

FIMI DETECTION as a Lived Professional Experience in the Brussels Bubble

Asya Metodieva *

August 2026

** Asya Metodieva is a Senior Researcher at the Institute of International Relations Prague. Her broader research interests include terrorism and other forms of political violence, polarisation and radicalisation activities, and content moderation. Her research is particularly focused on the Western Balkans and Southeastern Europe more generally. She is a member of the Centre for European Politics at the institute. She obtained her Ph.D. from the Central European University in Vienna.*

Note: This publication has been authored by external contributor/s. The contents do not necessarily reflect the opinion or the position of EUROPEUM Institute for European Policy

This policy paper was produced within the Think Visegrad in Brussels Fellowship programme. In the first half of 2016, eight think-tanks from the Visegrad Group that have been cooperating in the Think Visegrad platform, agreed on the idea proposed by the EUROPEUM Institute for European Policy, to create a common representation office in Brussels. The main motivation for it is the need to encourage debate on issues of common interest to the EU and the V4 and explain the positions of the V4 to a wide audience. Think Visegrad in Brussels would like to project an image of constructive partners, to explain the dynamics of the debates within our regions and to highlight our active contributions to EU policy-making. For more information about Think Visegrad and its members visit www.think.visegradfund.org.

Contents

<i>Summary</i>	<i>3</i>
<i>Introduction</i>	<i>3</i>
<i>Strategic Context and FIMI Monitoring</i>	<i>4</i>
<i>FIMI in Elections across Europe</i>	<i>5</i>
<i>Disinformation as a Lived Experience in the Brussels Bubble.....</i>	<i>7</i>
<i>Conclusion.....</i>	<i>15</i>
<i>Recommendations.....</i>	<i>16</i>
<i>About EUROPEUM.....</i>	<i>20</i>

Summary

This paper analyses how foreign information manipulation and interference (FIMI) targets key EU policy areas, including EU enlargement, sanctions, and support for Ukraine. This study shows that certain EU policies are more targeted by FIMI. This paper identifies recurring narratives linked to specific policy decisions at the EU level and electoral campaigns at the member/candidate-state level. The analysis focuses on how disinformation in these areas is professionally ‘experienced’ and addressed by key stakeholders through monitoring, analysis and crisis management. Rather than treating FIMI as an abstract threat, this study approaches it as a ‘lived’ information ecosystem that surrounds EU decision-making and triggers institutional responses. It collected and analysed the perceptions of EU officials, Brussels-based journalists, fact-checkers, and think tank representatives.

Introduction

Today’s geopolitical conflicts and the two major ongoing wars – between Russia and Ukraine and between the US/Israel and Iran—are highly reliant on the weaponisation of the information sphere. The security climate surrounding the EU has worsened, which has also impacted the EU’s information environment. The European Union External Action Service has reframed disinformation as an external threat, specifically examining the vulnerability of core democratic processes and regulatory frameworks to foreign interference (Proto et al. 2025; Athanasiou et al. 2025). FIMI does not function in a vacuum; rather, it is an element of a hybrid arsenal that combines digital interference with physical means and coercive tactics. Consequently, it is not simply a matter of communication but a component of a comprehensive strategy with political and security implications (European External Action Service, 2026).

The digital context does not make the task of combating FIMI easier. Social media platforms are instrumental in the formation of ideologically like-minded user groups, where individuals mutually reinforce their opinions without questioning their views. Thus, the attention economy offers a fertile ground for information manipulation, which is not always used to make individuals believe certain false claims but to distract them and generate distrust, or in the European Commission’s words, “to activate anti-democratic norms, authoritarian instincts and behaviours” (European Commission, Joint Research Centre et al. 2026). Because information goods are so cheap to reproduce so quickly and on a large scale online, the scarce resource shifts from the information itself to the audience’s attention — customers’ limited capacity to notice and engage with content becomes the valuable, constrained commodity that companies compete for (Shapiro and Varian 2010; Ciampaglia et al. 2015).

The EU remains a frequent target of disinformation within the region, with such content consistently accounting for at least 5% of all disinformation detected by the EEAS over a period of one year, until February 2026. Monitoring data from the EDMO indicate that this trend peaked in January 2026 (EDMO 2026). This is likely linked to political and economic developments, including Bulgaria’s adoption of the Euro and the signing of the EU-Mercosur Agreement, which triggered agricultural protests in several countries (ENR 2026). Additionally, the corruption scandal concerning former European Commission Vice President Federica Mogherini provided further fuel for the dissemination of false narratives targeting various European officials (European Digital Media Observatory 2026b). Since the end of 2025, various disinformation campaigns have exploited ongoing events to frame the EU as an unpopular, autocratic, and weak institution governed by a corrupt elite.

Meanwhile, the fine imposed on X under the Digital Services Act (European Commission 2025a) was portrayed as an act of censorship, fueling allegations that the EU suppresses political expression.

Agricultural protests were likewise framed as a "rebellion against the EU," with their scope exaggerated by AI-generated imagery and recycled media content (Benoist 2024). False narratives further included claims that Italian PM Giorgia Meloni had reclaimed national gold reserves from the European Central Bank and that the €10,000 cap on cash transactions signified the end of financial freedom (Fonte 2025). Regarding EU leadership, a viral rumour claimed that President Ursula von der Leyen fled Parliament after the then Hungarian PM Viktor Orbán supposedly disclosed damaging information. Additionally, an AI-generated image falsely depicted Vice President Kaja Kallas, known for her strong stance against Russian aggression in Ukraine, as a Soviet pioneer (European Digital Media Observatory 2026a).

Finally, data from the EDMO show that European governments and the EU have also served as secondary targets for xenophobic and Islamophobic disinformation campaigns, which frequently characterise these institutions as excessively permissive regarding immigration (European Digital Media Observatory 2026a). Such disinformation, which seeks to frame Europe as besieged by violent actors, aligns with the "Great Replacement" conspiracy theory, which posits that European cultural identity is undergoing a deliberate "ethnic substitution." This narrative has been utilised by European far-right political actors. Meanwhile, Islamophobic, antisemitic, and anti-immigration disinformation intensified following the Bondi Beach massacre in Sydney, where fake claims were spread online, arguing that Muslims celebrated the attack (European Digital Media Observatory 2026a).

This research combines semi-structured interviews with EU officials, journalists, and researchers based in Brussels to shed light on their professional experiences of encountering, monitoring, and responding to FIMI campaigns. The interviews explored strategic thinking and communication approaches, perceptions of information operations, and institutional responses. Additionally, this study relied on monitoring reports from the European Digital Media Observatory, the European External Action Service, transparency data, and platform reporting under the European Commission.

