



POLICY COMMENTARY

Manipulation of information as a hybrid threat: EU and the U.S. in comparative perspective

Susana Sanz-Caballero 

Legal Sciences, Universidad Cardenal Herrera-CEU, Spain
Email: ssanz@uchceu.es

(Received 13 October 2025; revised 28 February 2026; accepted 5 March 2026)

Abstract

This paper compares how the EU and the U.S. address hybrid threats, particularly the manipulation of information as a tool to undermine democracies. Hybrid threats include tactics like cyberattacks, disinformation, and electoral interference, often by foreign or non-state actors. The EU has adopted a regulatory approach, notably through the Digital Services Act (DSA) and Digital Markets Act (DMA), which impose duties on large platforms to mitigate systemic risks and enforce transparency. It combines hard and soft law tools, emphasizing human rights and co-regulation. In contrast, the U.S. prioritizes free speech, limiting government action against disinformation due to First Amendment protections. Although federal agencies play a key role in countering foreign interference, recent shifts signal a move away from fact-checking and cyber operations. The EU and U.S. face similar adversaries but diverge significantly in their strategies. This divergence may weaken democratic resilience unless efforts are coordinated and platform accountability is strengthened across both regions.

Keywords: manipulation of information; hybrid threats; European Union and United States of America; disinformation; rule of law decline

Introduction

As the global political landscape destabilizes, it becomes increasingly vital to understand how democratic states confront hybrid threats in the information environment. While the definition remains imprecise, hybrid threats generally involve covert tactics aimed at weakening democratic institutions. Hybrid strategies exploit vulnerabilities through a diverse toolkit ranging from cyber intrusions to electoral interference, sabotage, industrial espionage, energy blackmail, economic intimidation, organized crime, trafficking, manipulation of migratory movements, paramilitary involvement, legal warfare, and disinformation. Hybridity is a word that is increasingly used (Krzykowski 2018). These threats may originate both externally and internally and can be perpetrated by state actors, proxies, or independent non-state groups (Sökmen Alaca 2016; Pierro 2021; Sanz Caballero 2023; Marsh 2024; Missiroli 2025). Among them, the manipulation of information plays a particularly disruptive role (Ivancik 2022; Ivan, Chiru and Arco 2023; Barnard 2024; Pijpers 2025). Foreign influence operations spread false or misleading content that erodes democratic integrity, undermining judicial credibility, corroding public trust in institutions and media, and destabilizing systems of checks and balances. Tackling information-related hybrid threats is, therefore, not only a matter of national security but also a democratic imperative (Von der Leyen 2024).

‘Hybrid threats’ is understood here as an umbrella term describing malicious activities that combine conventional and unconventional methods (cyber, economic, informational, political, etc.) to undermine a target state, often covertly (EEAS 2018). To clarify the conceptual framework, the information domain is the environment in which many of these threats unfold; it encompasses societal trust, public opinion, and cultural values, making it a primary target for manipulation (Sweijts et al. 2021).

Within this context, information manipulation refers broadly to the act of distorting reality through either false, misleading, decontextualized, or selectively presented information to achieve a specific objective. Disinformation is a particular form of information manipulation that involves the deliberate creation and dissemination of false information – essentially, lies – with the intent to deceive. These efforts often form part of wider campaigns aimed at shaping beliefs, attitudes, and behaviors, and may also exploit identities, social divisions, or media ecosystems; such coordinated efforts are commonly referred to as information operations (European Commission 2025e).

When the attempts to manipulate information are directed at interfering with democratic processes and/or societal cohesion, and they are sponsored by foreign states, they are known as foreign information manipulation and interference, or FIMI (EEAS 2025). The EU and the U.S. are especially exposed to information manipulation challenges such as FIMI due to their openness and deep digital integration. As long-standing defenders of democratic principles, human rights, and the rule of law, both have been prime targets of well-orchestrated malign influence campaigns (Pollicino and Bietti 2019). A notable example of a hybrid threat in the U.S. information domain is the 2016 interference in the presidential election, which combined disinformation on social media, leaking of political emails, and amplification through bots to influence public opinion and undermine trust in democratic institutions. During the political campaign, hackers linked to Russian intelligence infiltrated the Democratic National Committee and leaked thousands of internal emails. The release caused major political turbulence and was widely interpreted as an effort to influence public opinion and undermine trust in democratic institutions (U.S. Department of State 2019). For its part, the EU has been confronted with hybrid threats in the form of pro-Kremlin disinformation campaigns since 2014 – especially during the annexation of Crimea and, later, following the 2022 invasion of Ukraine. These campaigns have targeted public opinion and manipulated media narratives to undermine trust in European and national institutions. For example, false reports and misleading social media posts aimed at influencing the 2019 European Parliament elections sought to delegitimize the EU and weaken support for common policies on security or migration (European Parliament 2019). These cases on both sides of the Atlantic illustrate how foreign actors use information manipulation to interfere in democracies and weaken societal cohesion. This paper analyzes the legal and strategic architecture governing the EU and U.S. respective responses to hybrid threats in the information space.

The rationale for comparing the EU and the United States is twofold. On the one hand, both share a long and well-established tradition of defending the indissoluble and mutually dependent trinity formed by the rule of law, democracy, and human rights. On the other hand, despite this common foundation, the EU and the U.S. appear to have developed markedly different approaches – particularly in recent years – when addressing attacks against that very trinity in a domain as contemporary and strategic as the information sphere. This situation calls for close examination to determine to what extent their approaches to hybrid threats in the information sector diverge, with particular attention to FIMI, as well as to identify best practices and explore how these differences might be bridged. The method adopted will begin with a legal and regulatory description and analysis of both the EU and U.S. frameworks, followed by a comparative assessment of their relevant policies and regulatory scope, and it will conclude with a set of proposed recommendations.

