

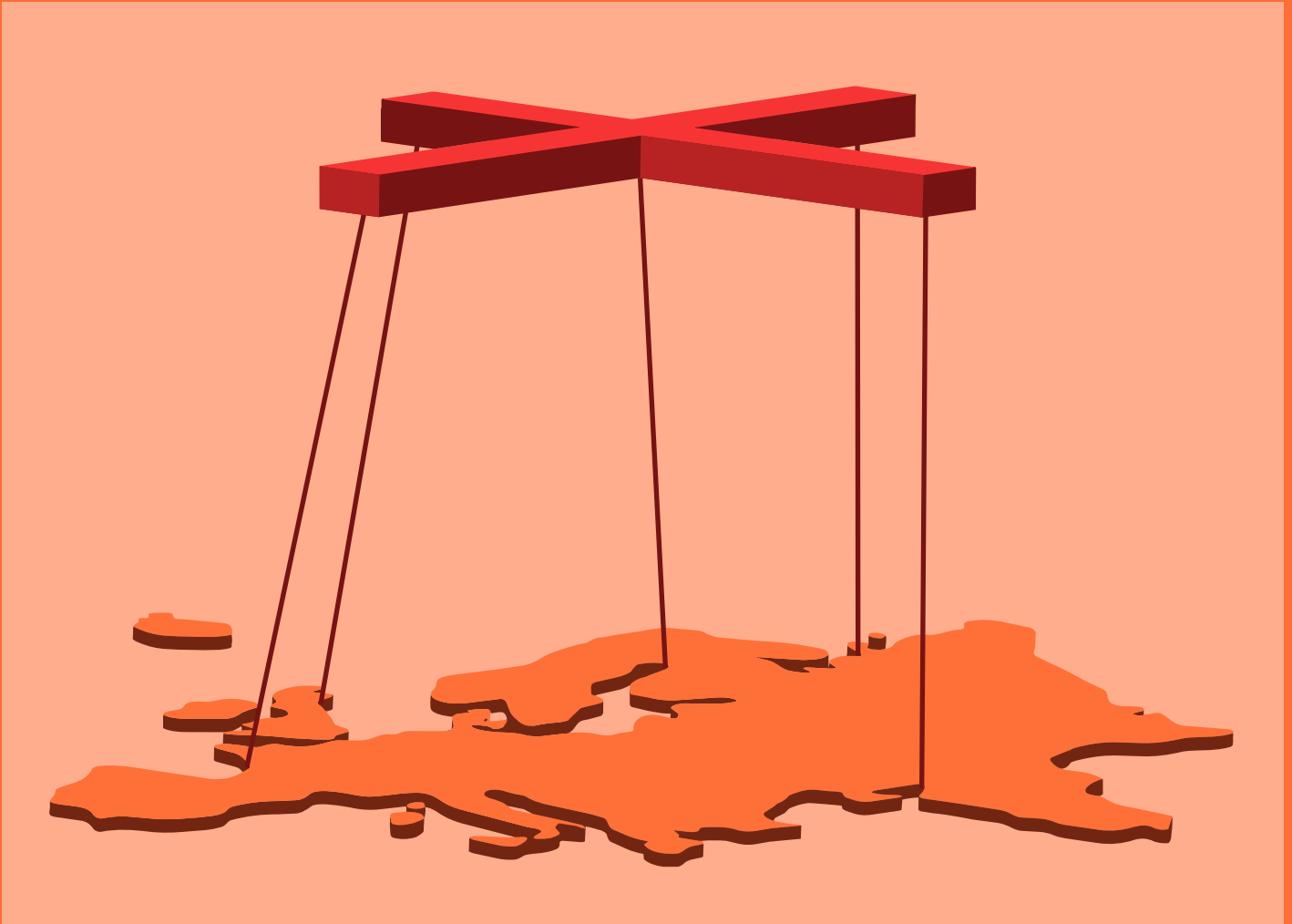


**FRIEDRICH NAUMANN
FOUNDATION** For Freedom.
Human Rights Hub



POLITICAL CAPITAL
POLICY RESEARCH & CONSULTING INSTITUTE

Policy Paper
August 2026



Richárd Demény

Mapping the Future of Political Disinformation in Europe

Mapping the Future of Political Disinformation in Europe

Richárd Demény

Imprint

Publisher

Friedrich Naumann
Foundation for Freedom
Human Rights Hub
Rue de Vermont 37-39
1202 Geneva
Switzerland

www.freiheit.org/european-union
LinkedIn: [fnfhumanrightshub](#)

Author

Richárd Demény

Editors

Bulcsú Hunyadi
Dr. Michaela Lissowsky

Date

August 2026

Contact

Phone: +41 22 733 06 58
Fax: +49 30 69 08 81 02
E-mail: geneva@freiheit.org

Notes on using this publication

This publication is an information offer of the Friedrich Naumann Foundation for Freedom.

It is available free of charge and not intended for sale. It may not be used by parties or election workers for the purpose of election advertising during election campaigns (federal, state or local government elections, or European Parliament elections).

Table of Contents

Executive Summary	5
Introduction	9
1. Disinformation Actors in a Changing Geopolitical Environment	11
An Adversary: Russia – Distort and Divide Europe	11
A Rival: China – A Latent but Growing Challenge	14
A Threat from the Inside: EU-Internal Actors	16
A Drifting Ally: The United States	18
2. Narratives Designed to Destabilize European Societies	21
Anti-EU/NATO: Sovereignty as a Weapon	21
Anti-Establishment: Exacerbating the Loss of Trust in Institutions	23
Anti-Ukraine: Making Solidarity Feel Dangerous	25
Anti-Migration	26
Anti-"Woke": Cultural Anxiety as a Political Tool	28
Strategies for Countering Disinformation Narratives: Debunking, Prebunking and Alternative Narratives	29
3. Platform and Technology Challenges	31
Big Tech Companies	31
The Rise of New Technologies and Tactics	33
4. Institutional and Policy Responses to Disinformation	36
EU Response Mechanisms	36
National Responses to FIMI	38
Taiwanese Model	40
5. Recommendations	41
Endnotes	44

Executive Summary

The information space is set to become the most critical ideological and geostrategic battleground. Over the coming years, competition to shape public perceptions, political identities, and interpretations of reality will intensify. In this environment, the ability to control and narrate events matters more than facts themselves, creating a hotbed for disinformation. Disinformation has become one of the greatest threats to the functioning of democracy because it has the potential to erode trust in democratic processes and institutions, polarize public opinion, and render citizens unable to distinguish facts from manipulation.

The future of disinformation will be defined not simply by an increasing amount of false content and information manipulations, but by the convergence of geopolitical competition, narrative battles, emerging technologies and tactics, and the evolving role of digital platforms. Consequently, this paper takes a holistic approach to assessing the factors that will likely shape the future of disinformation in the European Union.

The EU will have to address the challenges posed by disinformation actors, both within and beyond its borders, in the changing geopolitical environment.

- **Russia will continue to pose the most immediate threat of foreign information manipulation and interference (FIMI) to the EU.** It will pursue a dual-track strategy of intensifying FIMI operations while propagating pragmatism in EU-Russia relations. These operations will target elections, escalate security tensions, exacerbate divisions between and within member states, and widen the strain in transatlantic relations.
- **China represents a more latent but growing long-term challenge.** While the focus of European attention remains on

trade and industrial policy, the scale and intensity of Chinese FIMI operations expand in the background. China will intensify its charm offensive, presenting itself as an appealing and reliable economic partner to the EU. However, it will also exacerbate transatlantic tensions and target European trade and industrial policies by pressuring EU governments and societies with a carrot-and-stick approach.

- **Domestic disinformation actors within the EU pose the most complex threat.** These actors continue to converge on a similar narrative, facilitating the cross-border diffusion and amplification of disinformation within the EU. They not only make the fight against disinformation more contentious in the EU decision-making but also use it as a campaign strategy to mobilize voters by exploiting their anxieties, grievances, and perceived threats, thereby gaining electoral advantages over the mainstream. They will target contentious policy debates related to migration, the green transition, identity, European integration, deregulation and external threats.
- **The growing transatlantic divide over disinformation is poised to become a defining feature of EU-US relations in the years ahead.** The Trump administration will continue to push the idea of “free speech,” portraying EU’s digital regulations as censorship and an attack on the U.S. economy and “natural rights”. The dispute is expected to escalate with threats of sanctions, tariffs, and export restrictions. Meanwhile, US actors may bolster EU-internal disinformation actors by legitimizing and supporting their policies and narratives.

The European mainstream will have to respond to five narrative clusters designed to destabilize the EU. These are not isolated messages, but a mutually reinforcing ecosystem. Currently, mainstream parties are losing the battle to counter these narratives.

- **Anti-EU/NATO narratives can further erode support** for the European project and trust in the transatlantic security alliance.

- **Anti-establishment narratives** will **exacerbate public distrust** of the political establishment and independent institutions, thereby undermining the functioning of democratic societies.
- The battle of strategic **narratives about Ukraine** will continue to sit at the **intersection of the EU's vision of the international world order and its most important policy debates**. Disinformation actors will link existing concerns about the cost of living, sovereignty, and migration to Ukraine-related policies.
- **Anti-migration disinformation will remain the most electorally potent disinformation tactic**. This is because migration encompasses several perceived threats, such as economic insecurity, cultural change, health concerns, and identity issues.
- Disinformation actors will exacerbate the politicization of **gender and “woke” issues** because they provide **fertile ground for tribalism and polarization**.

Political actors, institutions, the media and civil society at the EU and national levels should **prioritize prebunking over debunking** by warning citizens in advance about manipulative narratives and techniques. This preemptive exposure raises critical awareness.

Big tech and new technologies will outpace the EU regulatory framework.

- Big Tech deploys **geopolitical leverage, lobbying, and strategic withdrawal to blunt enforcement**. The Commission's Digital Omnibus proposal signals that this pressure is working.
- The rapid spread of new technologies is transforming the disinformation landscape by enabling **large-scale production, lowering production costs, accelerating distribution**, and circumventing regulations faster than democratic institutions can respond. **AI-generated content, bot networks, superspreader**

accounts, monetization of disinformation, algorithmic challenges, and generative AI-enabled chatbots pose severe challenges.

- **The effectiveness of the EU's disinformation efforts will hinge on implementation, coordination, enforcement, and adequate resources.**

The EU's efforts are reflected in online platform regulation, media literacy, a toolbox to counter FIMI, risk assessment and mitigation, and strategic communications. However, relevant EU legislation, including the Digital Services Act, the Artificial Intelligence Act, and the Transparency and Targeting of Political Advertising, largely **suffers from fragmented implementation, enforcement, and limited resources.**

- European resilience requires a firm political will to **establish a legal, political, institutional, informational and societal infrastructures** that render disinformation less effective. **This requires a whole-of-society approach¹ across member states.**
- Although most EU member states have introduced **measures to counter disinformation**, the ambition, institutional design, and implementation of these responses **vary considerably**, creating **structural vulnerabilities** across the EU. While some member states have adopted ambitious and comprehensive anti-disinformation strategies, others have only made limited progress without a coherent framework. Disinformation actors are **expected to target the member states with the most vulnerable national frameworks** through cross-border information operations.

