commercial organisations including online platforms. Advisory services can address a range of needs including how to select and use appropriate intelligence gathering, analysis and defence tools for FIMI monitoring and resilience; information sharing and awareness-raising based on real-time intelligence on risks created by FIMI activity, including appropriate mitigation strategies and techniques; and guidance on stakeholders' regulatory responsibilities relating to FIMI activities and sharing best practices to help organisations meet these requirements.

3. Deploying countermeasures

As FIMI operations grow in sophistication and scale, the EU must work to build an arsenal of effective and stress-tested countermeasures. The ECDR should play a pivotal role in supporting relevant agencies and state-run task forces from Member States in mapping and deploying countermeasures tailored to the specific nature and context of each FIMI manifestation. As research developed under the ATHENA project demonstrates, effectiveness depends not only on the appropriateness of the selected response, but equally on its timeliness — the institutional agility to act before influence operations achieve their intended effect.

We recommend that the upcoming Centre:

- **Curates a knowledge repository of countermeasures, case studies, methodologies and similar resources.**

  This knowledge repository can concentrate findings gathered from EU-funded projects about FIMI and disinformation such as ATHENA. While extensive research on the topic exists, these results are scattered in different spaces, which hinders the optimal use of its findings. Similar to a digital library, this resource can support Member States in easily accessing accumulated knowledge on FIMI manifestations throughout the EU, helping them identify countermeasures' effectiveness contextually.

- **Serves as the operational coordinator for crisis response.**

  In addition to developing a new, strengthened early warning system, the Centre can act as the EU's supervision body for any Digital Services Act (DSA) crisis response protocols related to FIMI and disinformation. ECDR can coordinate and advise stakeholders to ensure rapid, unified responses during high-risk periods such as elections or geopolitical crises.

Conclusion

Countering FIMI is essential for safeguarding European democracy. The EDS can provide the regulatory, operational, and civic instruments needed to respond to increasingly sophisticated influence campaigns, while the ECDR can ensure the EU maintains the capacity to coordinate, innovate, and anticipate emerging threats. The ECDR should prioritise capacity building across Member States by training state agencies and civil society actors. It should also scale and deploy technical tools that support detection and response, facilitate the continuous exchange of intelligence and best practices among stakeholders, maintain a repository of countermeasures, and coordinate the crisis response protocol. The results of the Horizon Europe ATHENA project are reinforcing this work by improving the detection, analysis, and response to FIMI across the EU through advanced tools, shared data frameworks, and tested methodologies. In doing so, ATHENA and related Horizon projects strengthen the early identification of manipulation campaigns, enable coordinated cross-border responses, and empower institutions and civil society — making FIMI mitigation a practical driver of long-term democratic resilience.

About ATHENA

The Horizon Europe ATHENA project aims to support European democracy by providing a research-led approach to understanding, detecting, analysing and countering FIMI.

It does this by evaluating real-world cases of FIMI to both assess the societal impact of FIMI and provide countermeasures. These multifaceted countermeasures include developing a disinformation analysis toolbox, alongside offering training and educational resources, raising public awareness and formulating evidence-based policy recommendations.

Prepared by

TRILATERAL RESEARCH
Ethical AI

www. project-athena.eu

Funded by the European Union

UK participants in Horizon Europe Project ATHENA are supported by UKRI Grant number 10107667 (Trilateral Research). Views and opinions expressed are, however, those of the authors only and do not necessarily reflect those of the European Union or European Research Executive Agency (REA) or UKRI. Neither the European Union nor the granting authority not UKRI can be held responsible for them. Grant Agreement 101132686 ATHENA HORIZON-CL2-2023-DEMOCRACY-01