Strategic Context and FIMI Monitoring

The EEAS detected and analysed 540 FIMI incidents between January 1st and December 31st, 2025. 10 500 unique channels were involved in detected FIMI incidents over the last year, ranging from fabricated news websites to social media accounts or blogs, resulting in cross-platform activity and coordination between multiple assets of the FIMI ecosystem. 9,5% of these channels are directly related to state actors. The vast majority (90,5%) consisted of covert assets linked to or aligned with a threat actor, with the latter category remaining unattributed. In other words, the largest part of FIMI infrastructure is hidden or inauthentic (including CIB networks). Therefore, exposing the connections behind covert FIMI sources is crucial for mitigating their potential impact (European External Action Service 2026).

Of all the incidents of disinformation documented by the EEAS, 35% were attributed to Russia (29%) and China (6%). Beyond the attributed figures, Russia and China rely on extensive covert and fabricated networks aligned with their strategic objectives. By outsourcing capabilities through these opaque networks, they expand their reach while preserving plausible deniability and complicating attributions. Ukraine remains the primary target of FIMI efforts in the EU, as in previous years, followed by France, Moldova and Germany. These attacks have surged in both frequency and sophistication as FIMI rapidly evolves to exploit AI (European External Action Service, 2026).

Russian state institutions continue to play a key role in FIMI activities. The Foreign Intelligence Service (SVR) has taken on a more visible role, issuing official statements containing false or unsubstantiated claims that are later amplified across the FIMI networks. In 2025, this included false allegations of EU and NATO-backed plots to destabilise Moldova, Serbia, and Georgia (Russia Today 2025). According to the EEAS's latest (4th) report on FIMI, funding for foreign information operations in Russia increased in 2026 as part of the budget increase for state-controlled media, which reached 146.3 billion roubles (around 1.56 billion EUR) in 2026 (European External Action Service 2026, 13). In the EEAS assessment, the Kremlin continues to use FIMI as one of its core instruments of state power, fully integrating it into its broader strategic and hybrid toolkit. In 2025, Russia's disinformation priorities were centered on the war in Ukraine, targeting Ukraine's partners, including the EU. Manipulation activities appear along with hybrid actions, including drone incursions, acts of sabotage, and attacks on critical infrastructure in EU countries such as Poland, Romania, Lithuania, and Estonia. These incidents were accompanied by FIMI tailored to influence public perceptions and trigger responses (European External Action Service 2026).

Since 2024, Russian FIMI has shifted from simultaneously targeting the EU and the US to a more concentrated emphasis on Europe while keeping some room for maneuvering. Russian FIMI actors focused on the EU as an adversary, showed inconsistency regarding the US, and portrayed themselves as an alternative to a supposedly morally decadent West and a guarantor of a "multipolar world order" (European External Action Service, 2026).

FIMI in Elections across Europe

Electoral processes once again became the primary focus of FIMI activities. Nearly half of the recorded incidents in the EEAS' 4th Report were triggered by specific events, especially breaking-news events or electoral processes that provide fertile ground for information manipulation. Major democratic processes, such as parliamentary elections in Hungary, were highly anticipated events by the FIMI attackers (Léderer 2026; Deutsche Welle 2026).

In 2025, Russia targeted elections in Germany, Poland, Romania, Moldova (Marocico and Mirodan 2025; Organisation for Security and Cooperation in Europe 2025), and the Czech Republic. In 2026, electoral processes in member states, including Slovenia, Hungary, Bulgaria, Cyprus, Estonia, Sweden, Latvia, and Denmark, faced similar interference patterns (European External Action Service, 2026). Beyond the EU, while Ukraine remains at the heart of Russia's hybrid war efforts, Moldova appears as one of the key priorities of the Kremlin in 2025, following the parliamentary elections held in October 2025. The attack patterns observed during the presidential elections in Moldova revealed similarities with networks and tactics in Armenia. Armenia was a key target in the run-up to the June 2026 parliamentary elections. In Czechia, hundreds of anonymous TikTok accounts spread pro-Kremlin narratives ahead of the parliamentary elections, while the elections in Moldova faced an unprecedented wave of hybrid threats and FIMI (European External Action Service, 2026).

In April, the war between the USA, Israel, and Iran was the most targeted topic for disinformation. However, false news on the matter plummeted from 39% recorded in March. False news related to the Gaza crisis also decreased by three percentage points. Meanwhile, the focus of disinformation seemed to shift back to the war in Ukraine and immigration. The war in Ukraine gained more attention from disinformation actors, partly because of the electoral debate in Hungary and Bulgaria and its consequences on sanctions against Russia and economic support to Kyiv. False news on immigration took an Islamophobic turn during the Easter period, which is likely the reason for the increase in the circulation of such disinformation (European Digital Media Observatory 2026d).

In the first months of 2026, disinformation campaigns across Europe heavily targeted the Hungarian elections. Before the vote, false news mostly in favour of the former PM Viktor Orbán, claimed that he had terminated all agreements with the EU and that Hungary was joining the BRICS (European Digital Media Observatory 2026d). Furthermore, false news related to the Hungarian elections extensively used anti-Ukrainian messages. Former PM Viktor Orbán suggested that explosives found near a key gas pipeline in Serbia were evidence of Ukrainian sabotage. Before the elections, pro-Fidesz media misleadingly presented an interview with Ukraine's ambassador to Budapest as if he threatened Hungary with destabilisation. Meanwhile, other disinformation channels spread false news that newly elected PM Magyar planned to revoke Ukrainians' work permits in Hungary (European Digital Media Observatory 2026c). Thus, FIMI had a significant impact on the electoral space in Hungary. The key narrative that connected foreign and domestic politics through disinformation was that the then opposition party Tisza was on the leash of Brussels and Kyiv, and it would likely bring the country to war should it win. International disinformation actors, such as Matryoshka and Storm-1516, were particularly active and visible during Hungary's election campaign (European Digital Media Observatory, 2026c).

Meanwhile, anti-corruption protests in Bulgaria (Furlong, 2025) were misrepresented as a movement for the country's desire to leave the EU. Disinformation about Bulgaria joining the Eurozone, which was already detected in December 2025, persisted in the first months of 2026 (European Digital Media Observatory 2026d). FIMI activation was detected throughout the campaign before the vote in April 2026. After the spread of AI-generated images of Ukrainian cash and gold transport seized by Hungarian authorities, the pro-Russian disinformation network Pravda was rapidly activated and started circulating false claims, publishing 6,000 articles per month in Bulgarian. Pro-Kremlin narratives circulated false claims that Bulgarian ammunition was used against ethnic Bulgarians in the Ukrainian city of Kherson (European Digital Media Observatory 2026d).

