

Securing Democratic Discourse: Election Integrity in an AI-Disinformation Era

Thursday 17 September 2026

Europa Experience David Sassoli · Piazza Venezia, Rome

Summary. On 17 September 2026 the FIMI Defenders for Election Integrity (FDEI) project concluded its mandate with a working session in Rome. This session was hosted by the European Parliament Liaison Office in Italy and organised by DEN Institute and Debunk.org on behalf of the consortium. Fifty participants took part, including thirteen diplomatic missions accredited in Rome and representatives of the European Commission, the European External Action Service, and the Italian Parliament. This brief summarises the project and its outcomes, the substance of the discussion, and the conclusions drawn. The first session was held under the Chatham House Rule.

Purpose and participation

The session was designed as a working meeting rather than a presentation. The consortium presented the results of two years of monitoring and asked those present what they could use. Holding the meeting in Rome meant that it was attended by people who do not usually attend events in Brussels.

Representatives from the European institutions included the Commission's Directorate-General for Communication at Deputy Director-General level, by the European External Action Service division responsible for information integrity and FIMI, and by the Director of the European Parliament Liaison Office in Italy. On the Italian side a Senate representative delivered an institutional address. Thirteen missions accredited in Rome sent nineteen representatives, which is unusual profile for the closing event of a civil society project. This suggests that foreign information manipulation is now being monitored by member state missions as a bilateral interest, and not just as a Brussels issue.

Reference context

In 2025 the European External Action Service documented and analysed 540 FIMI incidents worldwide, involving approximately 10,500 channels and around 43,000 pieces of content. 29% were attributed to Russia and six per cent to China and the remaining 65% were unattributed but showed indicators of coordination with Russian or Chinese infrastructures. AI-enabled tactics were used in 27% of the incidents, up from 41 cases in 2024 to 147 cases in 2025. Electoral processes were again a primary focus, with Russia targeting elections in Germany, Poland, Romania, Moldova, the Czech Republic and Côte d'Ivoire. Two features are relevant to what follows. Firstly, roughly two thirds of recorded activity cannot be assigned to a state actor, which places it beyond the scope of instruments that require attribution to operate. Secondly, the rate of change in AI-enabled tactics outpaces any defence organised around periodic rather than continuous assessment.

Scale is easier to grasp at the level of a single network. The Pravda network, identified by France's VIGINUM as Portal Kombat, aggregates pro-Kremlin content from over than 200 countries and language-specific subdomains, 89 of which are under a single branch domain. Between 1 September and 9 October 2025, its Czech-language subdomain republished over 200,000 items, of which 822 were election-specific. More than a third of these originated from one Telegram channel. Almost none of this content is original, and is designed to be indexed, cited and recirculated by others. This infrastructure is designed to launder provenance rather than persuade, which is why detection alone achieves so little. It regenerates faster than any takedown can remove it.

The project

The FDEI has brought together ten organisations to monitor, respond to and counter foreign information manipulation and interference across electoral cycles, within the framework of the FIMI Information Sharing and Analysis Centre ([FIMI-ISAC](#)); the consortium and the FIMI-ISAC membership are not the same. The consortium's mandate runs from January 2025 to January 2027.

The composition of the consortium forms part of the methodology. Organisations with a European analytical and policy remit included Debunk.org (the coordinator), the Institute for Strategic Dialogue, Fundación Maldita.es, GLOBSEC, EU DisinfoLab, the Digital Forensic Research Lab at the Atlantic Council, Alliance4Europe, the DISARM Foundation, the Alliance for Securing Democracy at the German Marshall Fund and the [DEN Institute](#). These were paired with civil society organisations (CSOs) rooted in the national information environments under observation. The operational focus was on 2025 electoral cycle, and particularly the German federal election in February, the Polish presidential election, the Moldovan parliamentary election on 28th September and the Czech parliamentary election on 3rd -4th October. These differ in terms of exposure, in the maturity of the responding institutions, and the extent to which foreign operations could rely on domestic amplification. The same instruments were later applied to the Ceuta migration crisis outside the electoral calendar.

Outputs

The value of the framework is realised only in aggregate. A taxonomy used by one organisation is an internal convention; used by ten, it carries across borders.