Introduction

This policy paper examines the current state of political disinformation and explores potential future challenges. Scholars and European institutions define disinformation as the intentional distribution of misleading and harmful content for political or economic gain.² Disinformation has the potential to erode trust in democratic institutions and processes, polarize public opinion, and render citizens unable to distinguish fact from manipulation. As disinformation is often orchestrated by foreign and domestic actors, we also use the terms „foreign information manipulation and interference” (FIMI) and „domestic information manipulation and interference” (DIMI).

Disinformation is considered one of the greatest threats to the functioning of a democracy.³ It has become more sophisticated and dangerous because it is not necessarily based on completely unsubstantiated and fabricated claims but rather on a mixture of true and false information.⁴ The narration of information matters more than the facts themselves. Disinformation narratives exaggerate threats and anomalies while manipulating, distorting, and oversimplifying facts by taking them out of context and highlighting them in ways that exploit pre-existing fears and concerns. This makes manipulation more difficult to detect.

Since information manipulation does not operate in isolation, this paper takes a holistic approach to assessing the future of disinformation. First, it analyzes major actors—Russia, China, destructive EU internal actors, and the United States—in the changing disinformation landscape. Next, it addresses the five most significant disinformation narratives intended to destabilize the EU, followed by challenges related to platforms and technology. Lastly, the paper evaluates institutional and policy responses at the European and national levels and provides recommendations to counter disinformation.

With the support of the Friedrich Naumann Foundation for Freedom Europe, Political Capital prepared this paper on the future of disinformation. The research is based on desktop research, an expert policy workshop, and followed up by three interviews with experts. The policy paper consolidated the main findings.

1. Disinformation Actors in a Changing Geopolitical Environment

In order to defend its interests, protect its citizens, and safeguard its democracies, the EU must take the lead in combating disinformation from both external and internal actors. While the Trump administration has scaled back its efforts, China and Russia are waging information warfare. In this changing geopolitical environment, the EU must address its direct adversary, Russia; its growing opponent, China; and its internal destructive actors.

An Adversary: Russia – Distort and Divide Europe

Russia represents the EU's most significant external disinformation threat, seeking to destabilize individual member states and undermine the European project. The Kremlin aims to generate chaos to achieve its strategic geopolitical objectives.⁵ Its underlying logic is that Russia is unable to compete directly with the West, but it can succeed by undermining Western alliances, dividing them internally, and eroding trust in their democratic institutions, ultimately helping ensure the Putin regime's legitimacy and long-term survival. To this end, the Kremlin deploys hybrid warfare tactics strategically and opportunistically in target countries to shape events on the ground. These tactics include business ties, acts of sabotage, economic pressure, and disinformation campaigns. Information manipulation campaigns are crucial because they accompany all tactics to manage public perception.

Russia employs foreign information manipulation and interference (FIMI) as one of the fundamental tools of state power. Russian disinformation and propaganda weaponize information by tailoring FIMI operations for long-term viability and targeting specific national audiences.⁶ These operations primarily target elections following certain similar patterns. First, FIMI actors usually seek to consolidate their presence in the information space and delegitimize pro-EU or incumbent leadership. Second, they deliberately seek to sow new and exacerbate pre-existing political, ethnic, and social tensions.⁷ Third, they seek to undermine the electoral integrity.⁸ The repercussions of these disinformation campaigns extend beyond the campaign period as they have a long-lasting influence on beliefs and attitudes, even after they have been rectified.⁹ These recurring patterns form the Russian FIMI playbook for electoral influence, making future operations easier to anticipate and counter in advance.

The Kremlin's FIMI apparatus has developed a variety of strategies designed to deepen societal divisions and undermine democratic processes considered a threat to Russian strategic interests.

This apparatus, which involves covert and fabricated networks, has successfully integrated AI tools in its disinformation campaigns to accelerate its content production and increase interference activities with fewer resources. CopyCop (also known as Storm-1516)¹⁰ relies on AI tools to scale up automated creation of inauthentic websites disguised as news outlets, political parties, and even fact-checking organizations.¹¹ The Kremlin-linked bot networks, such as Overload (also known as Matryoshka) and Doppelgänger,¹² facilitate large-scale dissemination of disinformation through posts and videos that impersonate reputable news outlets.¹³ Consequently, AI-enhanced content creation and distribution ensure that disinformation narratives continually circulate within the information space of target countries.

The Kremlin has interfered in several European elections, but the impact of recent operations has diminished, and some have even backfired. Russia has used the aforementioned FIMI playbook to interfere in the electoral processes, with Russian state institutions

playing a more visible role in information manipulation operations. The Kremlin tasked the Foreign Intelligence Service with interfering in the 2025 elections in Georgia,¹⁴ Moldova, and Serbia,¹⁵ as well as the 2026 elections in Hungary,¹⁶ by releasing official statements containing disinformation narratives about EU and NATO-backed plots. Russia's military intelligence service (GRU) took a more proactive approach in the Moldovan¹⁷ and Hungarian¹⁸ elections by deploying operatives on the ground and employing troll farms and vote-buying networks. However, the effectiveness of Russian FIMI activities was significantly reduced by preemptive communications from local political figures, civil society, and investigative media.

Russia will pursue a dual-track strategy, intensifying FIMI operations while propagating pragmatism in relations. In 2025, the Kremlin recalibrated its strategy by shifting from a parallel approach to Europe and the United States to a more targeted effort on the EU.¹⁹ The Kremlin is expected to increase funding for FIMI activities as part of its 2026 budget for state-controlled media, which is set to reach €1.56 billion, a 7% increase from 2025. In 2026 and 2027, FIMI operations are highly likely to target key elections, including German state elections, the French presidential elections, and Italian and Polish parliamentary elections. In Germany, the Kremlin has escalated its efforts by undermining the governing Christian Democratic Union (CDU) and reinforcing the rising pro-Russian Alternative for Germany (AfD).²⁰ Beyond electoral interference, FIMI activities are also likely to escalate security tensions, particularly in the Baltic region, and exacerbate disputes concerning the EU's Multiannual Financial Framework (MFF) negotiations, support for Ukraine, and mounting tensions in transatlantic relations. At the same time, Russia will offer pragmatic engagement centered on restoring trade and energy relations. This „carrot and stick” approach could deepen divisions within and between member states regarding the future of relations with Russia.

Although it is impossible to prevent all Russian FIMI operations, European actors can significantly reduce their reach and effectiveness by taking a proactive, deterrence-oriented approach. Instead of merely reacting to incidents, democratic institutions, political actors, and civil

society should anticipate emerging threats and intervene before FIMI operations can reach scale.²¹ **This requires disrupting FIMI activities, raising the cost of interference, and constraining their operational space through a combination of sanctions, law enforcement, digital regulation, building societal resilience and preemptive communication strategies.** For example, in the 2026 Hungarian elections, political actors, foreign secret services, investigative journalists, and think tanks preemptively exposed attempted influence activities attributed to Russia. These activities including narrative amplification, digital propaganda, and covert influence operations. This exposure significantly reduced their persuasive power.

A Rival: China – A Latent but Growing Challenge

Although Chinese foreign manipulation largely remained in the background, the Chinese have become more active and capable of FIMI activities in Europe. Beyond relying on traditional tools such as economic sticks and carrots,²² China has, since the COVID-19 pandemic, increased FIMI activities to manage public perception abroad at scale.²³ Under the leadership of Xi Jinping, China seeks greater political and ideological assertiveness and control over how China and geopolitical developments are viewed.²⁴ Xi believes that China's rise is constrained by Western norms and interpretations. Beijing is investing in FIMI infrastructure and in an ecosystem of actors to shape narratives more closely aligned with its vision.²⁵

While seeking to present itself as a reliable global power, China is also undermining Western global influence. Chinese FIMI activities seek to promote the country's positive image and weaken Western societies by promoting the alleged superiority of Beijing's political and economic model.²⁶ The objective is to persuade Europeans that China is on the rise while the EU is in decline. These efforts also include transforming the international rule-based world order to make it more "democratic." China's FIMI goals tend to overlap with those of Russia, such as weakening the

credibility of NATO and holding NATO responsible for the war in Ukraine.²⁷ Ultimately, Chinese FIMI activities will influence European perceptions of the EU's economic strength, political clout, and ability to act collectively.

Beijing has developed a multifaceted FIMI strategy, deploying a wide range of actors to systematically embed pro-Beijing narratives in Europe's information space. Traditional FIMI activities, such as state-affiliated media messaging, diplomatic outreach, research and media partnerships, and diaspora networks, continue to shape public perception.²⁸ However, Beijing increasingly complements these overt channels with more sophisticated influence activities that utilize seemingly independent local voices and intermediaries. These activities include paying local influencers,²⁹ media outlets, and intermediaries³⁰ who lend credibility to Beijing's narratives, using synthetic amplification through bot networks,³¹ creating innocuous social media accounts³² that can later promote pro-Beijing messages, and cultivating local media outlets³³ that obscure the origin and attribution of China-driven content. By producing pro-Chinese messages locally, this strategy makes them appear pragmatic and credible while marginalizing critical views as ideologically motivated or biased. Such messaging, combined with Beijing's economic and trade leverage, could divide European governments, preventing them from producing assertive policy responses.

As EU-China trade and industrial relations intensify, Chinese FIMI operations are likely to expand in scale and intensity. The growing strain in transatlantic relations under the second Trump presidency provides Beijing with an opportunity to present itself as a neutral, pragmatic, and predictable superpower. China will launch a charm offensive to present itself as an appealing economic partner rather than an economic competitor or systemic rival. Beijing is likely to exacerbate transatlantic tensions and pressure EU governments and societies with a carrot-and-stick approach: offering economic incentives while warning of the potential costs of confrontation. Chinese FIMI activities will target European trade and industrial policies, such as EU-China trade and investment consultations.³⁴ Their goal is to dissuade European policymakers from adopting tougher trade, defense, and competition measures, reducing

dependencies on a single supplier for critical raw materials, imposing export controls, or using the anti-coercion instrument against China by portraying non-confrontation as the more reasonable, pragmatic, and economically beneficial policy choice. Additionally, they will also aim to influence key European policy debates on AI, industrial policy, critical infrastructure, and strategic supply chains.³⁵ By shaping these debates, Beijing will seek to obscure the extent to which its policies conflict with the EU's strategic interests, thereby weakening the EU's resolve to adopt a more hawkish position on China.