According to the EUvsDisinfo database, between January and May 2026, there were 30 false or manipulative narratives that focused on Europe, 19 of which specifically targeted the EU. The most exploited topics include the war in Ukraine, where NATO and the EU are often seen as a collective threat. Another topic is Energy and Sanctions, where Europe is presented as facing an energy collapse without Russia, which has been a repetitive frame since 2022 (Dubóczy and Dinič 2022). Finally, digital affairs have become a central theme to FIMI targeting the EU, where the EU's digital frameworks are often described as a threat to freedom of expression. Using the tag "War against Ukraine" combined with "European Union" leads to 57 sub-narratives used in the reporting period, as most of them refer to the EU, European leaders, or Europe. Reports from the European Commission, the Parliament, and the European External Action Service show that FIMI narratives often target EU democratic values and the rule of law. On the most recent occasion, documents released by the U.S. Department of Justice concerning the late Jeffrey Epstein were exploited to push the claim that Western institutions protect global elites from accountability, characterising the West as inherently corrupt and adversarial to the public (EUvsDisinfo 2026a).

Another disinformation narrative suggests that, building on French President Macron's stated desire to restrict social media access, the French government is preparing to block VPNs altogether (EUvsDisinfo 2026b). This claim asserts that such a measure would effectively cut off large portions of the French population from alternative information. The narrative argues that the French elite, threatened by information pluralism, aims to prohibit VPNs to establish an informational "Berlin Wall" across France and the West. Another related pro-Kremlin narrative portrays Western media as heavily censored and controlled, alleging that liberal democracies suppress dissent to advance their geopolitical objectives. This discourse, which intensified following the restrictions imposed on Russian outlets such as RT and Sputnik after the invasion of Ukraine, seeks to frame Western freedom of expression as a myth (EUvsDisinfo 2026c).

Disinformation as a Lived Experience in the Brussels Bubble

FIMI, as known in policy circles, is actively used in threat assessments, and for those working inside EU institutions, it has become a daily reality. Pro-Russian narratives, either created in Moscow or amplified through social media, find their way into debates in the European Parliament, shape the talking points of politicians, and appear in the work of think tanks and scholars whose Kremlin connections are anything but transparent.¹ Thus, the Brussels bubble is not isolated but is part of the battleground for FIMI operations, and professionals working within the EU institutions are increasingly aware of it.

The appearance of FIMI registered by the EEAS that often circulates within debates in the European Parliament correlates with what Russia perceives as a threat to its core interests. EU enlargement, sanctions policy, energy dependencies, and the bloc's support for Ukraine consistently attracted the heaviest volume of manipulation efforts.² FIMI spikes have been observed in Moldova and Armenia, where EU proximity is contested and the domestic political environments are vulnerable. Within the EU's policy agenda, support packages for Ukraine, the credibility of sanctions, and internal regulatory debates, including the Digital Services Act (DSA), have all been targeted in the recent years, according to most experts interviewed for this paper. Meanwhile, EU efforts on collective defence and military modernisation have attracted comparatively less attention from Russia, in part because they tend to be framed through individual member states rather than as a coherent EU initiative, which makes them less suitable targets for Brussels-directed messaging.³

The landscape of these operations has also shifted in response to global events. Following Donald Trump's return to the White House, FIMI narratives shifted away from targeting the US and focused more on the EU itself as a militaristic or security-driven actor, deliberately blurring the institutional boundaries between the EU and NATO. This repositioning serves two purposes. On the one hand, it feeds existing anxieties in candidate and neighbouring countries about being drawn into a conflict not of their making. However, it undermines the EU's image as a normative power. These dynamics are particularly evident in the Western Balkans. FIMI actors exploit historical grievances, including NATO's bombing campaigns in Yugoslavia in 1999 and the strike on the Chinese Embassy (Ponniah and Marinkovic 2019), to cultivate fear that history could repeat itself. Public anxieties concerning demographic decline, combined with narratives about migration and the "Great Replacement" are similarly weaponised. In such cases, foreign manipulation steps on pre-existing antagonisms rather than inventing new ones.⁴

Monitoring these operations requires both scale and sophistication from EU institutions. To understand the big FIMI picture, analysts simultaneously track official and unofficial media, social media channels, and known FIMI networks through multiple systems. The work is as predictive as it is reactive, although the pace of global events frequently forces a reactive posture. One telling pattern is that surprises tend not to come from unexpected topics but from an absence of anticipated activity, for example, the limited interest of FIMI networks in European defence.⁵ FIMI actors are highly opportunistic, especially when exploiting local events such as domestic political crises, bilateral disputes, or events involving migrants. They use such topics to channel them into long-running, strategic narratives. Monitoring has also expanded beyond the information space, tracking the growth of physical FIMI infrastructure on the

¹ Interview 1: An interview with a political advisor at the European Parliament, 13/05/2026.

² Interview 2: A group interview with EU representatives, 12/05/2026.

³ Interview 2.

⁴ Interview 2.

⁵ Interview 2.

ground, as well as developments in AI and large language models that are reshaping how influence operations are constructed and deployed.

Effective response demands what practitioners describe as an "infinite toolbox" which means that no single instrument is sufficient.⁶ The interviewed diplomats emphasize that framing issues in a proactive manner before hostile narratives gain popularity can sometimes prevent the spikes that reactive responses struggle to contain.⁷ Additionally, when journalistic investigations reveal that a campaign is coordinated and directed by the Kremlin, it changes how audiences in EU countries, as well as in EU institutions, receive the information. Knowing that a campaign is orchestrated alters how people read its messages, namely with skepticism rather than blind acceptance. Strategic communication through EU delegations, independent media, and civil society organisations reinforces this, while regulation, particularly the DSA, creates structural constraints on the spread of manipulative content.⁸

A key challenge for analysts and practitioners in Brussels is to convincingly stress the distinction between manipulation and legitimate political speech, especially when politicians using misleading narratives are louder.⁹ The answer, for those who do this professionally, lies not in the content of a message but in the behaviour of the networks that carry it.¹⁰ When a view that presents itself as a personal opinion is simultaneously expressed by thousands of accounts across multiple languages and continents, it is not an opinion; it is a coordinated manipulative action.¹¹ This behavioural lens makes it possible to move away from the politically fraught question of what counts as true or false and focuses attention instead on the mechanics of artificial amplification. It is a pragmatic approach, born of experience, and reflects how experts in EU institutions have come to understand the information environment in which they operate.