Analytical framework		One method for classifying and recording FIMI incidents across all partners and countries: the DISARM Red Framework is used for tactics, techniques and procedures; and a hierarchy of meta- and sub-narratives, is employed alongside promote/excuse/normalise/accuse model which was used in the Moldovan assessment to describe narrative function. Risk framing is adapted from a common election risk assessment framework. Incidents are encoded in DISARM and STIX and held in OpenCTI.
Operational handbook		The FIMI Response Team blueprint is designed to help defenders: how to stand up election monitoring, identify and mitigate vulnerabilities, conduct risk assessments, monitor and report incidents, identify the relevant stakeholders, and report violations.
Country election risk assessments	4	Produced before each monitored vote, and based on a fixed structure, it identifies the actors, narratives, infrastructure and vulnerabilities likely to be exploited in that national context.
Country election reports	4	The following are produced after each vote: tactics, channels, threat actors, reach and engagement, the conduct of political actors, attempted interventions, and policy recommendations.
Incident alerts	117	Structured alerts on individual incidents are written in a shared template with a fixed eleven-section schema and can be exported as structured data. This shortens the distance between a researcher detection and someone's response.
Structured case base	500+	There are high-priority cases in OpenCTI, with more than 800 further cases codified from EUvsDisinfo against a target of 18,000.
Capacity	100+	Ten to fifteen analysts per election were part of response teams that were trained by defenders. These teams combine local and international expertise.

The deliverables do not constitute attribution. The framework records and classifies observable phenomena, and the question of who is responsible for an operation remains with the relevant authorities. They do not substitute regulatory or platform action either. They are an analytical layer designed to prove usable information at the point where such action is decided.

What the reports document

The four election reports follow the same structure and are therefore comparable.

The German report, on the February 2025 federal election is based on a codified set of one hundred public reports from which ninety-eight distinct FIMI incidents were identified. The report documents Doppelgänger, which it attributes to the Social Design Agency acting for the Russian presidential administration. Doppelgänger was carried out in two waves, comprising 288 and 573 posts, respectively; Operation Overload, which involved at least 48 X accounts that were amplified by more than six thousand others. Every post in the dataset received all its reposts within a single minute. Finally, the report documents Storm-1516, involved the creation of over a hundred websites that produced AI-generated content in the three months prior to the vote. The total observed reach is estimated to be around fifty-five million views. However, it should be noted that no engagement figure can be considered reliable where amplification is artificial. Only three instances were recorded of this content demonstrably reaching the German information space.

The Polish report, on the presidential election, consolidates information from twenty-eight organisations and twenty incident alerts between April and June 2025. Its principal finding is persistence. Six hundred Doppelgänger posts were identified in April and May, and the operation continued to be published after X had acted on the flagged accounts, which the report suggests may have breached EU sanctions given the sanctioned status of the entities behind them. The report also documents a Meta advertising campaign that spent a €100,000 euro to reach one million users, as well as Polish-language Radio Belarus channel with over nine million views and more than nine hundred videos.

Of the four reports, the Moldovan report is the most comprehensive, consolidating information from thirty organisations and twenty-two incident alerts from August and September 2025. It documents a shift towards decentralised manipulation involving pseudo-media outlets and cloned websites, paid influencer networks and AI amplification. It also names Storm-1516, Operation Overload, REST Media and Info Leaders. The report also details an election-day cyberattack that forced the authorities to block the Host.md platform, briefly taking approximately four thousand websites offline. This did not affect the conduct or counting of the vote. Additionally, it describes a disrupted attempt to fabricate evidence of fraud involving a recruitment scheme offering €500 plus bonuses of up to €30,000 per alleged irregularity reported. This schema was advertised twenty-one times to over a million users across the EU and the United Kingdom. The vote returned PAS with 50.20 per cent of the votes against 24.20 for the Patriotic Electoral Bloc. This occurred against a background of energy insecurity, regional security pressure and distrust in institutions which the report identifies as enabling conditions. Russian-speaking minorities, rural communities, Gagauzia and Transnistria and the diaspora recur as target groups.

The Czech report, published in November 2025 on the parliamentary election of 3rd–4th October, documents the Czech subdomain of the Pravda network, and its 234,500 articles since launching in March 2024, and a TikTok network comprising 146 coordinated accounts with 309,000 followers and 76,000 videos. Of the four reports, this one is the most measured. While Russian-linked networks did attempt to undermine confidence in the vote, but no coordinated operation capable of influencing the result was detected. The report adds that the most impactful polarising narratives were those spread by domestic political representatives.

One finding recurs across the set. Both the Moldovan and German reports both describe a growing convergence between foreign and domestic manipulation, with pro-Russian groups acting as domestic amplifiers while foreign actors operate through local intermediaries. The German report distinguishes between foreign and domestic manipulation while acknowledging their interaction, and the Czech report reaches the same conclusion from a different perspective. A pattern found in more than one political system is a different order of claim to one found once.

The record on platform response

Monitoring four contests using one method produced what no single report yields, a comparable record of what happened after content flagged, which no single report could provide. In Germany every instance of the Storm-1516 campaign was reported to the relevant platforms, including through via Digital Services Act notification mechanism. X rejected them all, stating in correspondence that the content was not illegal, and no action was taken. Bluesky acted on the same reports, and activity on the platform fell away sharply. Similarly, enforcement of the sanctions against RT DE was uneven. Of 31 mirror domains and subdomains identified, 17 remained accessible via through Germany's largest internet service providers, one of which had blocked none.

