cogitatio

The EU's FIMI Turn: How the European Union External Action Service Reframed the Disinformation Fight

Lucas Proto [1], Paula Lamoso-González [2], and Luis Bouza García [3]

[1] Department of Political Science and International Relations, Universidad Autónoma de Madrid, Spain
[2] Department of International Studies, Universidad Loyola Andalucía, Spain
[3] Department of Political Science and International Relations, Universidad Autónoma de Madrid, Spain

Correspondence: Paula Lamoso-González (aplamoso@uloyola.es)

Abstract

This article critically examines the strategic decision of the European Union External Action Service (EEAS) to reframe the concept of misinformation as Foreign Information Manipulation and Interference. The EEAS, particularly its Strategic Communications Division, has been at the forefront of combating disinformation within the EU. Initially mandated by the European Council in 2015 to counter Russian disinformation campaigns, the EEAS pioneered the framing of this complex phenomenon as an external threat, significantly shaping subsequent European perceptions and policies. While the Covid-19 pandemic and the surge of accompanying disinformation originally shifted the EU focus towards a more regulatory approach, culminating in the approval of the Digital Services Act and the Digital Markets Act, the large-scale Russian invasion of Ukraine soon after prompted a return to geopolitical considerations, reinstating both the disinformation-as-external-threat dimension and, therefore, the prominent role of the EEAS. This research argues that the EEAS, which recognizes the limitations of the EU in effectively countering the phenomenon of misinformation, adopted the framing of Foreign Information Manipulation and Interference to both make the problem more manageable and align it with its mandate. Through this reframing, the EEAS has addressed disinformation similarly to traditional security threats, such as cyberattacks, thereby aligning with existing security paradigms and the competencies and limitations granted by the EU.

Keywords

disinformation; European Union; foreign information manipulation and interference; public diplomacy; Russia

1. Introduction

As early as 1998, General Vladimir Slipchenko then Vice President of the Russian Academy of Military Sciences, anticipated that in future conflicts great attention would be paid to information confrontation, because:

> Information is a weapon just like missiles, bombs, torpedoes, etc. It is now clear that the informational confrontation becomes a factor that will have a significant impact on the future of the war themselves, their origin, course and outcome. (De Spiegeleire et al., 2011, p. 108).

These words encapsulate the Russian leadership's long-standing belief that information is not merely a tool of communication but a potent form of non-kinetic or hybrid warfare (Splidsboel Hansen, 2017). In Russian military doctrine and government strategy, disinformation is systematically employed to destabilize adversaries, manipulate public opinion, and advance geopolitical objectives. This reality garnered widespread public and academic attention following Russia's interference in the 2016 US presidential election and has become even more pivotal since Vladimir Putin initiated the full-scale invasion of Ukraine in February 2022.

In contrast, the EU recognition of disinformation as part of a form of hybrid warfare is a relatively recent development. This delayed reaction was initially attributed to the significant challenge that the concept of information as a security threat poses to the EU's foundational principles of liberal democracy and freedom of expression (Wagnsson & Hellman, 2018). The notion of weaponizing information—using it to sow discord, manipulate public opinion, and undermine democratic institutions—directly conflicts with these core values (Szostek, 2020). Consequently, the EU is often described as being caught in a catch-22 (Van Raemdonck & Meyer, 2024), as it struggles to devise policies that effectively counter disinformation without undermining the very principles it seeks to uphold.

However, the EU's so-called fight against disinformation has been framed as an external security threat from the outset. Following the European Council meeting in March 2015, held a year after Russia's annexation of Crimea, EU leaders underscored "the need to challenge Russia's current disinformation campaigns" (European Council, 2015, p. 5) in their conclusions. They called upon the High Representative of the Union for Foreign Affairs and Security Policy/Vice President of the Commission (HR/VP), in collaboration with member states and EU institutions, to "prepare an action plan on strategic communication" (European Council, 2015, p. 5).

This initial framing of disinformation as primarily an external threat, particularly emanating from Russia, played a crucial role in shaping the EU's approach towards combating this challenge. By characterizing the multifaceted phenomenon as exclusively a foreign issue, the EU required the engagement of an institution with a dedicated focus on foreign affairs, thereby establishing the European Union External Action Service (EEAS) as the primary actor responsible for combating disinformation. This strategic choice led to EEAS concentrating its efforts almost exclusively on countering "foreign destabilization" while allowing other domestic aspects of disinformation—such as the role of internal political actors, the spread of false information within member states, or the need to strengthen citizens' media literacy—to receive less attention until 2018 (European Commission, 2018; European Commission & High Representative of the Union for Foreign Affairs and Security Policy, 2018) and not to truly foster regulatory responses until the Covid-19 pandemic in 2020 (Casero-Ripollés et al., 2023). This is the result of a policy debate about the security values at risk in the online ecosystem and a struggle between different policy communities (Ördén, 2019, p. 422).