Information manipulation has shifted from falsehoods to a mix of falsehoods, misleading claims, and partial truths, amplified by algorithms to create fragmented realities (European Commission. Joint Research Centre et al. 2026). If the first wave of FIMI awareness was about recognising that manipulation was happening at all, the current challenge is to understand which EU policies attract hostile attention, why, and what internal vulnerabilities make the bloc susceptible in the first place. Contrary to expectations, European defence policy has remained a relatively minor target. Part of the explanation is that external actors do not consistently frame defence as a core EU competency. Additionally, voices criticising the EU's rearmament already exist within the EU's own member states, making outside interference somewhat redundant. However, some of the interviewees expect that this may change in the coming years. The combination of Russia's war in Ukraine and the broader legitimisation of European defence efforts has opened what practitioners describe as a window of opportunity, which FIMI actors are likely to exploit by shifting narratives towards the economic costs of rearmament. The classic "bread versus butter" framing is being used to diminish public support for defence spending before it consolidates.

Among other areas, FIMI is most active in the domain of digital sovereignty. The EU's regulatory agenda, including the AI Act, Digital Services Act, Digital Markets Act, and CHIPS Act, has become one of the hottest targets in the digital information environment. The actors involved are not only foreign states, but also political stakeholders on a national level. Influence operations in this space draw on a multilayered ecosystem that includes EU member states, corporate lobbying networks, and advocacy

⁶ Interview 2: A group interview with EU representatives, 12/05/2026.

⁷ Interview 3: An interview with an EU representative, 14/05/2026.

⁸ Interview 2: A group interview with EU representatives, 12/05/2026.

⁹ Interview 4: An interview with a fact checker, 14/05/2026.

¹⁰ Interview 4: An interview with a fact checker, 14/05/2026.

¹¹ Interview 5: An interview with an EU representative, 12/05/2026.

organisations whose funding and affiliations are not always transparent.¹²

The most consequential dependency, however, is structural, as the EU relies on US providers for over 70% of its cloud infrastructure (Synergy Research Group 2025). Moreover, the major social media platforms that carry political discourse remain under American ownership and governance (Lynn et al. 2025). This creates a form of hybrid leverage that does not require foreign interference in domestic affairs. Control over Europe's critical technology translates continuously into influence over the information environment.¹³ The EU's reliance on U.S. tech companies means that four out of five European enterprises are tied to foreign platforms for their data operations (Gineikyte-Kanciere et al. 2025). In April 2026, The European Commission made a significant move towards "digital sovereignty" by awarding a 180 million (approximately \$ 213 million) cloud contract to a quartet of European providers. The deal will allow the Commission and the EU Parliament and Council - and all their various offices and agencies - to procure sovereign cloud services over the next six years from Luxembourg's Post Telecom, Germany's StackIT, France's Scaleway, and Belgium's Proximus. As the EU has recognised this as a threat to its autonomy, the bloc has developed a set of tools, including the AI Act and DSA. However, they seem to be open for revision, as current geopolitical shifts show that some of the EU's tech regulations in their current form prevent innovation and create compliance burdens for startups (European Commission 2025b).

The broader understanding of FIMI, which includes internal vulnerabilities alongside external actors, points to a change in how analysts and policymakers approach the problem in the current geopolitical context (Proto et al. 2025). While disinformation is often analysed at a narrative level, viewing such influence operations alongside cyberattacks and critical infrastructure disruptions offers a more ecosystemic perspective. What binds these elements together is the logic of weaponised interdependence, namely, the exploitation of operational gaps and dependencies that states and institutions have allowed to accumulate.¹⁴ Russia's manipulation of Europe's energy dependence in the past over 12 years since the annexation of Crimea served as a template. The concern now is that similar leverage could be applied to 6G deployment, supply chains, or other critical services, where European autonomy remains limited.¹⁵ One persistent narrative exploits the tension between regulation and innovation (Csernatori 2025). The criticism that is skillfully used in FIMI is that the EU's regulations over time, from the GDPR to the AI Act, are the key reason for Europe being technologically behind the US and China. The analysts interviewed for this study argue that it is not about recent regulatory choices but about decades of systemic under-investment, fragmented national frameworks, and an institutional culture with a limited appetite for risk.¹⁶ However, such vulnerabilities become a fertile ground for FIMI narratives and appear in political speech in the European Parliament, for example.

The question of how to respond to FIMI threats has produced a dilemma within EU institutions linked to the temptation to securitise. From a policy perspective, treating FIMI as a security threat has advantages because it creates urgency, but there are also some risks to this approach. Blurring the lines between civil and military responses, expanding the logic of national security into commercial technology, and concentrating authority in ways that lack clear legal grounding all carry serious costs to democracy.¹⁷ The fact that the same emerging technologies serve both commercial and military purposes makes these lines increasingly blurred. Thus, according to some interviewees, what the EU needs is not more securitisation, but more resilience through investments in media ecosystems and civil society that can

¹² Interview 6: An interview with an expert from Carnegie Europe, 12/05/2026.

¹³ Interview 6: An interview with an expert from Carnegie Europe, 12/05/2026.

¹⁴ Interview 2: A group interview with EU representatives, 12/05/2026.

¹⁵ Interview 5: An interview with an EU representative, 12/05/2026.

¹⁶ Interview 2: A group interview with EU representatives, 12/05/2026.

¹⁷ Interview 5.

resist manipulation operations before they affect significant parts of a population. The experience in Moldova has shown that the EU should use its tools to prevent FIMI early enough and with an understanding of the context that they are designed to protect.

At its core, countering disinformation is a race against time.¹⁸ Once a false or manipulated narrative has spread, it is challenging to reach the audiences who have already consumed it. Different communities inhabit different information ecosystems, and the boundaries between them are blurred, thus not allowing for a correction.

This asymmetry, in which manipulation spreads fast and a counter-reaction on a more massive level arrives late, has pushed EU strategic communication teams towards a more proactive approach.¹⁹ The goal is no longer primarily to refute what has already circulated but to establish a coherent EU narrative first, framing issues before hostile actors can fill the void. Prevention, as practitioners in the EU monitoring teams have argued, remains the most powerful tool available. The EEAS has now institutionalised this logic into a multi-year communication strategy developed with member states, built around three pillars: defending the EU, securing the neighbourhood and building partnerships.²⁰

The challenge is that the EU is structurally constrained to fast and coherent communication.²¹ Foreign policy messaging is produced simultaneously by the Commission President, High Representative for Foreign Affairs, Council Presidency, Parliament, and individual member states, each with their own mandates, audiences, and political calculations. The result is a contested environment in which the EU's voice is diffuse at precisely the moments when clarity matters most. Furthermore, for a long time, EU communication has been perceived as bureaucratic, technical, and/or "boring, complicated, unsexy" in the assessment of some of the Brussels-based experts interviewed for this paper.²² Within an information environment characterised by rapidity, emotional influence, and digital saturation, this institutional culture poses a liability for EU practitioners. Meanwhile, Russia and China have built their counter-narratives accordingly. Both Russia and China seek to portray the EU as weak, ineffective, or a residual colonial power. Such narratives aim not to persuade those who already share this view but to compromise the EU's credibility among audiences and in places where the EU's influence is most contested.