Member States can reduce Beijing's reach by exposing and disrupting Chinese FIMI networks. While the EU and its member states have thus far largely focused on Chinese economic, industrial, and political threats, they have given limited attention to Chinese FIMI activities.³⁶ To improve resilience against China, **European governments should strengthen their capacity to identify and publicly expose** the individuals, intermediaries, financial relationships, and distribution networks involved in Chinese information manipulation operations.³⁷ **Greater transparency requirements** for sponsored media content, influencer partnerships, and foreign-funded cooperation should make it more difficult to hide the source of China-driven narratives. Governments should also **invest in expertise on China and improve information sharing** among national authorities, researchers, journalists, and civil society to identify emerging tactics across borders. As Chinese FIMI increasingly relies on locally trusted voices and obscured attribution, exposing the infrastructure behind these operations can reduce their credibility and limit their ability to influence European policy debates.

A Threat from the Inside: EU-Internal Actors

While the EU recognizes Russian and Chinese FIMI activities,³⁸ it must also address disinformation propagated by internal actors – that is, domestic information manipulation and interference (DIMI). European actors play a crucial role in spreading and amplifying

disinformation narratives that are not necessarily coordinated with foreign manipulation efforts but often overlap with them. These actors primarily consist of radical and illiberal parties, predominantly on the right, who use disinformation as a campaign strategy to influence public opinion and gain electoral advantages against mainstream parties.³⁹ They rely on disinformation to erode societal trust and shrink the space for meaningful deliberation by oversimplifying complex issues and turning them into polarizing ideological conflicts.

DIMI actors increasingly converge on similar narratives, facilitating the cross-border diffusion of disinformation and its amplification across Europe. These actors use disinformation strategically to mobilize voters by exploiting anxieties, grievances, and perceived threats. A key source of their appeal lies in their anti-establishment and victimhood narratives. They portray themselves as outsiders who oppose the corrupt political elite that allegedly seeks to silence or marginalize them. While specific narratives are often adapted to national contexts, they reflect a broader pattern of narrative convergence enabled by transnational networks, alternative media ecosystems, and processes of mutual learning. By spreading similar anti-immigration, Eurosceptic, anti-establishment, anti-gender, anti-woke, and climate-skeptic disinformation, these actors reinforce and legitimize one another's messages, expand their reach across audiences, and strengthen a transnational illiberal information ecosystem.

The DIMI actors make the fight against disinformation more contentious in the EU. They often portray EU initiatives aimed at combating disinformation as threats to freedom of expression, political pluralism, and national sovereignty. As their presence in European and national parliaments has grown, so has their influence on legislative debates. They challenge regulatory proposals and organize opposition to anti-disinformation initiatives.

DIMI actors are expected to exploit political events and contentious policy debates to expand their political and discursive influence. The implementation of the EU Green Deal, the EU Migration and Asylum

Pact, Ukraine's accession process, and significant elections, such as the 2027 French presidential elections, will provide fertile ground for disinformation. While shared narratives will enable greater convergence, it is unlikely to result in sustained political cooperation. Regarding common themes, DIMI actors will maximize their discursive power to shape EU policies on migration, the green transition, and deregulation initiatives, such as omnibus packages. However, diverging national and party interests regarding the next Multiannual Financial Framework, enlargement, Russia, China, Ukraine, and transatlantic relations will continue to limit the extent of their cooperation. For instance, while Western DIMI actors generally oppose further enlargement and want to reduce the size of the EU's next budget, their Eastern counterparts often have different interests.

The European mainstream should challenge DIMI actors in the information space to prevent them from converting their growing discursive influence into political power. Mainstream parties should avoid legitimizing or co-opting disinformation narratives in an attempt to win over their voters. Co-opting these narratives risks normalizing polarizing framings and shifting the debate toward positions adopted by DIMI actors. Instead, mainstream parties should proactively frame political events and reframe legitimate economic and societal grievances through pre-bunking strategies that include counter- and alternative narratives.

A Drifting Ally: The United States

Donald Trump's presidential victory signaled the end of the West's common consensus to fight against disinformation. The Trump administration has scaled back its efforts to combat disinformation at home, which has implications for foreign policy that extend to the EU and its member states.⁴⁰ The administration has begun to dismantle its counter-disinformation infrastructures by shutting down the 'Counter Foreign Information Manipulation and Interference Hub' and 'the Global Engagement Center' and defunding other offices with similar duties.⁴¹

This retrenchment also involved cutting the federal funding to the Voice of America (VoA) and the United States Agency for International Development (USAID).⁴² These cuts have left severe funding gaps for numerous European media outlets, civil society organizations, and think tanks fighting disinformation and teaching media literacy.

The growing transatlantic divide over disinformation is likely to become a defining feature of EU-US relations in the coming years. The Trump administration has invoked the concept of “free speech,” particularly in the context of the EU’s efforts to combat disinformation.⁴³ Following Vice President JD Vance’s speech at the Munich Security Conference in 2025, the US has repeatedly criticized European counter-disinformation regulations, framing them as censorship and an attack on the US economy. The EU’s Digital Services Act (DSA) was portrayed as a tool to suppress freedom of speech and as a scam to censor and demonetize American companies.⁴⁴ This dispute is expected to escalate,⁴⁵ with the Trump administration’s visa bans,⁴⁶ threats of sanctions,⁴⁷ additional tariffs, and export restrictions⁴⁸ on countries that apply “discriminatory” rules against US companies. The administration has directly challenged the EU’s norm-setting in digital regulation by embedding anti-digital regulation clauses into trade agreements.⁴⁹

The Trump administration is expected to bolster DIMI actors across Europe by legitimizing and supporting their policies and narratives without clear interference. The United States has recalibrated⁵⁰ its foreign funding programs to align with the priorities outlined in the U.S. National Security Strategy,⁵¹ which calls for cultivating „resistance” to the current trajectory of the EU. The Trump administration aims to expand its reach and influence, ultimately transforming the West in its image, envisioning a “civilizational alliance” of Christian nation-states.⁵² Despite the ideological kinship, the European radical and far-right are divided over the Trump administration. Some parties, such as Fidesz and the AfD, have gravitated toward the MAGA line, while others, such as the French National Rally and Brothers of Italy, have drifted away from it.

The Trump administration's retreat from combating disinformation will force the EU to increase its efforts to counter Russian and Chinese disinformation in contested information spaces. The Trump administration has ended the cooperation with European partners to fight disinformation from Russia, China, and Iran.⁵³ The US also reduced its role in the Five Eyes Intelligence alliance, the G7's Rapid Response Mechanism, and various NATO initiatives dedicated to public diplomacy and FIMI.⁵⁴ At the same time, China and Russia rapidly seek to fill the void left by the United States. In this information environment, the EU cannot afford to stagnate and should step up as a coalition builder and global norm setter in fighting FIMI. The EU should seek enhanced cooperation through bilateral and multilateral initiatives worldwide to lead the charge against disinformation, taking over from Washington.

2. Narratives Designed to Destabilize European Societies

The EU's information space is a highly contested battleground. Five narratives – anti-EU/NATO, anti-establishment, anti-Ukraine, anti-migration, and anti-woke – are poised to dominate public discourse and the political agenda. Currently, EU institutions, member states, and mainstream parties are losing the battle of narratives. They have failed to effectively address disinformation narratives that aim to destabilize and disrupt the democratic process.

Anti-EU/NATO: Sovereignty as a Weapon

Anti-EU narratives exploit nationalist sentiment by portraying the EU as dominated by overarching institutions, globalist forces, and unelected bureaucrats, whose ultimate goal is to replace the nation-states with a “European superstate.” They emphasize national sovereignty and the perceived threats to national identity and way of life. The goal is to portray EU integration as a threat to individual European nations, while offering an alternative vision, “Europe of Nations”,⁵⁵ which is designed to emphasize national sovereignty.

Common sub-narratives include:

- **EU/NATO as tools of foreign domination:** EU institutions are reframed as the instruments of a “Brussels elite” and globalist forces that threaten not only the sovereignty of individual nations, but also their “true” national characteristics, values,

traditions, and the will of their populations. The narrative disguises opposition to EU and NATO integration as vocal skepticism about EU and NATO structures, presenting it as a legitimate act of self-determination.

- **Anti-globalist and antisemitic amplification:** Kremlin-linked and far-right networks frame European integration using anti-globalist rhetoric, often with antisemitic undertones that portray supranational governance as a project of shadowy elites. This gives the narrative emotional charge beyond conventional Euroscepticism.
- **Security institutions as threats to peace:** NATO is portrayed not as a defensive alliance but as a mechanism for drawing European countries into offensive conflicts. This sub-narrative is particularly effective in Germany, where historical memory of militarism makes populations sensitive to any framing that implicates German forces in escalatory risk.

The unchallenged spread of anti-EU and anti-NATO narratives in public discourse erodes support for the European project and trust in the transatlantic security alliance over time. Vocal criticism of the alliances has become a defining feature of many radical right and illiberal parties. For example, in Germany, the Alternative for Germany (AfD) party used AI-generated disinformation and Kremlin-linked narratives during the 2025 federal election campaign to portray NATO and the EU as threats to German sovereignty. This messaging carried antisemitic undertones and echoed anti-globalist frameworks.⁵⁶ Ultimately, AfD supporters have become 32% less likely than non-supporters to view NATO favorably (39% vs. 71%), representing one of the largest partisan gaps recorded across NATO countries.⁵⁷ Previously, pro-EU and pro-NATO stances enjoyed significant public support.

Anti-Establishment: Exacerbating the Loss of Trust in Institutions

The anti-establishment narratives capitalize on increasing public dissatisfaction and concerns about deteriorating socio-economic outlooks and the rapid technological and cultural transformation of societies. These narratives exacerbate public distrust of the political establishment and state institutions. A growing number of citizens are skeptical of the establishment's ability to provide policies and services that address their needs while upholding values such as transparency, integrity, and fairness.

Common sub-narratives include:

- **Anti-elitism, anti-institutionalism, anti-rule of law:**
These messages portray international and national elites as a powerful group that has illegitimately taken over institutions and the state for their own benefit. This messaging systematically delegitimizes independent institutions by portraying them as partisan and biased and as acting against the will of „the people“ and anti-establishment forces to serve the establishment's interests. This erodes public trust in these institutions and weakens the system of checks and balances. The most prominent vehicle for this narrative is the „deep state“ framing originating in the United States. This framing claims that an unelected bureaucratic class works against the will of the people. Hence, dismantling institutional independence is deemed a necessary step toward „democratic“ populist governance.
- **Discrediting politicians:** Deepfakes, fabricated quotes, and coordinated smear campaigns target individual mainstream, democratic politicians to undermine credibility and make accountability narratives feel hypocritical. The goal is to associate rule-of-law defenders with the corruption they claim to oppose, until voters can no longer identify a trustworthy actor.