Poland provides an example of a removal that did take place. In April 2025, two hundred and seventy-nine Doppelgänger accounts were taken down; monitoring published at the end of May recorded a further three hundred and twenty-one posts over the same two months. The report interpretes this as evidence that no systemic measure accompanied the account-level action. In the Czech Republic, the scale was different, but the conclusion was the same. One platform reported removing over 187,000 fake accounts, nearly 2.9 million fake likes and more than two million fake followers prior to the vote. Nevertheless, researchers discovered and reported a network promoting pro-Russian narratives that reached five to nine million views. Moldova is the fourth instance. Its authorities requested the blocking of 443 TikTok channels with over 1.2 million followers and over 4.5 million views. Afterwards the head of the national police stated that approximately 95% of flagged content had not been removed. The report notes that it could not independently review these requests.

One thing belongs to that record. The chain is not broken uniformly. In Germany the findings were adopted by the national authorities and incorporated into their threat assessments. They were also the Commission services responsible for the Digital Services Act, the Code of Practice secretariat and the national Digital Services Coordinator. Where the chain worked, it did so through institutions. Where it failed, it was when a notification met a platform. This asymmetry was examined in the first session, and the project's own record provides evidence of it.

Proceedings and discussion

Organisation	DEN Institute with Debunk.org, on behalf of the FDEI consortium
Host	European Parliament Liaison Office in Italy, Europa Experience David Sassoli
Institutional addresses	Senate of the Italian Republic · European Parliament Liaison Office in Italy, joining from Strasbourg
Presentation of outputs	Debunk.org
Session I — moderation	GLOBSEC
Session I — panel	European Commission, Directorate-General for Communication · European External Action Service · Ministry of Foreign Affairs and International Cooperation, Hybrid Threats Unit · EU DisinfoLab
Session II — moderation	Institute for Strategic Dialogue
Session II — panel	CEE Digital Democracy Watch · Debunk.org · Context.ro · Digital Forensic Research Lab, Atlantic Council · NASK · Fundación Maldita.es

The first session addressed the gap between detection and disruption. Operations such as Doppelgänger, the Pravda network, Operation Overload and Storm-1516 have persisted across electoral cycles, adapting their infrastructure, narratives and distribution methods as necessary. The following questions were raised: what happens after a researcher identifies a serious incident; is the path to platform or regulatory action rapidly enough; who is missing from the response chain; and what would a European Centre for Democratic Resilience need to do that existing structures do not? In the same context, data access for vetted researchers under the Digital Services Act was also reviewed. The list of actors is where the asymmetry lies. While a researcher who identifies a coordinated operation can publish and notify, but everything that follows (removal, demonetisation, deregistration, sanction and prosecution) belongs to others, across several legal regimes and two continents. No participant is accountable for the entire process.

Three problems dominated the discussion. First, Europe does not see the full picture of FIMI across its own territory and the uneven gaps between member states. Second, polarisation narrows the space for any response capable of commanding agreement. Third, capacity is thinnest at the local level, where the work is hardest. Regarding positioning, the question of duplication was raised and addressed. There is no strong cooperation hub in place yet, and a centre of this kind must be operational rather than advisory. Participants were informed that the Shield is expected to be operational next year.

The second session examined whether the tactics, infrastructure and escalation patterns recorded in 2025 could provide an early warning of approaching cycles in Sweden, Latvia, France and Italy. Four lines of argument ran through it. The main operational benefit of cooperation is saving time, as partners can address the problem immediately rather than rebuilding contacts at the start of each crisis. The adversary is not just the anti-democratic state anymore, as profit-driven actors are also monetising the same narratives with AI-generated content produced largely outside the Union. Furthermore, the evidence that the Commission relies on is collected by civil society organisations and would not exist without funding. The Moldovan diaspora vote was a declared target, attacked in order to both divert and to suppress it, with national responses differing sharply in maturity. Furthermore, the method can be transferred beyond elections. However, is not the risk assessment that is transferred, as crisis leaves no time for this, but rather the methodology, cooperation and local knowledge.

Where the model is intended to land

The design addressed a requirement that the EEAS has set out itself, the need for more structured and agile information sharing across sectors and jurisdictions, supported by cross-jurisdictional evidence pipelines based on open-source investigations. As each monitoring effort has classified what it saw in its own terms, so evidence gathered in one member state has rarely been in a

form that a regulator or a platform in another could act on. Interoperability converts these separate national efforts into a single body of evidence. Without it, cross-border cooperation remains dependent on the goodwill of individuals rather than being a capability that institution can rely on. The other half of the problem is access, since a framework can only organise what its users can observe and much of what matters sits inside platforms.