EU framework

In the EU, hybrid threats in the information sphere have gradually expanded, particularly through growing external interference (Bleyer-Simon 2025). The Union has crafted a relatively comprehensive, albeit diverse, array of legal and strategic instruments in response. Legally, Regulation 2022/2065, commonly known as the Digital Services Act or DSA (European Parliament and Council 2022a), represents a notable shift from previous EU approaches (Zingales 2022). Originally conceived as a directive, the DSA was ultimately adopted as a regulation in 2022. This binding legislation tackles issues such as online advertising transparency, illegal content, and disinformation. It governs how social media platforms and online intermediaries moderate content and aims to prevent the dissemination of unlawful or harmful material. Although the DSA continues to rely on cooperation with digital service providers, it now imposes specific duties on large online platforms to mitigate systemic risks, including the spread of disinformation, especially when this involves illegal content (Flonk Jachtenfuchs and Obendiek 2024; Geiger and Frosio 2024). The Regulation also introduces transparency obligations and auditing mechanisms (European Commission 2025a), reflecting a broader evolution from a self-regulatory to a co-regulatory model. Yet, these changes remain consistent with long-standing EU goals, namely, combating illegality, safeguarding human rights, and promoting consumer protection, an area formally recognized in Article 38 of the EU Charter of Fundamental Rights of 2000.

Historically, the EU has favored a soft power strategy in its dealings with online platforms, relying on voluntary commitments, partnerships, media literacy, and standard-setting instead of binding legislation (Prokopović and Vujović 2020). This approach emphasized persuasion, coordination, and consensus-building (Durach Bărgăoanu and Nastasiu 2020). The DSA represents a turning point, introducing binding rules designed to protect individual rights, even at the cost of imposing some limits on freedom of expression. Accordingly, the role of platforms has evolved: they are no longer just passive conduits. In the EU, they have become active agents responsible for enforcing human rights. What makes the DSA stand out is that it assigns platforms an explicit duty to curb harmful content in the interest of human rights protection. According to Article 52, noncompliant platforms face penalties of up to 6 percent of their global annual revenue. Thus, the EU's preference for collaboration, particularly with civil society and smaller intermediaries, now coexists with a tougher regulatory stance toward major tech companies, reflecting a shift toward risk-based regulation rooted in rights-based governance (Frosio and Geiger 2023). A clear example of this evolution is the transformation of the EU Code of Practice on Disinformation. Initially launched in October 2018 as a voluntary set of commitments signed by firms like Facebook, Google, Twitter, Mozilla, and later Microsoft and TikTok, the Code was revised in 2022. Then, in February 2025, it became part of the DSA's implementation, meaning that from July 2025 onward, the Code operates as a regulatory instrument rather than merely a voluntary one (European Commission 2025b; Panahi and Bittencourt Siqueira 2024). The first non-compliance decision under the DSA was issued on 5 December 2025, targeting X (the former Twitter). With this decision, the European Commission held the company responsible for undermining users' rights and evading accountability, imposing a fine of €120 million for breaching its transparency obligations under European legislation. Violations include the misleading design of its 'blue checkmark', insufficient transparency in its advertising repository, and the failure to provide researchers with access to public data. As concerns this 'blue checkmark' in particular, the EU complains that, on X, anyone can pay for a 'verified' status without meaningful checks, making it hard for users to assess the authenticity of accounts and content. This misleading practice exposes users to scams, impersonation, and other types of manipulation, eventually leading to FIMI. While the DSA does not require platforms to verify users, it prohibits falsely claiming that verification has occurred (European Commission 2025d). Subsequently, the Commission launched an investigation into X's AI tool Grok and X's recommender systems,

under suspicion that illegal content had been disseminated, including explicitly manipulated images (European Commission 2026).

Together with the DSA, Regulation 2022/1925, known as the Digital Markets Act or DMA (European Parliament and Council 2022b), should be mentioned. This Regulation complements the EU digital strategy by establishing a set of criteria to qualify large online platforms that the EU calls ‘gatekeepers’ – those that provide a pre-defined set of digital services (European Commission 2025c). The EU ensures gatekeepers behave online equitably and justly. With the DMA, the EU has also moved to enforcement. Article 30 imposes fines for up to 10 percent of their total worldwide turnover, where it finds that the gatekeepers did not meet their obligations. Following the implementation of this Act, in March 2024, the European Commission launched investigations against Google-Alphabet, Meta, and Apple for alleged violations of this mandatory instrument (European Commission 2024).

Beyond binding regulations, the EU also relies on soft instruments aligned with its traditional policy style. These include the European Democracy Action Plan, the Digital Education Action Plan, and the Media and Audiovisual Action Plan, initiatives that offer strategic guidance rather than enforceable mandates (European Commission 2020a; European Commission 2020b; European Commission 2023). While these tools encourage good practices and capacity building, the EU’s strategy in the information domain extends into the foreign policy realm. Key players such as the European External Action Service (EEAS) are active in identifying and countering disinformation campaigns, particularly those from foreign actors (EEAS 2025). In addition, the European Centre of Excellence for Countering Hybrid Threats, operating independently but closely linked with both the EU and NATO, supports member states through training, threat analysis, and coordination.

The EU’s framework is mixed in nature: it blends rights-based principles, preventive strategies, and soft law tools with more recent regulatory enforcement. Priorities such as data protection, digital literacy, and societal resilience reflect longstanding EU goals. Yet, this model is not without weaknesses. Its effectiveness depends heavily on national-level implementation, which varies due to differences in legal traditions, languages, and media ecosystems. These divergences can hinder coordinated action. Moreover, the EU’s strong emphasis on privacy rights, especially under the GDPR, can delay responses to subreptitious hybrid threats (Prokopovic and Vujovic 2020). This patchwork response reflects growing tensions between ‘digital sovereignty’ ambitions and the practical limits of supranational enforcement (European Parliament 2023; Turillazzi 2023).