Russia's communication apparatus is structured in a very contrasting manner, as it is centralised, well-funded, and fast (Berkane 2026). State-controlled media, fabricated news websites, and synchronized messaging across various channels facilitate the spread of narratives from their inception to widespread amplification within hours. The model is driven by fear and strict institutional control, which ensures the effectiveness and coherence of the information operation. The EU cannot and should not replicate this approach, but it can learn from its pace. Interviewees within the EU acknowledge that some past decisions, including the refusal to engage even with trusted Russian journalists, may have created communication vacuums that hostile actors were quick to fill. This reflection shows institutional understanding, which is crucial for adapting the EU approach to FIMI. The lesson is not that the EU should abandon its values-based approach, but that values-based communication must be faster, more intriguing, and more emotionally resonant if it is to compete for attention in the contemporary information environment.²³

The EU's new global campaign, built around the claim that the bloc is a "reliable" actor that is predictable

¹⁸ Interview 2.

¹⁹ Interview 3: An interview with an EU representative, 14/05/2026.

²⁰ Interview 7: An interview with an EU representative, 13/05/2026.

²¹ Interview 3.

²² Interview 3.

²³ Interview 3.

in a geopolitical landscape increasingly defined by transactional or coercive behaviour (European Commission & High Representative of the Union for Foreign Affairs and Security Policy 2025), is an attempt to operationalise this shift. Rather than leading with abstract principles or aggregate figures, the campaign emphasises concrete actions, human stories, and relatable examples. Specific regional campaigns are planned for the Middle East, the Russia-Ukraine theatre, the Indo-Pacific with a particular focus on India, and Africa, especially the Sahel, where EU security engagement competes directly with Russian influence on the ground (European Parliament 2026a; EEAS 2026b). What we know from previous analyses of FIMI show that hostile narratives succeed by being locally grounded and exploiting context-driven grievances. Thus, there is an understanding among EU practitioners and experts that broad institutional communication is insufficient to address those in some local information environments.

Alongside strategic communication, the EU has invested in long-term public diplomacy focused on relationship building and the slow accumulation of credibility. Initiatives such as "Our Voice, Our Future," a global network of young content creators who share EU values and produce their own material for local audiences (EEAS 2026a), and structured engagement with EU alumni networks, Erasmus Mundus graduates, journalists, business contacts, represent a bet on people-to-people trust rather than top-down messaging.²⁴ EU citizens living in third countries are increasingly seen as cultural ambassadors, as demonstrated by the post-Brexit experience in the UK. Co-creation projects with cultural institutions, including animation workshops at the Osaka World Expo, further extend these efforts. This approach seeks to build affinity and familiarity in contexts where formal EU communications would carry little weight.

Societies with dense, positive networks of connection to the EU are harder to manipulate (Humprecht et al. 2020; Roozenbeek et al. 2020). Disinformation does not spread equally across all audience types. It finds purchase where institutional trust is low and alternative narratives are absent. Building these networks of trust, patiently and at scale, is ultimately the most durable form of resilience the EU can invest in.

Elections are among the most exposed moments in any EU member and candidate state, and thus, they have been used as a triggering point for foreign information operations. In countries that the EU considers part of its strategic neighbourhood, including Ukraine, Moldova, Georgia, and the countries of the Western Balkans, the pattern is well established. As a vote approaches, FIMI tools that have been pre-positioned — financial networks, media proxies, and social media infrastructure, are switched on.

Moldova is the case that EU practitioners return to most often, not only as a warning but also as an example of an effective response. It was reported that Russia spent hundreds of millions of euros trying to influence the election result and push the country in a different political direction (POLITICO 2025). The EU's coordinated work with electoral committees, law enforcement, and strategic communication teams contributed to a cleaner electoral environment. This experience is now being applied elsewhere, most immediately in Armenia and Western Balkan countries such as Montenegro, where election cycles create the next windows of vulnerability.²⁵ However, candidate countries are not just recipients of this support. For instance, Ukraine and Moldova have already gained frontline experience in combating information operations, while some EU member states possess substantial experience in this area.

The EU's position is difficult not because of a lack of tools but because of the persistent asymmetry of resources. Russia and other hostile actors can invest heavily and with few accountability constraints in countries they are trying to destabilise. The EU operates under tighter budgetary and institutional limits,

²⁴ Interview 7: An interview with an EU representative, 13/05/2026.

²⁵ Interview 5: An interview with an EU representative, 12/05/2026

which means that its support must be more targeted. Thus, the key is to identify the specific vulnerabilities of each country, provide direct assistance to the authorities and civil society actors, and focus not only on the election period itself but also on the longer-term project of building resilience. The aim is to enable countries to independently develop the ability to identify and address manipulation campaigns without relying on external financial support or needing EU intervention for each crisis.²⁶

On the communication side, the EU strategy is built around what practitioners describe as "crowding out". This means filling the public sphere with factual, accessible information about the benefits of EU integration before disinformation can occupy that space. Ahead of major summits and accession steps of a given country, messaging is coordinated across EU institutions and delegations to achieve what one practitioner described as "many voices, one message."²⁷ Local journalists and stakeholders are involved in content co-creation rather than being treated as passive recipients of Brussels-generated material. EU delegations receive dedicated funding for local outreach campaigns and events. The concrete changes that EU integration makes to everyday life, such as SEPA payment transfers, roaming fee abolition, and visa liberalisation, help messages shift from abstract institutional language towards more tangible and personal. This approach reflects a broader lesson from opinion polling, which consistently shows that public awareness of what EU enlargement delivers remains low, even in countries that have already joined the bloc. In 2025, 67% of EU citizens said they did not feel well informed about the EU enlargement, despite the majority supporting it. In candidate countries, awareness is even lower; only 48% in Moldova and 39% in Montenegro consider themselves well or very well informed, while in Ukraine, that figure drops to 23%, and to just 20% in Serbia (Directorate-General for Enlargement and Eastern Neighbourhood 2025).