In this process, the EU defined disinformation as "verifiably false or misleading information that is created, presented, and disseminated for financial gain or to intentionally mislead the public" (European Commission, 2018, p. 3), therefore distinguishing it from "misinformation" as potentially harmful misleading content produced without intent and other forms of errors, satire, and parody, or clearly identified partisan news and opinion. This definition, which we follow in this article, aims to balance the identification of individual behaviour responsible for spreading harmful content with the complex processes of truth-finding in open societies.

It has been theorized that the lack of established procedures for addressing emerging challenges, such as digital disinformation, positions the sui generis character of the EEAS as uniquely suited to developing transformative practices through active experimentation (Hedling, 2021). We contend that this process of compartmentalization—focusing primarily on the external dimension of disinformation while allowing other aspects of the issue to be handled by different actors within the EU (see Casero-Ripollés et al., 2023)—has been crucial to the EEAS's ongoing success in shaping the agenda. While other EU institutions and member states grappled with the complexities of digital and domestic post-truth dynamics, the EEAS consistently advanced, expanded, and refined its framework for countering the hybrid threat of foreign disinformation, thereby shaping both policy and public perception in a way that aligns with its mandate and expertise.

In this context, the EEAS's recent promotion of foreign information manipulation and interference (FIMI) is particularly significant. Introduced in 2021, FIMI has increasingly featured alongside—and in some cases outright replaced—"disinformation" in EEAS communications (EEAS, 2024a). This shift has enabled the EEAS to address challenges that have hindered other EU institutions and member states from combating disinformation (Hénin, 2023). By broadening the scope to encompass all forms of manipulative behaviour that threaten democratic processes and public trust while focusing exclusively on external actors, the EEAS has crafted a framework that not only appeals to a wide range of EU decision-makers but is also versatile enough to be applied to any narrative perceived as harmful, particularly those originating from Russia.

This article argues that while the EEAS's framing of disinformation as primarily an external threat and its strategic pivot to FIMI have effectively advanced its institutional power and shaped the EU's response, this raises significant questions about its alignment with the EU's self-perception as a normative or civil power. This is part of an ongoing process of a well-known securitisation of disinformation (Casero-Ripollés et al., 2023; Szostek, 2020; Szostek & Orlova, 2024; Wagnsson et al., 2024) that has sought to address malign information influence (Wagnsson, 2020). Through an analysis of the emergence of FIMI in EEAS communications and strategy, this article explores the underlying meaning of the concept and its implications for the EU's public diplomacy.

While recent scholarship has deepened our understanding of FIMI operational dynamics (Buvarp, 2023; Morača et al., 2023; Yuskiv & Karpchuk, 2024), these studies largely explore its practical application. However, the strategic implications of the term itself and what its adoption reveals about the EU's evolving stance on disinformation remain mostly underexplored. This article seeks to fill that gap. The purpose of this article is not to dispute the existence or relevance of FIMI or the fact that Russia and other state actors may weaponize information as part of hybrid warfare. Rather, it critically examines whether the EU's adoption of this framing, albeit in an initial phase, is consistent with its core objectives and whether this approach reinforces its strategic position or risks complicating its broader diplomatic and normative aspirations.

2. What is FIMI

The concept of FIMI is rooted in efforts by the EEAS to refine its approach to disinformation and related threats. In 2020, the EEAS commissioned James Pamment of the Partnership for Countering Influence Operations at the Carnegie Endowment for International Peace to produce Future Threats, Future Solutions. This three-part series of papers aimed to provide a structured framework to inform EU policy.