While the former remains the EU’s general framework, a new concurring tendency is also taking shape, as the Union increasingly approaches disinformation not merely as a media or civic issue but as a geopolitical and security challenge. Whereas the EU had a clear preference for soft law for a long time, this has gradually shifted to more hard law over time (Flonk Jachtenfuchs and Obendiek 2024). Especially since the Russian aggression against Ukraine, intelligence agencies, law enforcement, and the military are progressively more involved in tackling misleading content with a more legalistic approach (Bradford 2023), reflecting the perception that false information, particularly from states like Russia, China, or Iran, can undermine European democracy and serve as a tool in global information conflicts. This shift gives disinformation an international dimension and elevates it to a strategic priority, as illustrated by the EU’s reaction to the Ukraine crisis. At the same time, the EU continues to rely on voluntary rules for digital platforms, creating a tension between strong security-oriented measures and soft, self-regulatory approaches (Casero-Ripollés et al. 2023). How this balance is resolved through the new DSA and DMA will be crucial for the success of future EU policies defending democracy. So far, the DSA and the DMA have reshaped the EU’s approach to online platform regulation, prompting major companies such as Meta and TikTok to increase transparency in how they moderate content and target advertisements, while also requiring large platforms to assess and mitigate risks related to illegal content and disinformation. For example, Facebook now provides more information on ads shown to EU users as a result of the DMA (Meta 2023), and YouTube has taken content moderation decisions

as a result of the application of the DMA (Dergacheva and Katzeenbach 2024). Yet Meta recently took the decision to stop running political, electoral, and social issue ads on its platforms (Facebook and Instagram) within the EU. This is due to what they understand as ‘unworkable requirements and legal uncertainties’ (Meta 2025) introduced by the EU’s 2024/900 Regulation on Transparency and Targeting of Political Advertising – a new piece of legislation closely related to the DSA and the DMA. As a matter of fact, the DSA and DMA also face challenges. Enforcement is uneven across member states due to differences in regulatory capacity, and smaller platforms often struggle with the compliance burden. Ambiguities in key concepts such as ‘illegal content’ or ‘systemic risk’ can lead to inconsistent application, and there is concern that platforms may remove lawful material out of caution, potentially limiting legitimate speech. While the DSA has encouraged more responsible behavior by online services, measuring concrete reductions in harmful content, such as coordinated disinformation campaigns, remains difficult. Overall, the DSA in particular has established a more transparent and accountable online environment, illustrated by improved reporting and content moderation practices, but its ultimate effectiveness will depend on persistent enforcement, cross-border coordination, and platforms’ continued commitment to addressing emerging risks (Gosztonyi 2024).

Consequently, although information manipulation and, especially, disinformation must be addressed to protect democracy and individual freedoms, the growing regulatory drive in Europe marks a shift away from its dialogue-based and collaborative approach to platform governance. As the EU introduces coercive measures and stronger obligations for platforms, even with the legitimate purpose of safeguarding the rights of the public and of vulnerable groups, the pressure to remove harmful content raises a genuine risk of censorship (Angin 2025). The fact that most online platforms used by malign actors to spread disinformation are not based in the EU is not of help. Whereas the EU has sufficient means to address the spread of information within its member states, its ability to regulate and influence non-European social media platforms and to hold them accountable is not so strong. Moreover, the EU’s new attempt to combine a civic and media-oriented framework with a more securitized one introduces an inherent tension (Casero-Ripollés et al. 2023): security actors tend to operate through hierarchical logics, which sit uneasily with the cooperative and flexible mechanisms on which co-regulation traditionally relied. In this sense, the EU’s response to new information threats could gradually erode both its preference for soft law instruments and the soft power identity that has long distinguished its approach to global digital governance.

U.S. framework

Looking at the United States, its legal and political stance differs markedly, centered on two main principles: the supreme value placed on freedom of speech and the influential role of the federal government, supported by a complex institutional framework. To begin with, the Constitution’s First Amendment protects free speech very clearly, even if the information provided is false. This limits what federal authorities can do when it comes to regulating disinformation (Keck 2024). The centrality of free speech in the United States has deep historical roots. The framers of the Constitution witnessed firsthand the dangers of censorship and political repression under British rule, where criticizing the crown could be punished, and public debate was tightly controlled. Determined to prevent such abuses, they enshrined free expression constitutionally, embedding the principle that open discussion and criticism of authority are essential to democracy (Bogen 1983). Enlightenment ideals reinforced this vision, emphasizing reason, individual liberty, and the free exchange of ideas as the foundation of a just society (Berman 1992). Over time, this commitment became a defining feature of American political culture: while different administrations may approach issues like disinformation or harmful speech in varying ways, the constitutional protection of free speech has been broadly respected, reflecting a nonpartisan belief that

democracy thrives only when citizens are free to speak, debate, and challenge power (Álvarez and Kimmelmeier 2018). As evidence of this, in 2017, the Honest Ads Act tried to introduce transparency to online political advertising, especially if it originated abroad (Goodman and Wajert 2017). The bill, however, failed to pass, largely due to concerns about free speech. A revised, more lenient version was reintroduced in 2023, but so far it has not been approved by the legislature. The U.S. position is exemplified by Section 230 of the Communications Decency Act of 1996, which grants providers and users of interactive computer services limited immunity from federal liability. Two key principles emerge: first, platforms are not legally accountable for content posted by third parties; second, platforms are permitted to moderate, remove, or label content without risking their immunity, as they are not legally classified as ‘publishers’ (Brannon and Holmes 2024).