- **Attacks on civil society and independent journalism:**
Independent media outlets and civil society organizations are portrayed as politically motivated entities that are paid to suppress inconvenient truths and delegitimize illiberal actors. By discrediting institutions that debunk disinformation, this sub-narrative removes the correction mechanism itself, allowing false claims to circulate unchallenged and making citizens less likely to trust rebuttals, even when they encounter them. In Hungary, for example, Viktor Orbán's government portrayed independent organizations as „foreign agents” of a coordinated globalist project in its campaign against „foreign funding”.⁵⁸
- **Legal exceptionalism and election fraud narratives:** Far-right populist parties across Europe have adopted the claim that elections are rigged. The persistent repetition of this claim can be enough to cast doubt on the integrity of elections, thereby undermining public trust in democratic institutions and electoral outcomes. This narrative undermines the very foundation of democratic legitimacy. In Germany, this subnarrative is amplified by claims of systematic vote manipulation and biased state media, normalizing the refusal to accept electoral results as a legitimate political stance.

This strand of disinformation narratives is likely to remain one of the most persistent threats to the integrity of democratic institutions.

It targets citizens who already harbor grievances against the political and business elites or feel that the institutional structure is incapable of providing adequate policy solutions to their problems. By eroding the credibility of institutions capable of holding power to account, this narrative clears the ground for populist alternatives that promise swift results without the constraints of democratic procedure. It is directly connected to the anti-EU/NATO cluster: both position institutions as illegitimate – one at the geopolitical level, the other at the domestic accountability level.

■ Anti-Ukraine: Making Solidarity Feel Dangerous

Disinformation narratives aim to legitimize Russia's aggression against Ukraine while also scaring off its supporters by undermining public support for Ukraine. Russia's FIMI campaigns portrayed the aggression against Ukraine as a legitimate action to defend alleged Russian security interests and the supposed rights of Russian-speaking minorities. At the same time, they depicted solidarity with Ukraine as economically self-destructive and geopolitically reckless. Those who show solidarity with Ukraine are portrayed as warmongers who are escalating tensions with Russia and threatening peace, security, and prosperity in Europe.

Common sub-narratives include:

- **Economic self-harm:** Support for Ukraine and sanctions against Russia are framed as acts of economic self-harm. Rising energy prices, inflation, and diverted public funds are directly attributed to solidarity with Kyiv. The subtext is that ordinary citizens bear the costs while political elites feel none of them.
- **Ukraine as an illegitimate state:** Ukraine is portrayed as a corrupt, unstable, or neo-Nazi-infiltrated state unworthy of European solidarity. Territorial losses are normalized as inevitable, and peace negotiations are framed as the morally responsible alternative to prolonging suffering.
- **Russia as a defensive actor:** Western expansion – via NATO enlargement and EU integration – is framed as an existential provocation, rendering Russia's military response comprehensible, if not justified. This sub-narrative functions to neutralize moral clarity about the aggressor.
- **Escalation risk:** Continued EU support is presented as dragging member states toward direct military confrontation with Russia. This narrative exploits genuine war-weariness and fears of escalation.

- **Opposition to EU accession:** Ukraine's EU membership trajectory is framed as a threat to existing member states – through competition for cohesion funds, labor migration, and agricultural market access. This sub-narrative is distinct from the war-focused clusters and targets economically anxious audiences skeptical of further enlargement.

The battle of strategic narratives about Ukraine will remain at the intersection of the EU's vision of the international order and its most important policy debates. The Kremlin will continue to see its war on Ukraine as part of a broader effort to accelerate the transition from a rule-based order to a multipolar world centered on great-power status and spheres of influence.⁵⁹ Consequently, the EU's support of Ukraine is integral to defending the broader rule-based order underpinned by sovereignty, territorial integrity, and international law.⁶⁰ Even if the intensity of the war in Ukraine changes, European governments and mainstream parties will face contentious decisions related to Ukraine, such as reconstruction costs, the country's path to EU accession, agricultural competition, migration, future relations with Russia, and the allocation of EU funds within the next MFF. These issues create opportunities for disinformation actors to link existing concerns about the cost of living, sovereignty, and migration to Ukraine-related policies.

Anti-Migration

Since migration became a prominent political issue in 2015, disinformation narratives about it have dominated public discourse. Narratives that exaggerate or generalize migrant criminality and welfare abuses have polarized public deliberation. The overpoliticization of migration has fueled anti-immigration sentiment, crowding out nuanced debates about challenges such as integration and inclusion policies, pressures on public services, and constraints on public resources.

Common anti-migration narratives include:

- **Migrants cause an increase in crime:** In 2016, Russian state media spread false claims that a 13-year-old Russian-German was abducted and assaulted by Arab migrants in Berlin. Despite German authorities disproving the claim, the right-populist party publicly supported and spread the narrative.⁶¹
- **Migrants undermine cultural cohesion and national identity:** This narrative interprets immigration as a threat to the 'native' (white) population, Western Christian culture and civilization.
- **Migrants are an economic burden:** AfD co-leader Alice Weidel claimed „two-thirds of foreigners“ in Germany receive social benefits (Bürgergeld). Despite fact-checkers at Infomigrants.net debunking the claim, it was not corrected on air and circulated widely.⁶²
- **Migrants circumvent legal systems and abuse the state's resources:** Some narratives are not exclusive to the far right; centrist parties have also adopted them. For example, CDU leader Friedrich Merz perpetuated the claim that migrants are exploiting the German social security system.⁶³
- **Immigration is expected to remain one of the most significant political divisions in the EU.** Rather than addressing misconceptions about migration, mainstream parties' adoption of anti-immigration narratives has reinforced their legitimacy and relevance. Migration remains a potent vehicle for disinformation and an effective driver of electoral mobilization because it encompasses perceived threats such as economic insecurity, cultural change, health concerns, and identity issues.

■ **Anti-"Woke": Cultural Anxiety as a Political Tool**

Anti-"woke" narratives generally reject gender and LGBTQ+ rights, particularly trans rights, under the guise of opposing modernity and defending traditional values and "normality." These narratives exacerbate voters' social and cultural anxieties in a rapidly changing world, polarizing and fragmenting social cohesion. Additionally, these narratives are part of the struggle against the „decadent and declining" liberal and left-wing ideologies and alleged oppression. In Germany, for example, far-right actors and Kremlin-linked networks deliberately amplify this dynamic by importing US frames, such as those against diversity, equity, and inclusion (DEI) policies.

Common sub-narratives include:

- **Anti-"gender ideology":** LGBTQ+ rights and gender-inclusive policy are framed as an ideological project imposed on society against its will – threatening children, erasing biological sex, and criminalizing dissent. In Germany, the right-populist party falsely framed the 2024 Self-Determination Act – which simplified legal gender recognition – as enabling predators and indoctrinating children, formalizing this claim in its 2025 manifesto.⁶⁴
- **Threat to traditional way of life:** Progressive social norms are presented as an existential threat to national identity, Christian heritage, and the traditional family. Changes to common language, liberties, and rights are treated as evidence of an assault on the traditional way of life, sustaining a permanent state of cultural emergency that far-right parties position themselves to resolve.
- **Anti-inclusion:** DEI policies in institutions and companies are framed as reverse discrimination – punishing merit, silencing majorities, and privileging identity over competence. For example, in the United States, anti-DEI campaigns and the dismantling of affirmative action have provided a high-visibility template that European far-right actors adapt directly: framing any institutional effort to address structural inequality as an ideological imposition

that harms ordinary white workers and students. Moreover, as more institutions seek compliance with the U.S., global firms operating in the EU will adjust their policies and messaging.

- **Medical disinformation:** Scientific consensus on health – particularly COVID-19 vaccines – is recast as a “woke” political project rather than evidence-based public health. Existing distrust in big pharmaceutical companies, globalism, and institutions was exploited to frame vaccination mandates and pandemic policy as liberal coercion. This sub-narrative is effective precisely because it links a concrete lived experience (the pandemic, bodily autonomy) to the broader frame of elite and corporate overreach, portraying them as seeking to profit from and exert control over ordinary citizens. Vaccine hesitancy is thus framed as a form of political resistance rather than a public health risk.

Radical right and illiberal parties will escalate the politicization of gender and “woke” themes because these issues provide fertile ground for tribalism and polarization. These disinformation narratives portray politics as a struggle between good and evil, making compromise with the other side unacceptable. Within this mindset, the alleged “gender ideology” is not just a political difference but an antagonistic opposition.

Strategies for Countering Disinformation Narratives: Debunking, Prebunking and Alternative Narratives

The EU and mainstream actors should consider moving beyond institutional responses to counter disinformation and play a more active role in shaping the information landscape. There are two primary approaches to consider:

- **Debunking:** While debunking is an effective tool to correct false claims after they have been circulated, they have a fundamental limitation. False information continues to shape beliefs and

attitudes even after it has been declared false. Corrections often fail to fully counter misinformation once it has become embedded in individuals' cognitive representations.⁶⁵ Therefore, debunking strategies may not be enough to tackle disinformation from shaping public discourse and the policy agenda.

- **Prebunking:** Prebunking functions like a psychological vaccine to enhance preparedness and societal resilience. People are warned in advance that they may be exposed to persuasive manipulation attempts, and pre-exposing them to weakened versions of common disinformation narratives can reduce the cognitive impact of those messages. Preemptive exposure to disinformation raises critical awareness while reducing the effectiveness of false claims.⁶⁶ Consequently, prebunking helps combat campaigns that constantly rotate their content while reusing the same underlying tactics (e.g., false amplification, manufactured outrage, fabricated authority), because the inoculation holds across future claims that use the same methods.
- **Alternative narratives:** Positive, values-based political communication that occupies space disinformation would otherwise fill. Rather than refuting individual claims, these narratives reframe debates and shift the discourse away from the grievances and threats exploited by disinformation actors.⁶⁷ By doing so, they can erode the appeal of false narratives and „inoculate“ electorates against disinformation.

To strengthen preparedness and societal resilience, democratic actors should adopt a preemptive strategy based on prebunking to combat disinformation.⁶⁸ Rather than attempting to correct false claims through fact-checking, European institutions, policymakers, and communicators should take proactive measures. They should systematically monitor trends and activities, establish early warning systems for rapid intervention, invest in foresight capabilities to achieve first-mover advantage, and promote compelling alternative narratives.

3. Platform and Technology Challenges

Although the EU has established an ambitious regulatory framework to counter disinformation, new technologies are outpacing it, and big tech is resisting it, resulting in enforcement gaps. The EU faces a compound risk of a rapidly shifting technological sphere without proper enforcement mechanisms. Governments and EU institutions should scale up their efforts to enforce digital regulations on big tech and adapt to emerging new technological challenges.

Big Tech Companies

Big Tech, particularly very large online platforms (VLOPs), primarily run from outside Europe, creating a complex geopolitical regulatory dynamic. Major social media platforms will challenge the EU regulatory framework with a multi-front strategy employing four tactics: geopolitical leverage, rhetorical delegitimization, open defiance, and strategic withdrawal.