These papers established a hierarchy of terms—misinformation, disinformation, influence operations, and foreign interference—each representing an increasingly severe threat (Pamment, 2020b). At the peak of this hierarchy, foreign interference is characterized as a deliberate and often aggressive attempt by foreign actors to undermine the sovereignty of democratic institutions through covert, coercive, or deceptive tactics. Notably, the EEAS was designated here as the European entity responsible for addressing this highest-level threat:

> This terminology is escalatory. Foreign interference can involve several influence operations. Influence operations can include many examples of disinformation. Disinformation can cause or be derived from misinformation. Institutional ownership should be developed on this understanding; for example, the EEAS would be responsible for countering disinformation spread by pro-Kremlin sources on the grounds that such disinformation is part of influence operations and a tool of foreign interference. (Pamment, 2020a, p. 17)

It stands to reason that "foreign interference" linked to disinformation soon evolved into its later conceptualization as "FIMI," a term developed within the EEAS. A framework that simultaneously characterizes disinformation as predominantly a foreign threat and designates the EEAS as the principal authority for addressing and countering such activities.

2.1. A Recent Adoption

The adoption of the term "FIMI" began in 2021. Its first notable mention, albeit without the acronym FIMI, featured in the US–EU Summit Statement in June 2021. Leaders from both sides of the Atlantic have pledged to address hybrid threats, explicitly including "FIMI," as part of a renewed transatlantic partnership. This summit declaration positioned this concept as a critical component of joint efforts to safeguard democracy and uphold the rules-based international order amidst escalating challenges from state and non-state actors (The White House, 2021).

Later that year, the concept resurfaced—again without the use of the acronym—in the joint communication on the EU strategy for cooperation in the Indo-Pacific, published in September 2021 by the HR/VP. The document declared, "The EU will help combat FIMI by state and nonstate actors in the Indo-Pacific region through new tools aimed at identifying, analysing, assessing, countering and imposing costs on information manipulation" (European Commission & High Representative of the Union for Foreign Affairs and Security Policy, 2021, p. 15).

Building on its initial mentions in 2021, the term "FIMI," still without its acronym, was officially introduced in the EU's Strategic Compass for Security and Defence, a comprehensive policy document published in March

2022 that outlines the EU's strategic vision and priorities for security and defence. The document explicitly states, "We will substantially enhance our resilience and ability to counter hybrid threats, cyberattacks, and foreign information manipulation and interference" (EEAS, 2022, p. 34).

The term is prominently featured as a heading under the broader section SECURE, named "Hybrid Threats, Cyber Diplomacy, and Foreign Information Manipulation and Interference" (EEAS, 2022, p. 34). The Strategic Compass dedicates significant focus to combating this threat, including the development of a specialized FIMI Toolbox and its integration into initiatives such as the EU Hybrid Toolbox and Common Security and Defence Policy missions.

Since then, the EEAS has consistently incorporated the acronym FIMI into its communications, underscoring its key role in the institution's approach. In a joint analysis with the European Union Agency for Cybersecurity (ENISA) published at the end of 2022, the EEAS proposed the concept "as a response to the call of the European Democracy Action Plan for a further refinement of the definitions around disinformation" and defined it as:

> A mostly non-illegal pattern of behavior that threatens or has the potential to negatively impact values, procedures, and political processes. Such activity is manipulative in character, conducted in an intentional and coordinated manner. Actors of such activity can be state or non-state actors, including their proxies inside and outside their own territory. (ENISA & EEAS, 2022, p. 4).

2.2. Defining FIMI

In the *Foreign Information Manipulation and Interference (FIMI) and Cybersecurity Threat Landscape* document, ENISA and EEAS clarify that while disinformation is a significant component of FIMI, the emphasis of FIMI shifts away from the "truthfulness of the content being delivered" and instead concentrates on the "manipulative behaviour" underlying such actions (ENISA & EEAS, 2022, p. 4). According to the EEAS, the term disinformation "captures only part of the problem: the manipulation of the content that is being pushed to distort facts and reality, to foster fear and hatred and to sow division in societies" (ENISA & EEAS, 2022, p. 6). FIMI, on the other hand, is an activity that "constitutes an integral part of modern warfare" (ENISA & EEAS, 2022, p. 7).

FIMI essentially replaces the multifaceted phenomenon of disinformation with a term more closely aligned with hybrid warfare, transplanting a concept rooted in political–military discourse into the civilian realm (Fridman, 2024). The conceptualisation of FIMI in military terms is the substitution of communication concepts such as "sender and receiver" by "operation owner" and "target" (Buvarp, 2023, p. 39). Furthermore, FIMI assumes that communication between FIMI operators and their targets is unidirectional and episodic, thereby neglecting the importance of feedback, responses, and context. Emphasis is placed on the message, therefore neglecting the reception process, the ability of the receiver to decode the message and the uses it makes of them.