However, not every critical opinion about the EU is the product of foreign manipulation. In Serbia, for example, public opposition to lithium mining projects tied to EU supply chain interests is a genuine political contestation, not a disinformation campaign, and treating it as one would be both analytically wrong and politically counterproductive. The EU's communication and FIMI teams have had to reflect this distinction in their work. The task is not to neutralise all criticism but to ensure that where manipulation appears, it does not push away a legitimate debate.²⁸ The risk of conflating the feeds directly into FIMI narratives that portray the EU as an actor seeking to manage and suppress rather than engage public opinion in candidate countries.²⁹

The institutional architecture that supports work on FIMI further includes the "European Democracy Shield" (EDS), which aims to contribute to the protection of democracy against attacks, including FIMI and disinformation (European Parliament 2026b; Bentzen 2026). The EDS instruments, including the Media Observatory and the Media Resilience Programme, are designed to strengthen the independent media's capacity to identify and respond to disinformation, regardless of whether it originates from external or domestic political actors or the grey zone between the two. In the Western Balkans, domestic political actors and media owners close to parties in power are often key sources of disinformation. This means that resilience cannot be directed only at foreign manipulation threats. Therefore, the division of labour within EU institutions reflects this interplay between domestic disinformation and FIMI. While DG-level bodies focus on long-term capacity and institution building, the EEAS is responsible for daily monitoring, content analysis, and crisis management related to FIMI campaigns. The system is imperfect, and the boundaries are sometimes blurred; however, it demonstrates an attempt to cover the full spectrum of threats with corresponding instruments.

²⁶ Interview 5: An interview with an EU representative, 12/05/2026.

²⁷ Interview 7: An interview with an EU representative, 13/05/2026.

²⁸ Interview 6: An interview with an EU representative, 13/05/2026.

²⁹ Interview 7: An interview with an EU representative, 13/05/2026.

For those whose job is to fact-check political speech inside EU institutions, disinformation circulates through identifiable actors, traceable networks, and recognisable patterns. The European Parliament has proven to be particularly fertile ground.³⁰ Far-right and, to a lesser extent, far-left MEPs have been observed amplifying false or manipulated information — sometimes knowingly, sometimes through failure to verify before sharing. The motivations differ: some MEPs appear to be ‘sources’ of narratives that align with Russian strategic interests. Others seem to deploy disinformation opportunistically, tailoring ready-made claims to fit a pre-existing Eurosceptic agenda. In either case, the effect is similar - a false or misleading claim gains institutional legitimacy when it passes through a political speech, press release, or social media account of an elected representative, and becomes harder to refute.

Fact-checkers working in Brussels report that when they trace the sources behind a claim circulating in parliamentary discourse, they often find links to low-follower social media accounts with no profile pictures, no biography, and no organic engagement, features that are typical for bot activities. Two Russian-linked networks, known in the monitoring community as Matryoshka and Storm-1516, have been identified as key amplification infrastructures (European Digital Media Observatory 2025). They artificially increase view counts and facilitate the circulation of certain narratives. From there, the content migrates upward through high-follower accounts with political agendas, through MEPs who pick it up without verification, and finally, into the media ecosystem. Thus, MEPs are not the origin point but a node of amplification in most cases. In this way, narratives that emerge through bots or disinformation platforms online acquire a human face and are legitimised through speeches in the European Parliament.³¹

Brussels-based journalists interviewed for this research said that it is difficult to challenge politicians directly over their use of disinformation in speeches. Fact-checkers who have attempted to contact MEPs for comments ahead of publication describe experiences of deliberate delays in response. For instance, press offices promise a response within days and then deliver it after the journalistic deadline has passed. This is not seen as accidental but as a strategy, as such situations occur quite often. By the time a correction could be made, the original false claim had already completed its circulation cycle. According to the interviewees, there is a difference between the press services of the various EU institutions, where they have contacts for each policy area, and they are described as highly responsive. The European Commission and the European External Action Service are seen as institutions with a reputational interest in a rapid response if the information needs to be corrected. On the other hand, the European Parliament presents a more complicated picture, as some politicians have an interest in the original narrative remaining unchallenged.³²

For experts and journalists who closely follow the work of EU institutions in Brussels, the topics that attract the most resilient and sophisticated FIMI activities are the war in Ukraine and EU enlargement. As one of them stated: “whenever a country moves visibly closer to the EU, through a summit, an accession milestone, or the election of a pro-European government, bot networks activate and disinformation spikes.”³³ Armenia is the most recent example where the pro-Western government of the centrist Civil Contract Party won the election in June 2026 despite the large-scale disinformation campaign in favor of the Kremlin that targeted the Armenian digital space in the weeks before the vote. In just one week in June, a Russia-linked disinformation campaign spread 31 fake news stories about Armenian Prime Minister Nikol Pashinyan, accusing him of election fraud and trying to drag Armenia into war with Russia (International Society for Human Rights, 2026). 343 fake videos were published in early May, making such an operation one of the most extensive in recent years. The election campaign

³⁰ Interview 4: An interview with a fact checker, 14/05/2026.

³¹ Interview 4.

³² Interview 4: An interview with a fact checker, 14/05/2026.

³³ Interview 4.

occurred against the backdrop of increasing cooperation between the EU and Armenia, exemplified by the first EU-Armenia summit held in the country a month before the vote. (European Council 2026). Russia's public suggestion that Armenia risks the fate of Ukraine precisely because it is getting closer to Europe is an established narrative that aims to make EU integration appear dangerous rather than beneficial. Therefore, EU Enlargement is a key policy target for FIMI.

The most telling example of how disinformation operations reach Brussels comes from journalists' experiences. Reporters covering EU affairs have found their voices, images, and editorial material cloned, manipulated, and repurposed to say things that they never said.³⁴ In cases referred to in the interviews, the AI-generated audio replicated the voice of the journalist, including their accent. Promotional videos from credible broadcasters have been taken, edited, and given fabricated voiceovers that direct audiences to false conclusions.

Fake versions of news logos, visual templates, and even entire broadcast formats have been constructed to spread disinformation while undermining the trust that real outlets have built over years. The pipeline for this material runs through Telegram channels that function as distribution hubs for the material. Such channels amplify fake content attributed to AFP, the BBC, Euronews, and others in a single account before spreading it across platforms, where view counts are then artificially inflated to make them look viral. For media organisations, the damage is difficult to quantify and nearly impossible to contain. It is often impossible to identify the source. Meanwhile, reputational harm spreads among audiences who never encounter the correction of a certain piece of disinformation. This is the lived professional reality of Brussels-based correspondents, fact checkers, and generally critical voices within the EU bubble. According to some interviewees, it reshapes what it means to report and be trusted for their work.

³⁴ Interview 4.

Conclusion

Over the first months of 2026, EU policies have been consistently the target of FIMI attacks, with most attention being paid to the EU's stances and actions related to the war in Ukraine, energy security, and digital sovereignty, and less to defence, where the role of NATO is more often used in FIMI campaigns. There is a need for strengthened institutional coordination across the European External Action Service (EEAS), the European Commission, and the European Parliament, especially concerning sensitive policies.