The European Democracy Shield takes a whole-of-society approach and proposes the establishment of a new Centre for Democratic Resilience. The EEAS has described its own role, in complementarity with the Shield, as that of an operational instrument that translates analysis and coordination into responses. FDEI's model is an input to the analytical layer on which that role depends.

Recommendations arising from the country reports

The report concludes with recommendations based on the findings rather than first principles, which are presented here as part of the project's output addressed directly to institutions. Regarding oversight capacity, they propose the establishment of an independent, dedicated and adequately resourced body performing functions like those of a Digital Services Coordinator. This body would be responsible for coordinating enforcement, platform engagement, data access and cross-border cooperation.

Regarding systemic platform risk, they advocate mandatory advertiser verification including the disclosure of ultimate funding sources during election periods. They also propose the establishment of publicly accessible political advertising archives which would contain spending, targeting and sponsorship data. These archives would be open to national oversight bodies and accredited researchers. Other recommendations include the implementation of political advertising labels that cannot be altered after verification, the development of election-integrity preparedness protocols, and the close monitoring of recommender systems. This monitoring would include providing users with the option to switch off personalised recommendations. Regarding research access, they propose legal provisions mirroring Article 40 of the Digital Services Act. These provisions would give qualified researchers, and state institutions proportionate access to essential platform datasets. There would be centralised data-access hub and sustained funding for analytical capacity.

Two further recommendations address questions raised in Rome. Accountability frameworks should explicitly cover domestic enablers and cross-border influence laundering, rather than stopping at the foreign origin of an operation, this is the convergence problem that the first session left open. Furthermore, public resilience requires sustained investment in media and digital literacy as well as in the monitoring capacity of independent media and civil society organisations, addressing the funding question raised in the second session in operational terms.

Findings

The two sessions support a small number of conclusions that can be stated without overreach. **On visibility**, FIMI's coverage across European territory is incomplete and uneven, with the sharpest deficit at local level. **On institutional design**, an operational body is required, rather than an advisory one, bearing in mind that no model can be transferred unchanged between member states. **On the adversary**, a response based solely on state attribution will not address a significant proportion of the activity, which aligns with the proportion of unattributed activity in the EEAS figures. **On method**, the approach extends beyond the electoral calendar, within the aforementioned limitations. **On the horizon**, the expected timetable for the Shield provides a near-term date against which the continuation of this work can be planned.

Two questions were raised in both sessions but not answered. The first is ownership. There was broad agreement on the remaining institutional and operational gaps, but no agreement on who is responsible for closing them. The second question concerns the continuity of funding. The evidence pipeline described here is maintained by organisations whose capacity depends on project finance. The interval between one instrument and the next is the period during which monitoring capability is lost rather than transferred.

Next steps

The mandate runs until January 2027. The project's core outputs will be circulated to participants alongside the photographic record of the day. An account of the event is also being prepared for the FIMI-ISAC website. The consortium is available to answer questions about the methodology and to facilitate contacts within the network and collaborations that participants may wish to initiate or continue. e. Based on the last two years, any successor arrangement would need to maintain a stable taxonomy, since the value of the evidence base is cumulative. It would also need to maintain standing teams rather than project-length ones; secure a route by which an alert reaches someone able to act on it; and to begin before the next contest, not alongside it.

Two things would make that outcome more likely. First is that those intending to work together after January 2027 should declare their intentions now, while the network is active and the contacts are up to date, rather than waiting for a call to be published and assembling partners against a deadline. Secondly is that the expected timetable for the Shield should be treated as a planning date rather than breaking news, since the time between now and then is the window in which a consortium can be formed deliberately rather than hurriedly.

Annex — the eight country documents, available on request

Risk assessment — Germany	February 2025	Authorship not recorded in the documents consulted.
Risk assessment — Poland	2025	Produced ahead of the monitored vote.
Risk assessment — Moldova	August 2025	DFRLab, Alliance4Europe, Debunk.org, with EU DisinfoLab.
Risk assessment — Czechia	August 2025	Alliance4Europe, Debunk.org, GLOBSEC, EU DisinfoLab, DFRLab, Institute for Strategic Dialogue.

Election report — Germany	February 2025	Institute for Strategic Dialogue, Alliance4Europe, Debunk.org, GMF Alliance for Securing Democracy, DEN Institute, EU DisinfoLab, with sixteen in-country partners.
Election report — Poland	2025	Debunk.org, Alliance4Europe, DFRLab, GLOBSEC, Institute for Strategic Dialogue, EU DisinfoLab, with seven contributing organisations.
Election report — Moldova	28 September 2025	DFRLab, Debunk.org, Alliance4Europe, EU DisinfoLab, GMF Alliance for Securing Democracy, GLOBSEC, with Reset Tech and LetsData.
Election report — Czechia	3–4 October 2025	GLOBSEC, Debunk.org, Institute for Strategic Dialogue, DEN Institute, Alliance4Europe.