Despite constitutional limits on regulating online content, U.S. federal agencies have taken significant steps to counter foreign interference. Agencies like the FBI, the Department of Homeland Security, and the Cybersecurity and Infrastructure Security Agency have increased their involvement, particularly since the 2016 election. They have worked to protect election infrastructure and raise public awareness about manipulation campaigns. However, coordination remains a persistent challenge. The mandates of the country’s eighteen intelligence agencies sometimes overlap, creating bureaucratic friction. Inter-agency rivalries and competition for influence can hinder a unified, timely response to hybrid threats (Committee on Oversight and Government Reform 2015). This fragmentation is often exploited by foreign actors using hybrid tactics. The very numerous U.S. social media companies also have their share, as they are relevant actors in moderating harmful content. After the Capitol riots, platforms were pushed to introduce content moderation, fact-checking, and labeling systems, and they took steps to label or remove content deemed misleading or violent, including content shared by high-ranking officials. However, allegations of censorship and political bias led to polarization (Teremetskyi et al. 2021; Alizadeh, Gilardi, Hoes et al. 2022).

In early 2025, shifts occurred in the U.S. approach to countering disinformation and cyber threats. Seeking to improve diplomatic relations with Russia, the new administration halted offensive operations led by its Cyber Command, scaling back other national security initiatives aimed at combating foreign sabotage and influence campaigns (CNN Politics 2025). Similarly, in April 2025 the new administration decided to close the U.S. State Department’s office for countering foreign disinformation (the Global Engagement Center). The decision was justified on the grounds that the office represented ‘censorship’ and that federal funds should not be used for such activities, effectively reducing institutional oversight of foreign disinformation campaigns (U.S. Department of State 2025b). In a similar vein, Executive Order 14149, titled ‘Restoring Freedom of Speech and Ending Federal Censorship’, was signed on 20 January 2025 directing in its Section 2(c) that federal agencies must not use taxpayer funds to support what the order deems censorship in Section 1, and calling into question prior efforts to supervise or moderate online speech (Trump 2025). Following this directive, the National Science Foundation announced in April 2025 that it would cancel hundreds of grants, including many focused on disinformation, deep-fake detection, election security, or media literacy (Scire 2025). The argument is that such research is no longer among the Foundation’s priorities (U.S. NSF 2025). This federal withdrawal of support puts into question the future readiness to address propaganda, disinformation campaigns, or AI-driven fake information. By abruptly halting federal funding for research on disinformation, the Foundation might be protecting online free speech, but it also risks weakening the scientific understanding of how false narratives spread, thereby undermining the ability to preserve democratic processes from manipulation (Kelley and DiMolfetta 2025). In another development, the U.S. government enacted visa restrictions targeting foreign officials implicated in efforts to suppress Americans’ speech on digital platforms (U.S. Department of State 2025a). This measure is framed as a defense of free expression and a response to growing global pressure on U.S.-based tech firms to moderate content. Together with the rollback of fact-checking and

cyber operations, these shifts mark a significant turn in U.S. policy. The current administration views many counter-disinformation initiatives as potentially infringing on civil liberties, especially freedom of speech. This shift has led to greater divergence between the U.S. and EU approaches (European Council on Foreign Relations 2025). Concurrently, major tech platforms have begun altering their policies. Meta, for instance, announced it would discontinue its U.S. third-party fact-checking program and adopt a community-driven notes model (CBN News 2025). This signals a broader pivot toward emphasizing freedom of expression over proactive content moderation, as questions persist about the platforms' democratic accountability (Bradford 2023).

How can the new developments be interpreted, and how do they relate to the previous scenario under the Biden mandate, as well as to the traditional American defense of freedom of speech? In the U.S., the approach to information manipulation has traditionally been rather lenient, reflecting the country's strong commitment to protecting free speech. However, after the 2016 elections, the Biden administration introduced some regulations in this area: it encouraged online platforms to take greater responsibility for the content they host and tasked federal agencies with investigating and neutralizing foreign campaigns that sought to manipulate public opinion. But recent developments under the second Trump administration signal a departure from this strategy. Ushering in a significant deregulatory shift – justified by the First Amendment and the right to speak freely in the public sphere without government interference – the administration frames previous regulatory efforts as an excessive intervention (Trump 2025). However, by prioritizing free expression above all else, the U.S. risks overlooking the dangers posed by both domestic and foreign manipulation of information, potentially leaving its citizens more vulnerable to hybrid threats precisely in the domain it seeks to protect.

This situation is further complicated by the fact that most of the world's largest online platforms, such as Facebook, X, and Google, are American. Domestically, this means that U.S. policies on free speech and content moderation directly shape how the majority of U.S. citizens experience and interact with information online, limiting the ability of these same platforms to intervene against harmful content. Internationally, the deregulatory approach sets a global precedent, affecting how these platforms govern information in other countries. Consequently, the American commitment to absolute free expression has both internal and external consequences, amplifying risks to democratic processes and the integrity of information at home and abroad. The changes in the U.S. political climate clearly affect the approach to addressing hybrid threats in the information sphere, not only in this country but worldwide.

EU and U.S. in comparative perspective

Both the EU and the U.S. are democracies that depend heavily on digital networks and have traditionally faced similar adversaries, including Russia, Iran, and China. In good logic, they should counter disinformation strategies designed to erode trust, inflame divisions, and destabilize their institutions. However, their approaches differ: the EU accepts some restrictions on speech, whereas in the U.S., freedom of expression is regarded as nearly inviolable. The EU attempts to balance free speech with other rights like dignity, privacy, equality, and combating hate, while the U.S. prioritizes the protection of speech itself (The Guardian 2024). The EU tends to rely on regulatory tools, multilateral cooperation, and shared values. It combines collaborative tools with hard law. The U.S. emphasizes national security, law enforcement, and intelligence gathering with more centralized federal tools but more legal constraints on content regulation. Disinformation actors often adapt their tactics accordingly, considering each state's vulnerabilities, to maximize division and distrust. For example, within the EU, disinformation actors have amplified secessionist messages, as demonstrated by the Russian interference in the illegal Catalan referendum of independence of 2017 (Lautman 2021); anti-European narratives, as evidenced by the spread of false stories alleging that EU institutions provoked the war in Ukraine (CCD 2025); and

nationalist messages, such as misleading narratives claiming that the EU aimed to destroy Hungary's national identity (Zgut-Przybylska 2024). In the United States, disinformation actors exacerbate divisions based on religion or race, for example, fabricating false narratives against Muslims or Jews, for instance, falsely claiming that Jews knew in advance about the 9/11 attacks (RTVE 2021) or that Muslims spread Covid-19 intentionally to infect Americans (Birmingham City University 2021). Topics such as migration, public health, gender, and climate change are exploited in both continents. However, in Europe, the EU's linguistic diversity adds further complexity, with campaigns tailored to local issues (for example, migration in Italy, LGBTIQ+ rights in Poland, corruption in Spain, or environmental populism in Germany). This diversity complicates efforts to detect and counter false narratives. Moreover, responses to these same threats often differ between member states, indicating a need for greater legal harmonization across the EU (Odarchenko 2025).