As a consequence, the "target"—European publics—is seen in a passive way, since harmful messages are received and are conceived as having direct and immediate effects. By framing the issue through the lens of warfare, the EEAS abandons any connection to the complex social and political dynamics that contribute to

the spread of false information, advancing a concept that is fundamentally based on circular reasoning. If we assume that Russia, as the EU's primary adversary, invariably intends to manipulate information, then any narrative or information emerging from Russian sources is, by definition, FIMI, regardless of its content, and is therefore a threat.

Currently, the application of the FIMI framework is limited to the two key actors identified by the EEAS: Russia and China. This selective focus is justified by the institution's mandate and strategic priorities (Hénin, 2023), aligning with the EU's broader geopolitical concerns. However, this approach reveals a central paradox: while the FIMI framework is intended as a comprehensive tool for identifying and combating information threats, its application is restricted to a predefined set of adversaries—actors for whom the intent to manipulate is already presumed. Therefore, what does the FIMI ultimately signify? In practice, FIMI risks becoming synonymous with whatever narrative Russia and China put forward. The turn of events at the time of writing at the end of 2024 with the election of Trump raises questions about FIMI's appropriateness to address attempts to influence European public opinion by actors such as the US or Israel. For instance, will the EU address Elon Musk's support to the AfD in Germany's 2025 snap election (Connolly, 2024) as a form of FIMI?

2.3. An Ongoing but Relevant Conceptual Innovation

Because this is a recent turn, only a few studies have focused on the implications of FIMI. Buvarp (2023) presented a methodological framework using general morphological analysis to dissect the inner workings of FIMI operations, offering a structured approach to understanding its mechanisms. Yuskiv and Karpchuk (2024) provide a detailed case study of Russia's deployment of the FIMI leading to its intervention in Ukraine, focusing on how state and nonstate actors manipulate information for strategic purposes. Morača et al. (2023) broadened the discussion by examining FIMI's effects in Africa and the Western Balkans, stressing how local and foreign narratives intertwine to challenge the EU's influence in these regions.

This article addresses a recent and ongoing, yet potentially decisive, innovation in the EEAS institutional discourse on disinformation. The EU awoke to the incorporation of disinformation into the aggressive toolbox of its systemic rivals in 2014, and from 2016, it deepened the reflection on the vulnerability of liberal societies to information manipulation.

This has led the EU to develop a response to disinformation founded upon a systemic view of democracy (García-Guitián et al., 2024) and a strong internal and external distinction (Casero-Ripollés et al., 2023). The EU has been well aware of the negative risks associated with "policing the truth" and "re-establishing centres of truth-making," as described by Farkas and Schou (2019), therefore adopting a combination of multilevel monitoring of external threats that are seen as potentially affecting security and democracy with a co-regulatory response consisting of collaboration between multiple stakeholders (social media, fact-checkers, and experts) in the identification and limitation of systemic risks to public speech. This creates a potential misfit between the ontological threat perceived from outside and the internal co-regulatory response where nonstate actors seek to redress attacks by improving the quality of available information, albeit without challenging the ability to dissent, for instance, by limiting the reach (but not eliminating) harmful content or tagging verification labels on contested information. In this sense, the banning of the Kremlin-backed channels RT and Sputnik in the EU came as a decision so misaligned with the existing frame that it has been explained as a decision taken outside of the existing disinformation policy

environment and in line with broader sanctions against Russia in the context of the Ukraine invasion (Datzer & Lonardo, 2023, p. 760).

This policy rests upon the identification of verifiably false information as the problem, and much of the work of the EU has been devoted to countering the politics of falsehood, in the terms of Farkas and Schou (2019), therefore discussing ways to empower truth sayers, provide the public with better information via improved fact-checking and increasing their ability to recognise false information through civic education. However, FIMI moves the EU's concern into a broader concern that can be termed malign information influence (Wagnsson, 2020; Wagnsson et al., 2024), where the focus is no longer placed on the detection and contention of wilfully forged information with a harmful intention and instead moves to the usage of information—either verifiable false or not—to manipulate public opinion. Whereas the disinformation agenda attempted to contain false information, FIMI increases concerns about the vulnerability of democracies by assuming that they can be manipulated by rivals using a combination of false information and malicious narratives. In other words, rivals can use factually correct information to articulate negative narratives that can be used to manipulate the preferences of citizens and political actors in decisive political decisions.