This analysis shows how FIMI has been perceived, monitored, and analysed by relevant teams across the EEAS and the European Commission, the European Parliament, and what the overall cycle of disinformation spread and consumption within the Brussels bubble is. The study finds that tackling FIMI is no longer seen as a job for communicators and analysts alone. Since FIMI is part of a broader arsenal of hybrid warfare tools, the response increasingly involves securitisation. The EU's own architecture reflects this. EEAS StratCom and the East StratCom Task Force emerged partly from a security logic (post-Crimea 2014), sitting within foreign-policy/security structures rather than media regulation bodies. This is because FIMI activities are not just information threats, and in some cases, they can have potential legal violations that can trigger sanctions against the individuals and networks involved.

However, to trace individuals directly participating in the spread of disinformation remains a challenge. The EU has already frameworks that can be applied to individuals and entities involved in disinformation, including the cyber sanctions regime (Regulation 2019/796) that allows for asset freezes and travel bans targeting those responsible for cyber operations. Russia-specific restrictive measures have established a precedent for naming disinformation actors, including media figures, under EU sanctions. Strategic communication is crucial for preventing the effects of FIMI, but if there are no legal or financial consequences for running a disinformation campaign, the cost of doing so remains very low.

In the long term, building societal resilience in both EU member and candidate states means that the EU should engage with the “proliferation and fragmentation of perceived realities” facilitated by technology, as democratic institutions and democracy itself cannot sustain themselves without “some degree of shared reality” (EuropeanCommission., Joint Research Centre et al. 2026). Thus, the implementation and enforcement of already adopted legislation must go hand in hand with additional steps towards digital sovereignty, such as encouraging alternative business models and overcoming echo chambers on social media.

Disclaimer on the use of AI tools:

In preparing this manuscript, the author used *Transkriptor* to transcribe the interviews and *Jenni.ai* to assist with language improvements. All content decisions, including the interpretation of sources and the final written output were made independently by the author. The tools were used responsibly, and all the data collected for this research were protected.

Recommendations

Athanasίου, Athanasios, Klimentini Diakomanoli, Athanasios Athanasίου, and Klimentini Diakomanoli. 2025. "Disinformation and Electoral Integrity in the Digital Age: Evidence From the Elections in the EU and the USA." *Https://Services.Igi-Global.Com/Resolvedoi/Resolve.Asp?Doi=10.4018/979-8-3373-1037-4.Ch010*, ahead of print. Disinformation-and-electoral-integrity-in-the-digital-age. <https://doi.org/10.4018/979-8-3373-1037-4.ch010>.

Benoist, Sandrine (The Conversation). 2024. "French Tractor Protests Are the Latest Rebellion of EU Farmers against Unfair Competition and Red Tape – Will Their Strategy Pay Off?" January 31. <https://doi.org/10.64628/AAK.mg4axskk7>.

Bentzen, Naja. 2026. "The European Democracy Shield: An Overview." *Epthinktank*, January 15. <https://epthinktank.eu/2026/01/15/the-european-democracy-shield-an-overview/>.

Berkane, Louise. 2026. "Propaganda Machine: Secret Documents Reveal Russia's Foreign Influence Strategy across Three Continents." *Forbidden Stories*, February 14. <https://forbiddenstories.org/propaganda-machine-secret-documents-reveal-russias-foreign-influence-strategy-across-three-continents/>.

Ciampaglia, Giovanni Luca, Alessandro Flammini, and Filippo Menczer. 2015. "The Production of Information in the Attention Economy." *Scientific Reports* 5 (1): 9452. <https://doi.org/10.1038/srep09452>.

Csernaton, Raluca. 2025. *The EU's AI Power Play: Between Deregulation and Innovation*. May 20. <https://carnegieendowment.org/europe/research/2025/05/the-eus-ai-power-play-between-deregulation-and-innovation>.

Deutsche Welle. 2026. "Pro-Russian 'Doppelgänger' Campaign Exploits DW Brand." Deutsche Welle, January 4. <https://corporate.dw.com/en/hungary-election-pro-russian-doppelganger-campaign-exploits-dw-brand/a-76626398>.

Directorate-General for Enlargement and Eastern Neighbourhood. 2025. "Special Eurobarometer and Perception Surveys - Enlargement and Eastern Neighbourhood." European Commission, February 9. https://enlargement.ec.europa.eu/news/special-eurobarometer-and-perception-surveys-2025-09-02_en.

Dubóczy, Peter, and Dávid Dinič. 2022. "DISINFORMATION: Pro-Russian Disinformers Blame European Sanctions for High Energy Prices." September 12. <https://www.freiheit.org/central-europe-and-baltic-states/pro-russian-disinformers-blame-european-sanctions-high-energy>.

EDMO. 2026. "Monthly Fact-Checking Brief No. 55 Is Out." *EDMO*, January 19. <https://edmo.eu/publications/monthly-fact-checking-brief-no-55-is-out/>.

EEAS. 2026a. "#OurVoiceOurFuture | EEAS." European External Action Service. https://www.eeas.europa.eu/eeas/ourvoiceourfuture-2024_en.

EEAS. 2026b. "The Common Security and Defence Policy: A Reliable Global Anchor." European External Action Service, July 24. https://www.eeas.europa.eu/eeas/common-security-and-defence-policy-reliable-global-anchor_en.

ENR. 2026. "Thousands of Farmers Protest Mercosur Deal in Front of EU Parliament." Europe in Brief. *European Newsroom*, January 21. <https://europeannewsroom.com/thousands-of-farmers-protest-mercosur-deal-in-front-of-eu-parliament/>.

European Commission. 2025a. "Commission Fines X €120 Million under the Digital Services Act | Shaping Europe's Digital Future." May 12. <https://digital-strategy.ec.europa.eu/en/news/commission-fines-x-eu120-million-under-digital-services-act>.

European Commission. 2025b. "Digital Omnibus Regulation Proposal | Shaping Europe's Digital Future." November 19. <https://digital-strategy.ec.europa.eu/en/library/digital-omnibus-regulation-proposal>.

European Commission & High Representative of the Union for Foreign Affairs and Security Policy. 2025. *An International Digital Strategy for the European Union - Diplo Resource*. May 6. <https://www.diplomacy.edu/resource/an-international-digital-strategy-for-the-european-union/>.

European Commission. Joint Research Centre, Mario Scharfbillig, Stephan Lewandowsky, et al. 2026. *Fractured Reality*. EUR. Publications Office of the European Union. <https://doi.org/10.2760/9358883>.

European Council, Council of the European Union (Consilium). 2026. "EU-Armenia Summit." May 4. <https://www.consilium.europa.eu/en/meetings/international-summit/2026/05/04-05/eu-armenia/>.