Both sides of the Atlantic face instability, though for different reasons. In Europe, the number of illiberal movements and governments from member states that tolerate or exploit disinformation for political purposes is increasing. Meanwhile, the U.S. is now changing its approach to disinformation. For example, public remarks by senior officials express doubt about Russian interference. Efforts to downsize the federal administration threaten the agencies and safeguards established. Online free speech is defended without limits. This creates a divergence between Europe and the U.S. in addressing disinformation: the EU insists on regulation and coordination, while the U.S. shifts toward deregulation (WSJ 2025).

However, both regions should harmonize their standards and hold social media platforms accountable. Should the world's largest democracies diverge in their approach to hybrid threats, adversaries will exploit these differences. Disinformation transcends borders, and hybrid threats in the information space are likely to persist and multiply, becoming increasingly complex and tailored. Europe and the U.S. must remain committed to democratic principles, coordinate their efforts, and remain vigilant against manipulation to build robust defenses. However, the situation today is not conducive to such collaboration. Unfortunately, the EU and the U.S. have recently acted more as competing powers than as allies in the information domain, among other areas.

The EU and the U.S., though both exposed to information manipulation as a form of hybrid threat, have adopted diverging strategies that reflect their legal, political, and cultural differences. The EU's approach rests on regulation, co-regulation, and multilateral coordination, reflecting its long-standing emphasis on fundamental rights and on the need to protect democratic institutions from systemic risks. However, since the pandemic and the invasion of Ukraine, the EU has progressively incorporated security considerations and a geopolitical perspective into this framework, thereby reinforcing a stronger hard law approach to regulating information manipulation. By contrast, the U.S. continues to exhibit reluctance to regulate the digital space, primarily due to its constitutional protections of free speech, which may limit the scope of government intervention even in the face of coordinated foreign interference.

While both actors recognize the potential destabilizing effects of disinformation, their asymmetry in legal responses and enforcement capacities could plausibly undermine joint efforts to protect the integrity of democratic systems. The EU is overtly leaning towards overregulation, whereas the U.S. is leaning towards deregulation. As hybrid threats grow increasingly sophisticated and cross-border, adversaries may exploit regulatory gaps and inconsistencies across the Atlantic. Disinformation does not respect jurisdictional boundaries, and its effectiveness may increase when responses are fragmented. Recent transatlantic tensions could reflect mutual perceptions of the other as a quasi-adversary rather than a partner, potentially complicating coordination. These tensions may have contributed to the EU's increasing focus on digital sovereignty, as it seeks greater regulatory and operational control over critical information infrastructures and platforms, independently of U.S. influence. Regulatory divergence might therefore constitute a strategic vulnerability in the face of adversaries who thrive on division.

Building greater transatlantic alignment remains advisable and could become increasingly necessary. Such alignment does not require full convergence, given the structural and constitutional constraints of each system, but both regions would likely benefit from sustained cooperation, regulatory dialogue, and the development of shared principles, particularly regarding platform accountability, algorithmic transparency, and electoral integrity. Enhanced coordination through NATO, the G7, and bilateral mechanisms involving the EEAS and the U.S. State Department could facilitate more unified responses to actors operating in the gray zone of information warfare. This may involve the systematic exchange of expertise and intelligence, regular coordination meetings, and joint initiatives aimed at identifying and countering information-related threats. As long-standing allies since the end of World War II, united by shared values and a commitment to free societies, these institutions appear well-positioned to deepen cooperation and enhance the resilience of their respective populations against strategic information operations.

Both the EU and the U.S. should also prioritize resilience. Legal measures, while important, may be insufficient without strong civic engagement, independent media, digital literacy, and public trust in institutions. As malicious actors seek to exploit societal fault lines to deepen polarization, reinforcing democratic culture appears increasingly crucial. This includes supporting journalism, fact-based public debate, and the cultivation of critical thinking skills from an early age.

Conclusions

To counter information manipulation, it is imperative to reconsider the role of online platforms, which now function as transnational gatekeepers of public discourse. The EU has initiated measures in this regard, although implementation and enforcement remain uneven, partly because these platforms are not European. The U.S., by contrast, holds a structural advantage: most of the world's most influential platforms are American, meaning the federal government could, in principle, exert more direct influence. Yet U.S. policy continues to rely heavily on self-regulation, market incentives, and the unrestricted freedom of speech, which may be insufficient to address broader public-interest and human rights concerns. This different approach might also reflect a recently emerged divergence in how policy actors in the EU and the U.S. understand what disinformation is and who is to blame for it.

Looking ahead, efforts should focus on fostering a shared understanding of platform obligations – one that protects freedom of expression while also mitigating systemic risks, including the rapid spread of disinformation, opaque moderation practices, and the commercial amplification of divisive narratives. Achieving this balance, however, remains highly challenging today, given recent administrative changes, the political will in the U.S., and the fact that the tools available to the EU and the U.S. to hold social media platforms accountable differ significantly.

The geopolitical use of information manipulation adds another layer of complexity. Hybrid operations are not solely domestic threats; they are often deployed strategically by external authoritarian regimes to erode Western influence, test institutional responses, and plausibly exacerbate transatlantic tensions. Responding effectively may therefore require integrating foreign policy, cyber diplomacy, and intelligence cooperation into legal and regulatory frameworks, something rather unlikely these days.