This subtle change is coherent with the EU's broader concern about narratives since the early 2010s (Manners & Murray, 2016) and with its position on the vulnerability of democracy to manipulation by foreign actors. However, it is potentially significant since the disinformation agenda assumes that the European public is vulnerable if it cannot identify falsehoods, but controversial opinions and narratives have a place for discussion in the public sphere. FIMI potentially moves all forms of communication arriving from foreign rivals into the space of potentially disruptive communication. It is the type of incremental change oriented with existing properties that may nevertheless evolve into a specific category and, therefore, merit particular discussion and analysis. We are also aware of the limited amount of evidence of change. FIMI is a very new addition to the EEAS toolbox and may expand or never be confirmed as a relevant contribution. However, its potential qualitative importance as a potentially significant transformation of the EU's strategy for democracy protection in the post-truth era justifies including it in conceptual debates and analyses beyond its still quantitatively minor importance.

This article intends to discuss the strategic implications that this conceptual pivot raises about the EU's identity as a global actor. Traditionally described and self-perceived as a civil, soft, or normative power (Manners, 2002), the EU's greatest asset has been its ability to shape global norms and values through diplomacy, dialogue, and peaceful engagement. However, the adoption of FIMI aligns with "information warfare" framing (Szostek, 2020), which risks reducing complex communicative processes to binary notions of attack and defence. As cautioned by Wagnsson and Hellman (2018), this shift could erode the EU's moral authority and credibility, diminishing its capacity to serve as a global advocate for peace and cooperation, even though citizens in EU member states (Wagnsson et al., 2024) and beyond (Szostek & Orlova, 2024) have also become more aware of the role of foreign interference. The Russian aggression on Ukraine has therefore largely contributed to moving decision-makers, scholars, and public opinion to positions more favourable to information control regarding foreign rivals than before, and we argue that along these lines, FIMI can have an effect on the EU's distinctive approach to international relations as a normative civilian power. At the moment of the emergence of the EU disinformation policy community, Ördén (2019, p. 427) highlighted a clear divide in policy preferences and risk attitudes: While the internet and security/defence communities shared a procedural approach focused on the continuous management of the digital space, the

media and education communities prioritized content pluralism and the diversity of viewpoints among citizens, viewing protection as empowering individuals to form their own judgements. The adoption of FIMI appears to be a move in the direction highlighted by the former.

3. Why FIMI Took Root in the EU

Because the EU has assumed since the beginning of its approach that disinformation is linked to foreign interference and has only recently addressed internal phenomena (Casero-Ripollés et al., 2023), member states tasked the EEAS to respond. In this context, the EEAS understood the necessity of increasing its strategic communication capacity, particularly focusing on digital disinformation and Russian media, as the new digitalization of diplomacy and social media represented a challenge to traditional diplomatic communication. The EEAS hired five communication experts from member states to create the East Strategic Communications Division (StratCom) task force, introducing new ways of doing diplomacy within the EEAS (Hedling, 2021) and reinforcing its role in front of member states.

To fully understand the emergence of FIMI, it is essential to consider several trends that have shaped the EU's approach to combating disinformation: the increased capabilities acquired by the EEAS, the conceptualization of narratives as a threat to the EU, and the polarizing effects of trying to regulate disinformation at both the EU level and the European national arenas.

3.1. The Incremental Acquisition of FIMI Capacities by the EEAS

Whereas, as we will discuss below, the adoption of FIMI is also de facto a call for new resources and capacities adapted to the new strategy, it is also expected that the strategy will incrementally build upon the structurally existing capacities and strategies against international disinformation campaigns. The FIMI toolbox addresses four interrelated priority dimensions: situational awareness, resilience, regulatory frameworks, and the EU's external action. Each of these areas encompasses various instruments aimed at either preventing or mitigating the impact of FIMI activities, deterring those who seek to engage in such actions, or effectively responding to them (EEAS, 2024b). Following the mandate of the European Council (2015), the first significant initiative launched by the EEAS was the creation of the StratCom together with the EUvsDisinfo platform.