- **Geopolitical leverage:** Big tech companies have aligned with the Trump administration's notion of defending "freedom of speech", using this justification to roll back their content moderation and challenge the EU's digital regulatory framework.⁶⁹ They claim that EU digital rules stifle European competitiveness and innovation and view tech fines as discriminatory "tariffs" on US companies.⁷⁰ Consequently, they lobby the administration to use maximum leverage in negotiations with the EU to secure concessions on the regulation of US-origin technology. While repealing the

DSA and Digital Markets Act entirely may be their ultimate goal, persuading the EU to soften the enforcement of these laws by changing how the rules are implemented is more feasible.⁷¹

- **Lobbying:** Big tech companies aim to influence the EU's digital regulations through lobbying. In 2025 alone, Amazon, Apple, Google, Meta, and Microsoft collectively spent over €35 million on EU lobbying, making Big Tech the largest corporate lobbying force in the EU ecosystem, surpassing finance, energy, and chemicals.⁷² Their lobbying efforts include industry messaging, astroturfing, and funding independent organizations to produce analyses that support Big Tech's positions.
- **Strategic withdrawal:** Platforms are withdrawing essential services from the EU to avoid complying with the new rules. When the EU's Regulation on the Transparency and Targeting of Political Advertising (TTPA) came into force in October 2025, Google and Meta responded by voluntarily banning political ads in the EU altogether – and Google deleted its pre-existing EU political ad archive entirely.⁷³

Big Tech will continue to succeed in watering down the EU's digital rules in weakened Europe. They will rely on the Trump administration to weaponize trade policy by portraying the digital rules as „anti-American“ and threatening retaliation. They will portray compliance as persecution rather than a legal obligation and as an obstacle to innovation and competitiveness. This strategy is working, as evidenced by the European Commission's new Digital Omnibus package proposal, which aims to simplify and soften digital regulations and address some of the American accusations.⁷⁴ The proposal will weaken the EU's ability to stand up to the coercion of Big Tech companies.

The Rise of New Technologies and Tactics

The rapid spread of new technologies is transforming the disinformation landscape by enabling large-scale production, lowering production costs, accelerating distribution, and circumventing regulations faster than democratic institutions can respond. AI-generated content has become a key instrument for the dissemination of electoral disinformation worldwide.

- **AI-generated content:** AI-generated images, videos, and audio, particularly deepfakes, are highly persuasive because they evoke strong emotional reactions – including fear, anger, or empathy – that shape perceptions more effectively and increase susceptibility to disinformation.⁷⁵ AI-generated content continues to shape judgments and beliefs even when it is exposed as false. Voice cloning represents an underappreciated dimension of the AI disinformation threat: fabricated audio is cheaper to produce than video deepfakes, harder to detect.⁷⁶ Consequently, disinformation actors increasingly rely on AI to produce and distribute false messages and narratives on social media. AI-generated videos, including those with political content, can slip through Meta’s filtering system, allowing such content to circulate as sponsored advertisements.⁷⁷
- **Synthetic amplification:** Bot networks allow disinformation actors to flood platforms with coordinated shares, likes, and reports to increase visibility.⁷⁸ Coordinated inauthentic networks can operate at a scale that exceeds human capabilities by automating interactions across numerous accounts.
- **Superspreader accounts:** Since disinformation thrives on volume, disinformation actors establish coordinated supporter networks to extend the reach of their content by mobilizing real supporters.⁷⁹ The goal is epistemic exhaustion when citizens cannot distinguish reliable from unreliable information.

- **Monetization of disinformation:** Although Meta and Google have suspended political advertising, enforcement remained imperfect. Political actors can still bypass restrictions using a range of tactics, such as continuously relaunching ads that have been removed; hiding the political nature of the content; creating false-flag pages and ads; and establishing new social media pages for the purpose of launching ads.⁸⁰ For instance, a Vietnamese AI clickbait network benefited from financial monetization and content arbitrage. They converted traffic into profit by redirecting users to ad-heavy websites via emotionally charged fake political content.⁸¹
- **Algorithmic challenges:** AI-driven recommendation systems are likely to become an increasingly influential vector for disinformation. Big Tech's recommendation algorithms remain largely opaque because they are protected as trade secrets, which limits public scrutiny and democratic oversight. As platforms integrate more AI-powered features and personalized recommendation systems, they exert greater influence over the political information available to citizens. Ahead of Germany's 2025 federal election, TikTok and X disproportionately promoted pro-AfD content to nonpartisan users.⁸²
- **Generative AI-enabled chatbots:** Generative AI chatbots are vulnerable to manipulation. The datasets used to train large language models (LLMs), such as OpenAI's ChatGPT, Google's Gemini, and Meta AI, can be biased, inaccurate, or intentionally manipulated by disinformation actors.⁸³ These actors can "pollute" the datasets with false or manipulated information "legitimized" through a network of intermediaries, which can skew algorithms and their outputs. It is high risk because some LLM companies use unpaid content to train their models, which makes it easier for malicious narratives to be embedded in training datasets. NewsGuard found that AI chatbots have already repeated Russian disinformation narratives.⁸⁴ Additionally, even users' prompts can feed disinformation into the process. As a result, AI chatbots can generate, spread, and amplify disinformation narratives.⁸⁵

→ **Although disinformation actors will rely on emerging technologies and manipulative techniques, their impact may be limited.** AI-generated content is poised to become a defining feature of political campaigns because political actors can use it to amplify existing narratives and fabricate scenarios that visually reinforce disinformation targeting opposition figures.⁸⁶ However, the use of AI has some shortcomings, such as its low public acceptance. Parties could face public backlash for using AI-generated content. While AI can accelerate tribalism by reinforcing pre-existing partisan attitudes and validating voters' perspectives and biases at scale, it is not well-suited to expanding support beyond a core voter base. Mainstream actors could further limit the effectiveness of manipulative techniques and narratives by communicating about them proactively and engaging directly with voters online and offline.

4. Institutional and Policy Responses to Disinformation

EU institutions and some member states have been at the forefront of developing policies that combat disinformation while safeguarding freedom of expression. Although these mechanisms promote convergence and cooperation within the EU, some member states have developed national policies that go beyond European frameworks.

EU Response Mechanisms

The EU has built a multi-layered but imperfect toolkit to counter disinformation campaigns. The EU efforts are reflected in online platform regulation, media literacy, a toolbox to counter FIMI, risk assessment and mitigation, and strategic communications. While the EU has several pieces of legislation relevant to information manipulation, they largely suffer from fragmented implementation, coordination challenges, limited performance measurement, and a lack of resources. These efforts primarily aim to regulate VLOPs because disinformation actors exploit them to disseminate their messages.

- **Digital Services Act (DSA):** The DSA is a powerful regulatory framework that holds VLOPs accountable for identifying and mitigating systemic risks, including disinformation, through transparency obligations and algorithmic risk assessments. However, its effectiveness is constrained by fragmented enforcement,⁸⁷ uneven implementation, persistent limitations in platform and algorithmic transparency,⁸⁸ and the growing politicization of its enforcement. The DSA is complemented

by the Code of Practice on Disinformation, which serves as guidance for VLOP's mandatory risk mitigation efforts, including demonetizing disinformation, improving advertising transparency, limiting the use of bots, and empowering researchers.

- **Artificial Intelligence (AI) Act:** The AI Act also employs a risk-based approach to regulating the use of AI.⁸⁹ The Act identifies and prohibits AI practices that pose „unacceptable risks.“ However, practices intended to influence elections and referendums are classified as „high risk“ and are subject to regulatory controls. Deepfakes and other forms of manipulative content are classified as “limited risk” and only require compliance with transparency obligations.
- **Transparency and Targeting of Political Advertising (TTPA):** The TTPA establishes detailed transparency and targeting requirements for service providers regarding political advertising.⁹⁰ To avoid these requirements, Meta and Google have banned all political advertising from their platforms. However, disinformation actors can adapt to ad bans by relying on emerging technologies and tactics (see Chapter 3.2).
- **European Digital Media Observatory (EDMO):** EDMO is a project that supports fact-checkers, researchers, and media literacy professionals in implementing and coordinating activities to counter disinformation.⁹¹ The EDMO network consists of 15 national and multinational hubs that detect, analyze and debunk disinformation, organize media literacy initiatives, and provide support to national authorities.
- **The European Democracy Shield:** The European Democracy Shield aims to complement the EU's digital rules by proposing action points covering three priority areas: information space integrity, media and elections, and societal resilience.⁹² The initiative includes new guidance on the responsible use of AI, the establishment of the European Center for Democratic Resilience to coordinate efforts to tackle FIMI, and a common

research support framework to provide access to data and advance technology. However, most of the action points are just commitments by the European Commission to improve voluntary coordination and information-sharing structures.

National Responses to FIMI

Although most EU member states have introduced measures to counter disinformation, their responses vary considerably in ambition, institutional design, and implementation. The nature of the threats keeps disinformation on the national agenda, but the way these threats are perceived leads to different policy outcomes and levels of resilience. Counter-disinformation measures include national strategy, legislative measures, institutional capacity, media literacy and societal resilience, fact-checking and civil society involvement, and strategic communications.

Although some member states have adopted comprehensive national strategies, their approaches to tackling disinformation markedly differ.⁹³ France and Germany have comprehensive national strategies combining legislative and non-legislative measures with the work of civil society and fact-checkers. The French approach is more centralized and operational under VIGINUM,⁹⁴ which is a technical and operational state service responsible for identifying and countering FIMI campaigns. The German model is more decentralized, distributing responsibilities across many actors to contribute to anti-disinformation efforts. In contrast, the Netherlands, the Nordic and Baltic countries prioritize strengthening societal resilience. The Dutch disinformation strategy is built around non-legislative measures, such as supporting media literacy and fact-checking, coupled with an active government approach. The Swedish Psychological Defense Agency⁹⁵ is dedicated to strengthening the psychological resilience of the Swedish population and to preventing and countering FIMI operations. Estonia has adopted the National Security Concept to strengthen societal resilience through strategic communications, media policy, international policy, election integrity, and media literacy. Despite

not adopting anti-disinformation legislation, Finland is one of the most resilient countries to the threats of information manipulation due to its long-standing investment in media literacy, education, institutional trust, and disinformation preparedness.

Most member states have implemented measures to counter disinformation, but have yet to develop a comprehensive strategy.⁹⁶

Belgium and Portugal have invested in improving societal resilience without adopting policies dedicated to disinformation. Italy and Ireland have adopted certain policies, but their impact is limited. Ireland's national security plan to tackle disinformation is still being developed and has yet to be implemented. Spain and Croatia have primarily invested in fact-checking initiatives, but there are shortcomings in other areas. Austria has adopted limited measures against disinformation and has struggled to develop a comprehensive national strategy. Poland has adopted some legislation and non-legislative tools to counter disinformation in areas relating to national security but has not yet developed comprehensive policies.