In brief, the EU is reinforcing its regulatory framework while the U.S. is rolling back many initiatives in the name of constitutional liberties. In parallel, threats are evolving faster than institutions: artificial intelligence, deepfakes, and algorithmic manipulation further complicate efforts to counter information-based hybrid threats. Without coordinated adaptation, current legal and institutional frameworks on both sides of the Atlantic risk becoming obsolete.

Both the EU and the U.S. must remain steadfast in defending democratic principles in the digital age. While their strategies differ, their shared values and specific vulnerabilities require stronger cooperation. Recent transatlantic tensions, partly stemming from perceptions of each other as rivals rather than partners, strain coordination and may undermine a satisfactory response. A more harmonized, rights-respecting, and forward-looking transatlantic response is essential to safeguard the democratic information environment in the years to come.

Data availability statement. This manuscript has no associated data.

Acknowledgements. An earlier version of this article was presented and discussed at the Conference ‘The European Union in an illiberal world’ organized by the Global Governance Research Group on June 3rd, 2025. The author thanks all commentators for their suggestions. The author is also grateful to Prof. Sowels (Université Panthéon-Sorbonne) for organizing the Conference and his inspiring insights.

Funding statement. This article is one of the results of the research projects PID2021-126765NB-I00 of the MICINN and CIACO/2024/191 of the GVA on the crisis of values in Europe and resilience to hybrid threats.

Competing interests. The corresponding author states that there is no conflict of interest.

Statement on AI Use. The author used ChatGPT to polish the English language and to review the final text.

References

- Alizadeh, M., Gilardi, F., Hoes, E., Klüser, K.J., Kubli, M., and Marchal, N. (2022). ‘Content moderation as a political issue: the Twitter discourse around Trump’s ban’. *Journal of Quantitative Description*, **2**, 1–44.
- Álvarez, M.J., and K Emmelmeier, M. (2018). ‘Free speech as a cultural value in the United States’. *Journal of Social and Political Psychology*, **5**(2), 707–735. <https://doi.org/10.5964/jssp.v5i2.590>
- Angm, C. (2025). ‘European Union and global experiences in combating disinformation: a comparative analysis’. *Kafkas Üniversitesi İktisadi Ve İdari Bilimler Fakültesi Dergisi*, **16**(31), 520–549. <https://doi.org/10.36543/kauibfd.2025.020>
- Barnard, S.R. (2024). *Hacking Hybrid Media: Power and Practice in an Age of Manipulation*. Oxford University Press.
- Berman, H.J. (1992). ‘The impact of the enlightenment on American constitutional law’. *Yale Journal of Law & the Humanities*, **4**(2), 311–334.
- Birmingham City University. (2021). ‘New research uncovers Covid-19 Islamophobic misinformation theories and suggests four types of Islamophobic social media posters’. 15 December 2021, available at <https://www.bcu.ac.uk/news-events/social-sciences/>. Consulted 7 December 2025.
- Bleyer-Simon, K. (2025). ‘Addressing foreign information manipulation in the context of European regulations’. Institute of Communication Studies, [Centre for Media Pluralism and Media Freedom (CMPF)]. Policy Paper. Consulted 7 December 2025, available at <https://hdl.handle.net/1814/92874>.
- Bogen, D. (1983). ‘The origins of freedom of speech and press’. *Maryland Law Review*, **42**(3), 429–465.
- Bradford, A. (2023). *Digital empires: The global battle to regulate technology*. Oxford University Press.
- Bannon, V., and Holmes, E. (2024). ‘Section 230: An Overview’. Congress.gov. 1 April 2024, Consulted 7 December 2025, available at <https://www.congress.gov/crs-product/R46751>.
- Casero-Ripollés, A., Tuñón, J., and Bouza-García, L. (2023). ‘The European approach to online disinformation: geopolitical and regulatory dissonance’. *Humanities and Social Sciences Communications* **10**(657), 1–10.
- CBN News (2025). ‘Meta is ending its fact-checking program in favor of a ‘community notes’ system similar to X’s. 7 March.
- Center for Countering Disinformation (2025). ‘Russian information operations in Poland: key narratives’. 9 October 2025. Consulted 9 December 2025, available at <https://cpd.gov.ua/en/international-threats-en/europe/russian-information-operations-in-poland-key-narratives/>
- Committee on Government Oversight and Government Reform (2015). ‘Hearing wrap up: Identifying duplicative and redundant programs within the federal government’. 15 April 2015. Consulted 14 June 2025, available at <https://oversight.house.gov/release/hearing-wrap-identifying-duplicative-redundant-programs-within-federal-government/>
- CNN Politics (2025). ‘US suspends offensive cyber operations against Russia, senior US official says. 3 March.
- Dergacheva, D., and Katzeenbach, C. (2024). ‘Copyright moderation on YouTube following the implementation of Article 17 CDSMD’. Kluwer Copyright Blog. 14 August 2024. Consulted 7 December 2025, available at <https://legalblogs.wolterskluwer.com/copyright-blog>
- Durach, F., Bărgăoanu, A., and Nastasiu, C. (2020). ‘Tackling disinformation: EU Regulation of the digital space’. *Romanian Journal of European Affairs*, **20**(1), 5–20.
- European Commission (2020a). ‘Communication ‘Digital Education Action Plan 2021–2027 Resetting education and training for the digital age’. 30 September 2020. COM/2020/624 final.