This division leads efforts to combat foreign disinformation, manipulation, and interference by developing strategies to engage with key audiences, particularly in the EU's neighbourhood. Their proactive approach combines regional expertise, policy development, communication initiatives, and data analysis to amplify the EU's voice and support its strategic interests. This campaign-based communication strategy is complemented by strategic engagements, support for independent media and organized civil society, and training for EU delegations and public communicators (European Union External Action Service, 2021). The EUvsDisinfo was also created in 2015 to increase the ability to anticipate, address, and counter the Russian Federation's persistent disinformation campaigns targeting the EU, its member states, and neighbouring countries. Its primary objective is to raise public awareness and deepen the understanding of the Kremlin's disinformation tactics while empowering citizens in Europe and beyond to build resilience against the manipulation of digital information and media (EUvsDiSiNFO, n.d.). In December 2019, the General Affairs Council Conclusions regarding EEAS StratCom's efforts to combat foreign disinformation, information manipulation, and interference confirmed three key work strands: "(1) proactive communication

and raising awareness, (2) support for independent media, and (3) detection, analysis, and counteraction of such activities by threat actors" (EEAS, 2015, p. 1). This mandate was explicitly broadened to include new threat actors and geographic regions.

The next step was the Action Plan Against Disinformation launched in 2018 by the HR/VP in collaboration with the Commission to coordinate efforts to address the growing threat of disinformation. In particular, to ensure that the relevant EEAS strategic communication teams were equipped with the necessary mandates and resources, considering the 2019 European Parliament elections (European Council, 2018, p. 6). The action plan aims to enhance EU institutions' disinformation capabilities, strengthen coordinated responses with member states, mobilize the private sector, and improve societal resilience (Butcher & Neidhardt, 2021). The next EEAS step was to implement the Rapid Alert System, which focused on facilitating the sharing of insights related to disinformation campaigns and coordinating responses among EU institutions and member states. It relies on open-source information and incorporates insights from academia, fact-checkers, online platforms, and international partners (EEAS, 2019a). Its primary objective is to address disinformation campaigns that interfere with or undermine European democratic processes, focusing on two categories: (a) campaigns originating from or disseminated with the support or involvement of foreign actors; and (b) campaigns aiming to influence national or European elections. The last initiative supported by the EEAS was the creation of the FIMI-Information Sharing and Analysis Centre in 2023. It enhances its members' capacity to detect, analyse, and respond swiftly and efficiently to FIMI while adhering to the core principle of protecting freedom of expression (Information Sharing and Analysis Centre, n.d.).

3.2. Narratives as a Threat

As the first Von der Leyen commission took office in 2019, the concept of "geopolitics" gained renewed prominence within EU policy circles and the media. Faced with escalating external threats—from intensifying competition between the US and China to growing instability in its own neighbourhood—the new administration committed to reasserting the EU's global role by integrating geopolitics into its strategic framework. This "geopolitical Commission" placed strategic communication at the forefront of its agenda, as reflected in the Commission's 2020 Work Programme, which explicitly aimed to counter "multiple challenges, both from outside and from within," confronting the democratic systems of EU member states and enhancing their long-term resilience (European Commission, 2020, p. 8).

As Valenza (2021) observes, this emphasis on strategic communication gained further momentum amidst the Covid-19 pandemic. In February 2020, Josep Borrell (HR/VP) argued that the EU must "relearn the language of power" and strategically align its resources to maximize its geopolitical impact (Borrell, 2019). Borrell underscored the critical role of narratives, asserting that "whoever is best at organizing the response, quickly drawing on lessons learned from around the world, and communicating successfully to citizens and the wider world, will emerge strongest" (Borrell, 2020). He depicted a global landscape marked by "a struggle of influence through spinning" and urged EU institutions and member states to be "armed with facts" to defend Europe against its detractors (Borrell, 2020).

To fully grasp this strategic shift, it is essential to consider the "narrative turn," a concept introduced in the early 2010s to explain the EU's legitimacy challenges (Bouza García, 2017). This turn marked the first time

the EU recognized its lack of control over popular narratives about Europe as a significant risk to the Union. The realization that the EU needed to establish a new narrative to win back the hearts and minds of Europeans became central to the continuation of the EU integration project.

This renewed focus on narratives and strategic communication—aimed at promoting "beneficial" internal narratives while countering "dangerous" external narratives—was built on the foundations laid by the EEAS, which includes a dedicated StratCom. This division includes the East Stratcom Task Force, the Western Balkans Task Force, and the Task Force South, each tasked with addressing disinformation in key regions critical to the EU's strategic interests. Both the division and its regional task forces are specifically charged with "narrative positioning" (EEAS, 2021). For example, when the East Stratcom Task Force was established in 2015 as the first unit deployed by the EEAS following the Council's mandate, its explicit goal was to develop a positive narrative about the Union's actions in the Eastern neighbourhood while simultaneously deconstructing conspiracy theories and debunking disinformation (Missiroli et al., 2016).