European Digital Media Observatory (EDMO). 2025. "Storm-1516, the pro-Russian Disinformation Operation Threatening the Public Debate." <https://edmo.eu/publications/storm-1516-the-pro-russian-disinformation-operation-threatening-the-public-debate/>.

European Digital Media Observatory. 2026a. *EDMO-Horizontal-55*. European Digital Media Observatory.

European Digital Media Observatory. 2026b. *EDMO-Horizontal-56*. European Digital Media Observatory.

European Digital Media Observatory. 2026c. *Monthly Brief No. 58 – EDMO Fact-Checking Network*. European Digital Media Observatory.

European Digital Media Observatory. 2026d. *Monthly Brief No. 59 – EDMO Fact-Checking Network*. European Digital Media Observatory.

European External Action Service. 2026. *4th EEAS Report on Foreign Information Manipulation and Interference Threats*. European External Action Service.

European Parliament. 2026a. "A New EU Approach to the Sahel Region | Think Tank | European Parliament." June 29. [https://www.europarl.europa.eu/thinktank/en/document/EXPO_STU\(2026\)783618](https://www.europarl.europa.eu/thinktank/en/document/EXPO_STU(2026)783618).

European Parliament (Epthinktank.Eu). 2026b. "The European Democracy Shield: An Overview." January 15. <https://epthinktank.eu/2026/01/15/the-european-democracy-shield-an-overview/>.

EUvsDisinfo (EUvsDisinfo). 2026a. "Disinfo: Epstein Case Shows the West Refuses to Investigate Crimes

Involving Global Elites.” June 2. <https://euvsdisinfo.eu/report/epstein-case-shows-the-west-refuses-to-investigate-crimes-involving-global-elites/>.

EUvsDisinfo (EUvsDisinfo). 2026b. “Disinfo: France Is about to Ban VPN and Transform the EU in an Informational Concentration Camp.” February 19. <https://euvsdisinfo.eu/report/france-is-about-to-ban-vpn-and-transform-the-eu-in-an-informational-concentration-camp/>.

EUvsDisinfo (EUvsDisinfo). 2026c. “Disinfo: Freedom of Expression in the West Is a Myth.” March 13. <https://euvsdisinfo.eu/report/freedom-of-expression-in-the-west-is-a-myth/>.

Fonte, Giuseppe. 2025. “Italy Has Resolved Dispute with ECB over Gold Reserves, Treasury Sources Say.” Business. *Reuters*, December 11. <https://www.reuters.com/business/italy-has-resolved-dispute-with-ecb-over-gold-reserves-treasury-sources-say-2025-12-11/>.

Furlong, Ray. 2025. “What’s Fueling Bulgaria’s Biggest Protests In Decades?” February 12. <https://www.rferl.org/a/bulgaria-protests-anger-corruption-budget-government/33610871.html>.

Gineikyte-Kanclere, Vaida, Militsa Eggert, Goda Skiotyte, and Visionary Analytics. 2025. “European Software and Cyber Dependencies.” European Parliamentary Research Service, Strategic Foresight and Capabilities Unit, December.

Humprecht, Edda, Frank Esser, and Peter Van Aelst. 2020. “Resilience to Online Disinformation: A Framework for Cross-National Comparative Research.” *The International Journal of Press/Politics* 25 (3): 493–516. <https://doi.org/10.1177/1940161219900126>.

International Society for Human Rights. 2026. “Anatomy of Manipulation: The 2026 Election in Light of the Facts.” June 15. <https://ishr.org/armenia-anatomy-of-manipulation/undefined>.

Léderer, András. 2026. “Flash Report Ahead of the 2026 Hungarian Parliamentary Elections.” *Hungarian Helsinki Committee*, April 1. <https://helsinki.hu/en/flash-report-ahead-of-the-2026-hungarian-parliamentary-elections/>.

Lynn, Barry, Phillip Longman, and Anita Jain. 2025. *Courtney C. Radsch Max von Thun*. Open Markets Institute.

Marocico, Oana, and Seamus Mirodan. 2025. *How Russian-Funded Fake News Network Aims to Disrupt European Election - BBC Investigation*. September 21. <https://www.bbc.com/news/articles/c4g5kl0n5d2o>.

Organisation for Security and Cooperation in Europe. 2025. *Moldova’s Parliamentary Elections Were Competitive but Campaign Marred by Cyberattacks, Illegal Funding and Disinformation, International Observers Say | OSCE Office for Democratic Institutions and Human Rights*. <https://odihr.osce.org/odihr/598219>.

POLITICO (POLITICO). 2025. “Russia Spending Hundreds of Millions to Buy Moldova’s Election, President Warns.” September 22. <https://www.politico.eu/article/moldova-election-russian-interference-maia-sandu/>.

Ponniah, Kevin, and Lazara Marinkovic. 2019. *The Night the US Bombed a Chinese Embassy*. May 6. <https://www.bbc.com/news/world-europe-48134881>.

Proto, Lucas, Paula Lamoso-González, and Luis Bouza García. 2025. *The EU's FIMI Turn: How the European Union External Action Service Reframed the Disinformation Fight | Article | Media and Communication*. 13. <https://www.cogitatiopress.com/mediaandcommunication/article/view/9474>.

Roozenbeek, Jon, Claudia R. Schneider, Sarah Dryhurst, et al. 2020. "Susceptibility to Misinformation about COVID-19 around the World." *Royal Society Open Science* 7 (10): 201199. <https://doi.org/10.1098/rsos.201199>.

Russia Today (RT International). 2025. "EU Plotting Ukraine-Style Coup in Serbia – Moscow." September 15. <https://www.rt.com/russia/624676-eu-plotting-ukraine-style-coup-serbia/>.

Shapiro, Carl, and Hal R. Varian. 2010. *Information Rules: A Strategic Guide to the Network Economy*. Nachdr. Harvard Business School Press.

Synergy Research Group. 2025. "European Cloud Providers' Local Market Share Now Holds Steady at 15%." July 24. <https://www.srgresearch.com/articles/european-cloud-providers-local-market-share-now-holds-steady-at-15>.

About EUROPEUM

EUROPEUM Institute for European Policy is a non-profit, non-partisan, and independent think-tank focusing on European integration and cohesion. EUROPEUM contributes to democracy, security, stability, freedom, and solidarity across Europe as well as to active engagement of the Czech Republic in the European Union. EUROPEUM undertakes original research, organizes public events and educational activities, and formulates new ideas and recommendations to improve European and Czech policy making. We are the recipient of institutional funding from the European Commission under the Citizens, Equality, Rights and Values (CERV) programme.



Co-funded by
the European Union