- European Commission** (2020b). 'Communication 'Europe's media in the digital decade: An action plan to support recovery and transformation'. 3 December 2020. COM/2020/784 final.
- European Commission** (2023). 'Communication on defense of democracy'. 12 December 2023. COM/2023/630 final.
- European Commission** (2024). 'Press release 25 March 2024'. Directorate-General for Competition'. Commission opens non-compliance investigations against Alphabet, Apple and Meta under the Digital Markets Act.
- European Commission** (2025a). 'The enforcement framework of the digital services act'. Consulted 12 June 2025. <https://digital-strategy.ec.europa.eu/en/policies/dsa-enforcement>
- European Commission** (2025b). 'The code of conduct on disinformation'. Consulted 12 June 2025, available at <https://digital-strategy.ec.europa.eu/en/library/code-conduct-disinformation>
- European Commission** (2025c). 'Digital markets act'. Gatekeepers, available at Consulted 12 June 2025. https://digital-markets-act.ec.europa.eu/gatekeepers_en
- European Commission** (2025d). 'Press Release 5 December 2025'. Commission fines X €120 million under the Digital Services Act. Press Release. Consulted 6 December 2025, available at https://ec.europa.eu/commission/presscorner/detail/en/ip_25_2934
- European Commission** (2025e). 'Information manipulation and misinformation'. 14 November 2025. Consulted 7 December 2025, available at https://civil-protection-humanitarian-aid.ec.europa.eu/resources-campaigns/information-manipulation-and-misinformation_en
- European Commission** (2026). Commission investigates Grok and X's recommender systems under the Digital Services Act. 26 January 2026. Consulted 28 February 2026, available at <https://digital-strategy.ec.europa.eu/en/news/commission-investigates-grok-and-xs-recommender-systems-under-digital-services-act>
- European Council on Foreign Relations**. (2025). 'Alone we stand: How Europe can counter hybrid threats in a post-transatlantic era'. 14 May. Consulted 12 June 2025, available at <https://ecfr.eu/article/alone-we-stand-how-europe-can-counter-hybrid-threats-in-a-post-transatlantic-era/>
- European External Action Service**. (2018). 'A Europe that protects: Countering hybrid threats. 13 June 2018. Consulted 12 June 2025, available at https://www.eeas.europa.eu/node/46393_en.
- European External Action Service**. (2025). '3rd EEAS report on foreign information manipulation and interference threats'. 19 March 2025.
- European Parliament** (2019). Resolution of 10 October 2019 on foreign electoral interference and disinformation in national and European democratic processes (2019/2810(RSP)).
- European Parliament** (2023). 'Report on foreign interference in all democratic processes in the European Union, including disinformation (2022/2075(INI))'. (INGE 2). 15 May 2023.
- European Parliament and Council** (2022a). 'Regulation (EU) 2022/2065 of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act)'. PE/30/2022/REV/1. OJ L 277, 27 October 2022.
- European Parliament and Council** (2022b). 'Regulation (EU) 2022/1925 of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives 2019/1937 and 2020/1828 (Digital Markets Act)'. PE/17/2022/REV/1. OJ L 265, 12 October 2022.
- Flonk, D., Jachtenfuchs, M., and Obendiek, A.** (2024). 'Controlling internet content in the EU: towards digital sovereignty'. *Journal of European Public Policy*, 31(8), 2316–2342.
- Frosio, G. and Geiger, C.** (2023). 'Taking fundamental rights seriously in the digital services act's platform liability regime'. *European Law Journal* 29(1–2), 31–77.
- Geiger, C., and Frosio, G.** (2024). 'Towards a digital constitution: how the digital services act shapes the future of online governance'. From the DMCA to the DSA. A Transatlantic Dialogue on Online Platform Regulation and Copyright. *Verfassungsbook*.
- Goodman, E., and Wajert, L.** (2017). 'The honest ads act won't end social media disinformation, but it's a start'. Consulted 12 June 2025, available at <https://ssrn.com/abstract=3064451> or <https://doi.org/10.2139/ssrn.3064451>
- Gosztonyi, G.** (2024). 'How the European Union had tried to tackle fake news and disinformation with soft law and what changed with the digital services act?'. *Frontiers of Law*, 3, 102–113.
- Ivan, C., Chiru, I., and Arco, R.** (2023). 'Hybrid security threats and the information domain: concepts and definitions', in *Routledge Handbook of Disinformation and National Security* (pp. 9–19). Routledge. <https://doi.org/10.4324/9781003190363>
- Ivancik, R.** (2022). 'On disinformation as a hybrid threat spread through social networks'. *Entrepreneurship and Sustainability Issues*, 10(1). Consulted 11 June 2025. <https://jssidoi.org/jesi/>
- Keck, T.** (2024). 'Free speech and democratic backsliding in the contemporary United States'. 29 May 2024. Consulted 7 December 2025, available at <https://doi.org/10.2139/ssrn.4353026>
- Kelley, A., and DiMolfetta, D.** (2025). 'NSF cancels over 400 grants covering disinformation, deepfakes and STEM education'. Nextgov/FCW. 22 April 2025. Consulted 10 December 2025, available at <https://www.nextgov.com/policy/2025/04/nsf-cancels-over-400-grants-covering-disinformation-deepfakes-and-stem-education/404731/>
- Krzykowski, P.** (2018). 'Hybridity of contemporary threats'. *Visnyk of the Lviv University. Series International Relations*. Issue 45.