3.3. Polarization Challenges

In the lead-up to the 2019 European elections that ushered in the Von der Leyen commission and amidst the fallout from the Cambridge Analytica scandal and Russia's interference in the 2016 US presidential election, the EU significantly bolstered its disinformation countermeasures through the Action Plan against Disinformation. This initiative included the establishment of the Rapid Alert System, which was designed to facilitate swift data exchange on disinformation campaigns between member states, the European Commission, and the EEAS, thereby enhancing the EU's capacity for a coordinated response. The plan also underscored the importance of member states' involvement, urging them to "complement and support the actions of the Union institutions" by expanding their national capacities and contributing additional resources to the collective effort (European Commission & High Representative of the Union for Foreign Affairs and Security Policy, 2018, p. 6).

However, as Dragomir et al. (2024) recently noted, despite the comprehensive plans and various EU measures implemented to address disinformation over the past decade, these strategies have not uniformly fortified member states against the phenomenon. A closer examination of the divergent responses from EU capitals highlights the significant limitations that national governments face in combating disinformation. One of the most glaring issues is that "politicians and government officials remain a major source of disinformation accross Europe" (Dragomir et al., 2024, p. 7). Additionally, legislation intended to penalize the spread of fake news can be vulnerable to misuse and can exacerbate polarization by fostering mistrust and perceptions of manipulation by authorities.

The recent clash between the former EU Commissioner Thierry Breton and Elon Musk, CEO of X (formerly Twitter), over the Digital Services Act highlights the challenges of regulating disinformation in a politically charged environment. Before an August 2024 interview between Musk and Donald Trump, Breton urged Musk to ensure that X complied with the Digital Services Act, which mandated that platforms limit harmful content and address disinformation. Musk dismissed this as an attack on free speech, igniting a broader debate, with Trump's supporters accusing the EU of electoral meddling and right-wing European parties calling the Digital Services Act politically biased ("Abascal critica que la UE," 2024; Starcevic, 2024).

At the national level, Spain provides another relevant example. In April 2018, under a Partido Popular government, a working group was formed in Congress to study disinformation, which was proposed by the defence minister. Unidas Podemos rejected it. A year later, now under socialist administration, the Coordination Network for Security in Electoral Processes was created, including the Permanent Commission Against Disinformation. This time, the Partido Popular condemned it as a "Ministry of Truth," sparking a heated debate amplified by Vox and opposition media (Correyero-Ruiz & Baladrón-Pazos, 2023).

The clash across the political spectrum underscores the reality that in highly polarized environments, such as those prevalent in many member states, any initiative by the ruling party to combat disinformation risks being perceived as a partisan tool, potentially weaponized by the opposition.

3.4. Logical Conclusions

As previously noted, the recent pivot towards FIMI within the EU's disinformation strategy can be attributed to three key factors. First, the incremental capacities acquired by the EEAS have significantly expanded the institution's influence, allowing it to take the lead in shaping disinformation frameworks. Second, the EU's growing perception that external narratives pose an existential threat to the European project has placed a renewed emphasis on strategic communication, driving a focus on "defending" and "responding" to these perceived threats. Finally, the difficulty of legislating disinformation at both the EU and national levels has created an imbalance, as the EEAS has been able to advance its external disinformation agenda far more rapidly than other EU institutions and member state parliaments, which struggle with fragmented and polarized domestic contexts.

These converging trends have both capitalized on and strengthened the EEAS's exclusive focus on the external dimension of disinformation. By positioning foreign actors as the primary culprits, the EEAS has navigated the politically fraught environments within member states. Simultaneously, it has emerged as the greatest beneficiary of the European Commission's broader geopolitical pivot and its strategic emphasis on narrative building and strategic communication as tools of defence. These shifts have not only validated but also amplified the role of this institution in shaping the EU's response to disinformation.

There is no better example of this dynamic than the recent promotion by the EEAS of the concept of FIMI. As stated by Nicolas Hénin, the clinical approach of FIMI, almost completely detached from the content or from other actors other than the most obvious geopolitical rivals of the EU, "responds to strong political pressures and limitations of consensus demanded by the different perspectives of the Member States" (Hénin, 2023, p. 4).