A small group of member states has made only limited progress in addressing disinformation challenges.⁹⁷ Greece and the Czech Republic have taken small steps to address disinformation challenges. Romania, Malta, and Hungary lack dedicated national strategies or comprehensive policy frameworks for countering disinformation.

The diverging national approaches to countering disinformation will be one of the structural vulnerabilities for the EU. While the EU's digital rules and voluntary, participatory initiatives establish a shared foundation, disparities in national strategies, institutional capabilities, and societal resilience create vulnerabilities that hostile actors may leverage through cross-border information operations targeting the weakest links within the EU. Member states should make better use of existing infrastructure and, where necessary, identify best practices from other countries and adapt them to create new strategies tailored to their own national contexts in a constantly evolving disinformation landscape.

Taiwanese Model

Taiwan has developed a coordinated and whole-of-society approach to counter disinformation. The Taiwanese government has established a team within the executive branch to oversee counter-disinformation policies and collaborate with relevant agencies and ministries, enabling rapid and coordinated responses.⁹⁸ The framework builds on the following:

- **Identification:** Taiwan emphasizes media literacy as a core tool that empowers citizens to discern disinformation and make informed decisions. Media literacy is included in the latest curriculum guidelines.
- **Debunking:** Taiwan seeks to produce and spread debunking messages as fast as possible. All debunking messages are short and humorous ("memeified"), so the audience is happy to spread them online. They are packaged using the 2-2-2 principle, which means each message can have a title of no more than 20 characters, content of no more than 200 characters, and no more than 2 images.
- **Combat:** Taiwan has tried to limit the spread of disinformation through legislation, but civil society and the judiciary have criticized the proposals, fearing they will restrict freedom of expression. The country has also faced strong opposition from social media platforms regarding regulations and transparency requirements.
- **Punishment:** Although Taiwan has introduced legislation based on punishment, it has proven to be inefficient. It has been difficult to enforce penalties because much of the disinformation is orchestrated by false accounts and foreign actors.
- **Civil society response to disinformation:** Taiwanese civil society and fact-checkers support the government's efforts but maintain their independence and distance. This creates a relationship that reinforces both sides rather than a formal partnership.

5. Recommendations

The EU is facing a complex matrix of geopolitical disinformation challenges, with different geopolitical actors requiring different policy responses.

- **Disrupt Russia:** The EU should prioritize shifting its focus from detecting and exposing Russian FIMI towards deterring it.⁹⁹ Rather than exclusively debunking the Russian disinformation campaigns, European policymakers should disrupt the infrastructures, intermediaries, and financial and technical enablers that support FIMI operations. They should seek to increase costs, target critical infrastructure, and reduce the operational space through sanctions, digital regulations, and law enforcement.
- **Raise awareness about China:** The EU should dedicate attention and resources to countering Chinese FIMI efforts and improving the resilience of European societies against Beijing's influence.¹⁰⁰ The most effective response to Chinese FIMI would be to address structural vulnerabilities. This would require stricter enforcement of platform transparency obligations, stronger detection of FIMI campaigns, and greater investment in strategic communication capabilities to challenge the spread of disinformation.
- **De-risking from the US:** While the EU should cooperate with the US where possible, it is highly uncertain that genuine collaboration on disinformation can be revived.¹⁰¹ The EU should aim to engage with the US on selective matters, such as developing technologies, creating knowledge hubs of best practices, and addressing Chinese disinformation. However, the EU should de-risk its reliance on the US to achieve digital sovereignty by building its own critical infrastructure, including digital platforms.

- **Enhance the Brussels effect:** The EU and its member states have to scale their efforts to act as a norm setter and a coalition builder in tackling disinformation.¹⁰² The EU should take up a more leadership role in the G7's Rapid Response Mechanism and enhance cooperation with its partners in Latin America and Africa, where Russian and Chinese FIMI operations are escalating. In particular, the EU should provide policy support to countries such as South Korea and Brazil that are working on DSA-inspired legislation to tackle FIMI. Lastly, the European actors should fill the gaps left by the Trump administration in multilateral frameworks, including funding, initiatives, and institutions.
- **Cooperate with media, researchers and civil society:** The EU should invest in rapid response capabilities to address emerging disinformation narratives within hours. The EU should provide funding for fact-checking, research, and civil society organizations while maintaining distance. This will help these organizations maintain public confidence in their integrity and independence, dispelling any false suspicions that they are part of a propaganda machine. Therefore, it is essential that these organizations and public institutions operate in a mutually enabling manner and cooperate to achieve shared goals.
- **Use AI to detect and analyze FIMI:** EU institutions and member states should invest in AI capabilities to detect and analyze FIMI operations at scale.¹⁰³ AI tools can support semantic analysis of text content, verify information, identify content duplication, and detect bot networks and AI-generated content.
- **Prebunking over debunking:** To combat the spread of disinformation, pro-democracy actors, institutions, the media, researchers, and civil society should prioritize prebunking over debunking. European resilience depends on establishing a cognitive and emotional infrastructure that renders disinformation less effective. At the same time, prebunking should be accompanied by efforts to dismantle the financial and logistical

infrastructure that funds disinformation operations.¹⁰⁴ Strategic communication and structural disruption are complementary and reactionary, not alternative, responses.

- **Guidelines for an effective national approach to combating disinformation:** While respecting the autonomy of Member States in this area, the EU should develop guidelines on the cornerstones of an effective, whole-of-society approach to combating disinformation at the national level. These guidelines should address the legal and institutional framework, strategic communications, and cooperation with non-state actors.
- **Guidelines for media literacy curricula development:** To promote the strengthening of critical media literacy skills across the EU, the EU should develop guidelines for the development of such curricula while recognizing the autonomy of Member States in this area.

Endnotes

- 1 Wigell, M., Mikkola H., Juntunen, T. (2021). Best Practices in the whole-of-society approach in countering hybrid threats. Brussels: European Parliament. Available at: [https://www.europarl.europa.eu/RegData/etudes/STUD/2021/653632/EXPO_STU\(2021\)653632_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2021/653632/EXPO_STU(2021)653632_EN.pdf)
- 2 Wardle, C. & Derakhshan, H. (2017). Information disorder: Toward an interdisciplinary framework for research and policymaking. Strasbourg: Council of Europe.
- 3 Bennett, W., & Livingston, S. (2020). The disinformation age. Cambridge University Press
- 4 Political Capital (2024) *Methodological Toolkit*. Political Capital. Available at: https://politicalcapital.hu/news.php?article_read=1&article_id=3404
- 5 Polyakova, A. and Boulègue, M. (2021) *The evolution of Russian hybrid warfare: Executive summary*. Center for European Policy Analysis (CEPA), 29 January. Available at: <https://cepa.org/comprehensive-reports/the-evolution-of-russian-hybrid-warfare-executive-summary>
- 6 European External Action Service (EEAS) (2026) *4th EEAS report on foreign information manipulation and interference threats*. Available at: <https://euvsdisinfo.eu/eeas-4th-fimi-threat-report-march-2026/>
- 7 Colomina, C. and Margalef, H. (2024) *Disinformation and EU enlargement: Instability and the battle of narratives in the Eastern neighbourhood*. Barcelona Centre for International Affairs (CIDOB). Available at: <https://www.cidob.org/en/publications/disinformation-and-eu-enlargement-instability-and-battle-narratives-eastern>
- 8 European External Action Service (EEAS) (2026) *4th EEAS report on foreign information manipulation and interference threats*. Available at: <https://euvsdisinfo.eu/eeas-4th-fimi-threat-report-march-2026/>
- 9 Lewandowsky, S., Ecker, U.K.H., Seifert, C.M., Schwarz, N. and Cook, J. (2012) 'Misinformation and its correction: Continued influence and successful debiasing', *Psychological Science in the Public Interest*, 13(3), pp. 106–131. Available at: https://www.researchgate.net/publication/258180567_Misinformation_and_Its_Correction_Continued_Influence_and_Successful_Debiasing
- 10 European Policy Centre (EPC) (2025) *Storm-1516: A wake-up call for Europe's cognitive defence*. European Policy Centre. Available at: <https://www.epc.eu/publication/Storm-1516-A-wake-up-call-for-Europes-cognitive-defence-650d24/>
- 11 Recorded Future (2024) *Inside the CopyCop playbook: How a Russian influence network repurposes LLM-powered content to target audiences in the US, UK, and Ukraine*. Recorded Future. Available at: <https://www.recordedfuture.com/blog/inside-the-copycop-playbook>
- 12 German Federal Foreign Office (2024) *Germany targeted by the pro-Russian disinformation campaign "Doppelgänger"*. Technical Report on an Analysis by the Federal Foreign Office Berlin: Federal Foreign Office
- 13 Institute for Strategic Dialogue (ISD) (2024) *Operation Overload's underwhelming influence and evolving tactics*. Institute for Strategic Dialogue. Available at: <https://www.isdglobal.org/digital-dispatch/operation-overloads-underwhelming-influence-and-evolving-tactics/>