- Lautman, O.** (2021). 'Catalonia: Where there's trouble there's Russia'. Center for European Policy Analysis. 27 September 2021. Consulted 12 June 2025, available at <https://cepa.org/article/catalonia-where-theres-trouble-theres-russia/>
- Marsh, C.** (2024). 'The grey zone and hybrid conflict. A conceptual introduction', in M. Regan and A. Sari (Eds.), *Hybrid Threats and Grey Zone Conflict: The Challenge to Liberal Democracies* (pp. 31–44). Oxford University Press.
- Meta.** (2023). 'New features and additional transparency measures as the digital services act comes into effect'. 22 August 2023. Consulted 7 December 2025, available at <https://about.fb.com/news/2023/08/new-features-and-additional-transparency-measures-as-the-digital-services-act-comes-into-effect>
- Meta.** (2025). 'Ending, political electoral and social issue advertising in the EU in response to incoming European regulation'. 25 July 2025. Consulted 7 December 2025, available at <https://about.fb.com/news/2025/07/ending-political-electoral-and-social-issue-advertising-in-the-eu/>
- Missiroli, A.** (2025). 'Hybrid threats', in S. Lucarelli and J. Sperling (Eds.), *Handbook of European Union Governance* (pp. 414–429). Edward Elgar Publishing.
- Odarchenko, K.** (2025). 'The fight against disinformation: A persistent challenge for democracy'. Foreign Policy Research Institute. 24 January 2025. Consulted 14 June 2025, available at <https://www.fpri.org/article/2025/01/the-fight-against-disinformation-a-persistent-challenge-for-democracy/>
- Panahi, T., and Bittencourt Siqueira, A.** (2024). 'The legal enforcement of codes of conduct under the digital services act'. Verfassungsblog. 3 June 2024. Consulted 13 June 2025, available at <https://verfassungsblog.de/soft-law-dsa-co-regulation/>
- Pierro, M.** (2021). 'Contemporary conflict: The role of hybrid and asymmetric threats'. *The Internationalist: Undergraduate Journal of Foreign Affairs*, 5(2), 24–39. <https://doi.org/10.17615/63b9-sf69>
- Pijpers, P.B.M.J.** (2025). 'Hybrid threats in the information environment: An international law perspective'. Consulted 12 June 2025. Amsterdam Law School Research Paper 2025–06.
- Pollicino, O., and Bietti, E.** (2019). 'Truth and deception across the Atlantic: a roadmap of disinformation in the US and Europe'. *Italian Journal of Public Law*, 11, 43.
- Prokopovic, A.M. and Vujovic, M.** (2020). 'The European approach to regulating disinformation'. *Facta Universitatis*, 18(3), 175–183.
- RTVE.** (2021). 'Así fue cómo cambió EE.UU. 20 años después'. Ataques de falsa bandera y profecías: el 11-S según las teorías de la conspiración. 11 September 2021. Consulted 7 December 2021, available at https://www.rtve.es/noticias/especial-aniversario-11s/#bLibre_1631260844151
- Sanz-Caballero, S.** (2023). 'The concepts and laws applicable to hybrid threats, with a special focus on Europe'. *Humanities & Social Sciences Communications*, 10(360), 1–8.
- Scire, S.** (2025). 'National science foundation cancels research grants related to misinformation and disinformation'. NiemanLab. 21 April 2025, available at <https://www.niemanlab.org/2025/04/national-science-foundation-cancels-research-grants-related-to-misinformation-and-disinformation/>
- Sökmen Alaca, A.I.** (2016). 'Hybrid threats and new conflicts in the international system'. *Journal of International Relations and Foreign Policy*, 4(2), 27–43.
- Sweijis, T., Zilincik, S., Bekkers, F. and Meessen, R.** (2021). 'A framework for cross-domain strategies against hybrid threats'. The Hague Centre for Strategic Studies. 12 January 2021. Consulted 7 December 2025, available at <https://hcsc.nl/report-a-framework-for-cross-domain-strategies-against-hybrid-threats/>
- Teremetskiy, Vladyslav, Tokarieva, Kseniia, Predmestnikov, Olha and Parpan, Ulyana.** (2021). 'Combating disinformation and cyber threats in the EU and US: Lessons for Ukraine'. *Journal of Legal, Ethical and Regulatory Issues* 24. Special issue.
- The Guardian** (2024). 'US leading global alliance to counter foreign government disinformation', 26 February 2024.
- Trump, D.J.** (2025). 'Executive order 14149: Restoring freedom of speech and ending federal censorship'. 20 January 2025, available at <https://www.presidency.ucsb.edu/documents/executive-order-14149-restoring-freedom-speech-and-ending-federal-censorship>
- Turillazzi, A.** (2023). 'The digital services act: an analysis of its ethical, legal, and social implications'. *Law, Innovation and Technology*, 15(1), 83–106.
- U.S. Department of State.** (2019). 'Report on the investigation into Russian interference in the 2016 Presidential election'. Volume I. Special Counsel Robert S. Mueller, III. Submitted Pursuant to 28 C.F.R. § 600.8(c). Washington, D.C. March 2019.
- U.S. Department of State.** (2025a). 'Statement: Announcement of a visa restriction policy targeting foreign nationals who censor Americans'. 28 May 2025. Consulted 14 June 2025, available at <https://www.state.gov/announcement-of-a-visa-restriction-policy-targeting-foreign-nationals-who-censor-americans/>
- U.S. Department of State.** (2025b). 'United States champions free expression, ceases censorship frameworks'. Press Statement'. Thomas "Tommy" Pigott, Principal Deputy Spokesperson. 17 September 2025. Consulted 10 December 2025, available at <https://www.state.gov/releases/office-of-the-spokesperson/2025/09/united-states-champions-free-expression-ceases-censorship-frameworks>
- U.S. National Science Foundation.** (2025). 'NSF implementation of recent executive orders'. 9 June 2025. Consulted 7 December 2025. <https://www.nsf.gov/executive-orders>

- Von der Leyen, U.** (2024). 'Statement at the European Parliament Plenary by President Ursula von der Leyen, candidate for a second mandate 2024–2029'. 18 July 2024, available at https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_24_3871
- Wall Street Journal.** (2025). 'Trump Administration Targets Europe's Digital Laws as a Threat to Basic Rights and U.S. Business'. 15 May.
- Zingales, N.** (2022). 'The DSA as a paradigm shift for online intermediaries' due diligence'. Verfassungsblog. 2 November 2022. Consulted 12 June 2025, available at <https://verfassungsblog.de/blog/>
- Zgut-Przybylska, E.** (2024). 'Pro-kremlin disinformation is distorting democracy in Central and Eastern Europe.' RevDem. The Review of Democracy, available at <https://revdem.ceu.edu/2024/10/08/pro-kremlin-disinformation-cee/> Consulted 7 December 2025.