- 14 EUvsDisinfo (2025) 'Russian scripts, Georgian voices: How disinformation targets the country's Western allies – the US, EU and UK – in Georgia' Available at: <https://euvsdisinfo.eu/russian-scripts-georgian-voices-how-disinformation-targets-the-countrys-western-allies-the-us-eu-and-uk-in-georgia/>
- 15 EUvsDisinfo (2025) 'The shadowy SVR openly pushes disinformation narratives' Available at: <https://euvsdisinfo.eu/the-shadowy-svr-openly-pushes-disinformation-narratives/>
- 16 Belton, C. (2026) 'To tilt Hungarian election, Russians proposed staging assassination attempt', *The Washington Post*, 21 March. Available at: <https://www.washingtonpost.com/world/2026/03/21/hungary-election-interference-russia-orban/>
- 17 Eristavi, M. (2025) 'Kremlin's Game of Thrones: Moldova's 2025 elections as Europe's hybrid war', *E&K Strategies*. Available at: <https://ekstrategies.org/articles/kremlins-game-of-thrones-moldovas-2025-elections-as-europes-hybrid-war>
- 18 Panyi, S. (2026) 'Putin's GRU-linked election fixers are already in Budapest to help Orbán', *VSquare*. Available at: <https://vsquare.org/putins-gru-linked-election-fixers-are-already-in-budapest-to-help-orban/>
- 19 European External Action Service (EEAS) (2026) *4th EEAS report on foreign information manipulation and interference threats*. Available at: <https://euvsdisinfo.eu/eeas-4th-fimi-threat-report-march-2026/>
- 20 Angelos, J. and Nöstlinger, N. (2026) 'Merz says Putin wants to boost Germany's far right', *Politico*, 9 June. Available at: <https://www.politico.eu/article/friedrich-merz-vladimir-putin-boost-russia-far-right/>
- 21 European External Action Service (EEAS) (2026) *4th EEAS report on foreign information manipulation and interference threats*. Available at: <https://euvsdisinfo.eu/eeas-4th-fimi-threat-report-march-2026/>
- 22 Karásková, I., Bachulska, A., Kelemen, B., Matura, T., Šebok, F. and Šimalčík, M. (2020) *China's sticks and carrots in Central Europe: The logic and power of Chinese influence*. Prague: Association for International Affairs (AMO). Available at: https://mapinfluence.eu/wp-content/uploads/2020/06/Handbook_Chinas-Sticks-and-Carrots-in-Central-Europe.pdf
- 23 Teitelbaum, B. (2025) *Chinese disinformation: A growing threat to the Alliance*. NATO Parliamentary Assembly. Available at: <https://www.nato-pa.int/document/2025-chinese-disinformation-report-teitelbaum-011-cdsrscs>
- 24 Bachulska, A., Karásková, I. and Szatters, K. (2025) *Borrowed mouths and laundered messages: China's influence playbook in Europe*. European Council on Foreign Relations (ECFR). Available at: <https://ecfr.eu/publication/borrowed-mouths-and-laundered-messages-chinas-influence-playbook-in-europe/#the-new-playbook>
- 25 Drinhausen, K., Stec, G., Karásková, I. and Ohlberg, M. (2023) *Image control: How China struggles for discourse power*. Mercator Institute for China Studies (MERICS). Available at: <https://merics.org/en/report/image-control-how-china-struggles-discourse-power>
- 26 Bachulska, A., Karásková, I. and Szatters, K. (2025) *Borrowed mouths and laundered messages: China's influence playbook in Europe*. European Council on Foreign Relations (ECFR). Available at: <https://ecfr.eu/publication/borrowed-mouths-and-laundered-messages-chinas-influence-playbook-in-europe/#the-new-playbook>
- 27 Karásková, I., Bachulska, A., Bērziņa-Čerenkova, U.A., Godec, T., Karindi, L., Leonte, A., Shopov, V., Szunomár, Á. and Šimalčík, M. (2022) *Backing Russia on Ukraine: China's messaging in Central and Eastern Europe*. China Observers in Central and Eastern Europe (CHOICE).

- 28 Bachulska, A., Karásková, I. and Szatters, K. (2025) *Borrowed mouths and laundered messages: China's influence playbook in Europe*. European Council on Foreign Relations (ECFR). Available at: <https://ecfr.eu/publication/borrowed-mouths-and-laundered-messages-chinas-influence-playbook-in-europe/#the-new-playbook>
- 29 Ryan, F., Ruser N., Zhang, A., and Impiobato D. (2021) *Borrowing mouths to speak on Xinjiang*. Canberra: Australian Strategic Policy Institute (ASPI). Available at: <https://www.aspi.org.au/report/borrowing-mouths-speak-xinjiang>
- 30 Karásková, I. (2023) Analysing China Radio International's tactics' Central European Digital Media Observatory (CEDMO). Available at: <https://cedmohub.eu/analysing-china-radio-internationals-tactics/>
- 31 Teitelbaum, B. (2025) *Chinese disinformation: A growing threat to the Alliance*. NATO Parliamentary Assembly. Available at: <https://www.nato-pa.int/document/2025-chinese-disinformation-report-teitelbaum-011-cdsrscs>
- 32 China Observers in Central and Eastern Europe (2025) CHOICE Newsletter: Influencers, and the influenced Available: <https://chinaobservers.eu/choice-newsletter-influencers-and-the-influenced/>
- 33 Karásková, I., (2019) How China Influences Media in Central and Eastern Europe, *The Diplomat* Available at: <https://thediplomat.com/2019/11/how-china-influences-media-in-central-and-eastern-europe/>
- 34 European Commission (2026) *Speech by President von der Leyen at the European Parliament Plenary debate on the conclusions of the special European Council meeting of 6 March 2026*. European Commission, 11 March. Available at: https://ec.europa.eu/commission/presscorner/detail/en/speech_26_1344
- 35 Bachulska, A., Karásková, I. and Szatters, K. (2025) *Borrowed mouths and laundered messages: China's influence playbook in Europe*. European Council on Foreign Relations (ECFR). Available at: <https://ecfr.eu/publication/borrowed-mouths-and-laundered-messages-chinas-influence-playbook-in-europe/#the-new-playbook>
- 36 Small, A. (2026) *The art of the swarm: Systemic rivalry with China on European terms*. European Council on Foreign Relations (ECFR). Available at: <https://ecfr.eu/publication/the-art-of-the-swarm-systemic-rivalry-with-china-on-european-terms>
- 37 Bachulska, A., Karásková, I. and Szatters, K. (2025) *Borrowed mouths and laundered messages: China's influence playbook in Europe*. European Council on Foreign Relations (ECFR). Available at: <https://ecfr.eu/publication/borrowed-mouths-and-laundered-messages-chinas-influence-playbook-in-europe/#the-new-playbook>
- 38 European External Action Service (EEAS) (n.d.) *Information integrity and countering foreign information manipulation and interference (FIMI)*. Available at: https://www.eeas.europa.eu/eeas/information-integrity-and-countering-foreign-information-manipulation-interference-fimi_en
- 39 de Dompablo J. A., (2023) *The Illiberalism of fear as a disinformation strategy*. Institute of European Democrats (IED).
- 40 De Agostini, L. (2025) 'Parting ways? Europe and the US on the disinformation frontline', in *Low trust: Navigating transatlantic relations under Trump 2.0*. Paris: European Union Institute for Security Studies (EUISS), pp. 32–37
- 41 Wong, E., 'Trump aides close State Dept. Office on Foreign Disinformation', *The New York Times*, 16 April 2025 Available at: <https://www.nytimes.com/2025/04/16/us/politics/trump-rubio-state-department-foreigndisinformation.html>

- 42 The White House, 'Continuing the reduction of the federal bureaucracy', 14 March 2025. Available at: <https://www.whitehouse.gov/presidential-actions/2025/03/continuing-the-reduction-of-the-federal-bureaucracy>
- 43 De Agostini, L. (2025) 'Parting ways? Europe and the US on the disinformation frontline', in *Low trust: Navigating transatlantic relations under Trump 2.0*. Paris: European Union Institute for Security Studies (EUISS), pp. 32–37
- 44 The White House (2025) *National Security Strategy of the United States of America*. Washington, DC: The White House
- 45 Propp, K. (2025) 'Talking past each other: Why the US–EU dispute over "free speech" is set to escalate', *Atlantic Council*, 15 August. Available at: <https://www.atlanticcouncil.org/blogs/new-atlanticist/us-eu-dispute-over-free-speech-is-set-to-escalate>
- 46 Wintour P. (2025) 'European leaders condemn US visa bans as row over 'censorship' escalates', *The Guardian*, 24 December. Available at: <https://www.theguardian.com/technology/2025/dec/24/macron-eu-condemn-us-visa-bans-row-censorship-escalates>
- 47 Pamuk H. (2025) 'Trump administration weighs sanctions on officials implementing EU tech law, sources say', *Reuters*, 26 August. Available at: <https://www.reuters.com/world/us/trump-administration-weighs-sanctions-officials-implementing-eu-tech-law-sources-2025-08-26/>
- 48 Bloomberg (2025) 'Lutnick says deal on EU metal tariffs depends on changes to digital rules', *Bloomberg*, 24 November. Available at: <https://www.bloomberg.com/news/newsletters/2025-11-24/lutnick-says-deal-on-eu-metal-tariffs-depends-on-changes-to-digital-rul>
- 49 Nguyen, D. M. N., and Luck, P. (2025) 'A new containment doctrine? How the United States is using trade to stop digital regulation', *Center for Strategic and International Studies (CSIS)*, 18 September. Available at: <https://www.csis.org/analysis/new-containment-doctrine-how-united-states-using-trade-stop-digital-regulation>
- 50 Mathiesen, K., Solletty, M., Ross, T., Eccles, M., Nöstlinger N. 'MAGA-friendly European think tanks get Trump funding', *Politico*. Available at: <https://www.politico.eu/article/maga-friendly-european-think-tanks-donald-trump-funding/>
- 51 The White House (2025) *National Security Strategy of the United States of America*. Washington, DC: The White House
- 52 U.S. Department of State (2026) *Agency Strategic Plan for Fiscal Years 2026–2030*. Washington, DC: U.S. Department of State. Available a
- 53 Mackinnon, A., 'US ends international push to combat fake news from hostile states', *Financial Times*, 8 September 2025 (<https://www.ft.com/content/d31b56e3-aca9-4ee7-af5a-abec74830455>)
- 54 De Agostini, L. (2025) 'Parting ways? Europe and the US on the disinformation frontline', in *Low trust: Navigating transatlantic relations under Trump 2.0*. Paris: European Union Institute for Security Studies (EUISS), pp. 32–37
- 55 Panyi, S. (2025) 'The Heritage Foundation, MCC and Ordo Iuris: How a transatlantic conservative network is reshaping Europe.' *VSquare*. Available at: <https://vsquare.org/heritage-foundation-mcc-ordo-iuris-russia-european-union-european-court-of-justice/>
- 56 Global Disinformation Index (GDI) (2025) *State of disinformation in Germany – June 2025*. Global Disinformation Index, 13 September. <https://www.disinformationindex.org/research/2025-09-13-state-of-disinformation-germany-june-2025/>

- 57 Hernandez Ramones, S. (2024) 7 facts about Germany's AfD party. *Pew Research Center* <https://www.pewresearch.org/short-reads/2024/09/20/7-facts-about-germanys-afd-party/>
- 58 European Federation of Journalists (EFJ) (2026) 'Hungary: EFJ calls on the new political leaders to restore media pluralism', *European Federation of Journalists*, 13 April. Available at: <https://europeanjournalists.org/blog/2026/04/13/hungary-efj-calls-on-the-new-political-leaders-to-restore-media-pluralism/>
- 59 Cooley, A. (2025) 'Russia stakes global ambitions on regional dominance', in Vinjamuri, L. (ed.) *Competing visions of international order*. London: Chatham House
- 60 Homolar, A. and Turner, O. (2024) 'Narrative alliances: The discursive foundations of international order', *International Affairs*, 100(1), pp. 203–220. Available at: <https://academic.oup.com/ia/article/100/1/203/7506707>
- 61 Chan, M. (2016). 'German Girl, 13, Admits to Lying About Migrant Rape Claim.' *TIME* February 1. Available at: <https://time.com/4202091/germany-migrant-rape/>
- 62 MacGregor, M. (2024) 'Fact Check: False and Misleading Claims by AfD's Alice Weidel in German TV Interview.' *InfoMigrants* July 16. Available at: <https://www.infomigrants.net/en/post/58420/fact-check-false-and-misleading-claims-by-afds-alice-weidel-in-german-tv-interview>.
- 63 Karnitschnig, M. (2022). 'German Conservative Leader Accuses Ukrainian Refugees of 'Welfare Tourism.' *Politico*. September 27. <https://www.politico.eu/article/german-conservative-leader-accuses-ukrainian-refugees-of-welfare-tourism/>
- 64 Office of the United Nations High Commissioner for Human Rights (OHCHR) (2024) 'Germany: Gender self-ID law fails to address implications for women and girls, says UN expert' *OHCHR*, 17 October. Available at: <https://www.ohchr.org/en/press-releases/2024/10/germany-gender-self-id-law-fails-address-implications-women-and-girls-says>
- 65 Rai, R., Sharma, R., and Meena, C., (2025). "IPSR Model: Misinformation Intervention through Prebunking in Social Systems." arXiv:2502.12740. Preprint, arXiv, July 9. Available at: <https://arxiv.org/html/2502.12740v1>
- 66 Kupferschmidt, K. (2024). "Can People Be 'Inoculated' against Misinformation?" *Science*, October 31. Available at: <https://www.science.org/content/article/can-people-be-inoculated-against-misinformation>
- 67 Neidhardt, A.-H. and Butcher, P. (2021) *From debunking to prebunking: How to get ahead of disinformation on migration in the EU*. Foundation for European Progressive Studies (FEPS). Available at: <https://feps-europe.eu/publication/770-fear-and-lying-in-the-eu-fighting-disinformation-on-migration-with-alternative-narratives/>
- 68 Neidhardt, A.-H. (2022) *Disinformation on refugees from Ukraine: Boosting Europe's resilience*. European Policy Centre (EPC). Available at: <https://www.epc.eu/publication/Disinformation-on-refugees-from-Ukraine-Boosting-Europes-resilience-4c56f8/>
- 69 Anti-Defamation League (ADL) (2025) 'Alarming proliferation of antisemitism and extremism on Instagram, new ADL report finds' *Anti-Defamation League*. Available at: <https://www.adl.org/resources/press-release/alarming-proliferation-antisemitism-and-extremism-instagram-new-adl-report>
- 70 Haeck, P. (2025) 'Meta chief to lobby EU on tech, AI, fines and marketplace' *Politico*. Available at: <https://www.politico.eu/article/meta-chief-lobby-eu-tech-artificial-intelligence-fines-marketplace-joel-kaplan/>

- 71 Benson, E. (2025) 'U.S.-EU tech tensions: Escalation or diffusion?'. *Center for Strategic and International Studies (CSIS)*, 10 September. Available at: <https://www.csis.org/analysis/us-eu-tech-tensions-escalation-or-diffusion>
- 72 Norigami, M., Silva, M. (2026) *How Big Tech framed EU choices*. Centre for Research on Multinational Corporations (SOMO). Available at: <https://www.somo.nl/how-big-tech-framed-eu-choices/>
- 73 Meta (2025) 'Ending political, electoral and social issue advertising in the EU'. *Meta*, 25 July. Available at: <https://about.fb.com/news/2025/07/ending-political-electoral-and-social-issue-advertising-in-the-eu>
- 74 Torreblance, J. I. (2025) Thrown under the omnibus: How the EU's digital deregulation fuels US coercion'. *European Council on Foreign Relations (ECFR)*. Available at: <https://ecfr.eu/article/thrown-under-the-omnibus-how-the-eus-digital-deregulation-fuels-us-coercion/>
- 75 Demény, R., Krekó, P., Molnár, Cs., Tilistyák, A., and Bleyer-Simon, K. (2026). *Synthetic Influence: Deepfakes and Artificial Intelligence in the Hungarian Election Campaign*. Political Capital Available at: https://politicalcapital.hu/news.php?article_read=1&article_id=3679
- 76 Romanishyn, A., Malytska, O., and Goncharuk, V., (2025). "AI-Driven Disinformation: Policy Recommendations for Democratic Resilience." *Frontiers in Artificial Intelligence* 8 (July): 1569115. Available at: <https://www.frontiersin.org/journals/artificial-intelligence/articles/10.3389/frai.2025.1569115/full>
- 77 Political Capital (2025) *The Houdini Ads: How political advertising circumvents Meta's EU ban*. Political Capital. Available at: https://politicalcapital.hu/pc-admin/source/documents/HDMO_PC_TheHoudiniAds_251219.pdfpolitical
- 78 Political Capital (2026). Political campaigning on social media in the "post-reality" and post-advertisement era: Lessons from Hungary's 2026 election campaign. Political Capital. Available at: https://politicalcapital.hu/news.php?article_read=1&article_id=3687
- 79 Political Capital (2026) *Political campaigning on social media in the „post-reality” and post-advertisement era: Lessons from Hungary's 2026 election campaign* Political Capital. Available at: https://politicalcapital.hu/news.php?article_read=1&article_id=3687
- 80 Political Capital (2026) *Political campaigning on social media in the “post-reality” and post-advertisement era: Lessons from Hungary's 2026 election campaign* Political Capital Available at: https://politicalcapital.hu/news.php?article_read=1&article_id=3687
- 81 Political Capital (2026) 'Vietnam-linked AI clickbait network spreads fake political content in Europe'. Political Capital, 26 May. Available at: https://politicalcapital.hu/news.php?article_read=1&article_id=3699
- 82 Global Witness (2025) 'TikTok and X recommend pro-AfD content to non-partisan users ahead of the German elections'. *Global Witness*. Available at: <https://globalwitness.org/en/campaigns/digital-threats/tiktok-and-x-recommend-pro-afd-content-to-non-partisan-users-ahead-of-the-german-elections/>
- 83 Bentzen, N. (2025). *Information Manipulation in the Age of Generative Artificial Intelligence*. European Parliamentary Research Service December. Available at: [https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI\(2025\)779259](https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2025)779259)
- 84 Huet, N., Sadeghi, M., and Labbe, C. (2025). Russian propaganda campaign targets France with AI-fabricated scandals. *NewsGuard*. Available at: <https://www.newsguardtech.com/special-reports/russian-propaganda-campaign-targets-france-with-ai-fabricated-scandals/>

- 85 Krack, N., Dutkiewicz, L. and De Meyere, J. (2025) 'Generative artificial intelligence and disinformation.' SSRN Electronic Journal. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=519299
- 86 Political Capital (2026) *Political campaigning on social media in the "post-reality" and post-advertisement era: Lessons from Hungary's 2026 election campaign* Political Capital Available at: https://politicalcapital.hu/news.php?article_read=1&article_id=3687
- 87 Jaursch, J. (2022) *The DSA draft: Ambitious rules, weak enforcement*. Stiftung Neue Verantwortung (SNV). Available at: https://www.interface-eu.org/storage/archive/files/snv_dsa_oversight.pdf
- 88 Trujillo, A., Tessa, B. and Cresci, S. (2026) 'Disarranged harmonization of transparency reporting by social media platforms under the Digital Services Act' Available at: <https://arxiv.org/html/2605.17655v1>
- 89 Demény, R., Krekó, P., Molnár, Cs., Tilistyák, A., and Bleyer-Simon, K. (2026). *Synthetic Influence: Deepfakes and Artificial Intelligence in the Hungarian Election Campaign*. Political Capital Available at: https://politicalcapital.hu/news.php?article_read=1&article_id=3679
- 90 Political Capital (2025) *The Houdini Ads: How political advertising circumvents Meta's EU ban*. Political Capital. Available at: https://politicalcapital.hu/pc-admin/source/documents/HDMO_PC_TheHoudiniAds_251219.pdf
- 91 European Digital Media Observatory (EDMO) (n.d.) *EDMO hubs*. Available at: <https://edmo.eu/about-us/edmo-hubs>
- 92 Bentzen, N. (2025). *Information Manipulation in the Age of Generative Artificial Intelligence*. European Parliamentary Research Service December. Available at: [https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI\(2025\)779259](https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2025)779259)
- 93 European Digital Media Observatory (2025) *How is disinformation addressed in the Member States of the European Union? 27 country cases*. European Digital Media Observatory (EDMO). Available at <https://edmo.eu/publications/how-is-disinformation-addressed-in-the-member-states-of-the-european-union-27-country-cases/>
- 94 VIGINUM (n.d.) *VIGINUM*. Secrétariat général de la défense et de la sécurité nationale (SGDSN). Available at: <https://www.sgdsn.gouv.fr/viginum>
- 95 Swedish Psychological Defence Agency (n.d.) *Our mission*. Available at: <https://mpf.se/psychological-defence-agency/about-us/our-mission>
- 96 European Digital Media Observatory (2025) *How is disinformation addressed in the Member States of the European Union? 27 country cases*. European Digital Media Observatory (EDMO). Available at <https://edmo.eu/publications/how-is-disinformation-addressed-in-the-member-states-of-the-european-union-27-country-cases/>
- 97 European Digital Media Observatory (2025) *How is disinformation addressed in the Member States of the European Union? 27 country cases*. European Digital Media Observatory (EDMO). Available at <https://edmo.eu/publications/how-is-disinformation-addressed-in-the-member-states-of-the-european-union-27-country-cases/>
- 98 Kao, S-S. (2021) *Taiwan's response to disinformation: A Model for Coordination to Counter a Complicated Threat*. NBR Special Report No. 93. Seattle, WA: The National Bureau of Asian Research (NBR).
- 99 European External Action Service (EEAS) (2026) *4th EEAS report on foreign information manipulation and interference threats*. Available at: <https://euvsdisinfo.eu/eeas-4th-fimi-threat-report-march-2026/>

- 100 Bachulska, A., Karásková, I. and Szatters, K. (2025) *Borrowed mouths and laundered messages: China's influence playbook in Europe*. European Council on Foreign Relations (ECFR). Available at: <https://ecfr.eu/publication/borrowed-mouths-and-laundered-messages-chinas-influence-playbook-in-europe/#the-new-playbook>
- 101 De Agostini, L. (2025) 'Parting ways? Europe and the US on the disinformation frontline', in *Low trust: Navigating transatlantic relations under Trump 2.0*. Paris: European Union Institute for Security Studies (EUISS), pp. 32–37
- 102 De Agostini, L. (2025) 'Parting ways? Europe and the US on the disinformation frontline', in *Low trust: Navigating transatlantic relations under Trump 2.0*. Paris: European Union Institute for Security Studies (EUISS), pp. 32–37
- 103 VIGINUM (2025) *Challenges and opportunities of Artificial Intelligence in the fight against disinformation manipulation*. Secrétariat général de la défense et de la sécurité nationale (SGDSN). Available at: https://www.sgdsn.gouv.fr/files/files/Publications/20250207_NP_SGDSN_VIGINUM_Rapport%20menace%20informationnelle%20IA_EN_0.pdf
- 104 Odarchenko, K. (2025). "The Fight Against Disinformation: A Persistent Challenge for Democracy." Analysis. *Foreign Policy Research Institute*, January 24. Available at: <https://www.fpri.org/article/2025/01/the-fight-against-disinformation-a-persistent-challenge-for-democracy/>.