In defining FIMI, the EEAS avoids the pitfalls of the debate about disinformation (value pluralism and democracy, balance between values and rights, polarization and populism) or about ways to respond (regulatory complexities, national diversity, and differing capacities) and focuses exclusively on the external dimension. However, it also provides a politically neutral understanding of the threat. By not addressing the nature of disinformation or the best tools to respond but instead objectifying information—even factually correct information—as an asset that can be manipulated against democracies, FIMI provides a bureaucratic tool that allows EEAS to define its contribution to the EU response on the grounds closer to its interests and expertise.

4. Public Diplomacy in a World of Narrative Rivals?

The EU has traditionally perceived itself as an international power closely associated with the concept of normative power that uses public diplomacy as a tool of international influence. Public diplomacy is an international diplomatic and political communication activity aimed at creating a positive image and/or political influence to support the achievement of foreign policy objectives, which is close to a less intrusive and less malign-minded form of propaganda (Cull, 2009, pp. 22–23). It functions as a tool to enhance soft power—a form of power based on the capacity for attraction, influence, and persuasion that occurs indirectly through the mobilization of resources such as culture, principles, foreign policy strategies, and institutions (Nye, 1990).

Public diplomacy aims to promote EU interests by understanding, informing, and influencing. This involves clearly explaining the EU's goals, policies, and activities and fostering understanding through dialogue with individual citizens, groups, institutions, and the media. This broad definition encapsulates the essence of the EU's internal and external public diplomacy. Essentially, it concerns self-image, or the image that a given actor intends to project to a third party. The complex linkage between the internal and external dimensions of EU public diplomacy can be best understood as a self-reaffirming process, wherein messages communicated internally are also directed externally as part of the EU's ongoing internal identity construction. The attraction of the EU is based on the will of its partners to emulate the peace, stability, and prosperity characteristic of EU members. The legitimacy of internal identity construction, the acceptance of norms, and the consensus around the narrative significantly influence the legitimacy of external public diplomacy for both EU citizens (who wish to see reflections of themselves) and third parties (who wish to see the virtues of the European example reflected towards themselves).

With the adoption of the Lisbon Treaty, public diplomacy is no longer conducted exclusively by the Council Secretariat and the Commission but also by the EEAS. The advent of the EEAS held the promise of integrating strategic communication, public diplomacy, and stakeholder engagements in ways that had previously eluded the EU, intending to create a comprehensive communication culture across the EU institutions involved in external actions (Song & Fanoulis, 2023). The EEAS plays a crucial role in shaping the EU's positive image globally. The primary requirement is to ensure that its foreign policy actions align coherently with the EU's self-representation and professed values (Chaban & Lucarelli, 2021).

What made public diplomacy an acceptable and successful form of diplomacy rather than an aggressive form of propaganda was the liberal understanding of a rules-based international order where partners did not harm each other with hostile actions and instead competed under generally accepted rules of behaviour. This is in stark contrast with a geopolitical understanding of international relations where information can be weaponized (Valenza, 2021). Defining FIMI as a mostly nonillegal yet hostile behaviour establishes self-interest on the side of the sender despite the civilian nature of action as the primary rule of thumb for acceptable informational exchanges. Even though the aggressive form of communication, the use of disinformation and the combination of other warfare techniques clearly situate FIMI outside the consensus on public diplomacy, conceptual clarity between liberal public diplomacy and manipulative behaviour is difficult to achieve (Szostek, 2020, pp. 2740–2741).

The process of securitization of the object is therefore fully in line with decisions adopted since 2018 (Casero-Ripollés et al., 2023) and implies not only a bureaucratic specialization logic but also a much broader

definition of the threat. Given that concerns with disinformation emphasize that geopolitical rivals could attempt to manipulate EU political processes using false information, FIMI focuses on manipulative behaviour against EU values, procedures, and political processes. In summary, exercising soft power via diplomacy is a form of using information in the form of publicly articulated narratives to shape (therefore manipulate) preferences, values, or political processes into positions more favourable to the EU.

An example of how the EU has tried to promote its soft power is the usage of strategic communication. The EU adopted an action plan on strategic communication in the decisive mid-2010s, effectively the interregnum between liberal narratives and the advent of new geopoliticised understandings (Manners & Murray, 2016), whose objectives are:

> Effective communication and the promotion of EU policies and values towards the Eastern neighbourhood, strengthening the media environment. (East Stratcom Task Force, 2015, p. 2)

In 2014, former HR/VP Federica Mogherini stated that the EU was working on making X one of its fundamental diplomatic tools (Mann, 2015). Additionally, the EU Global Strategy (EEAS, 2016, p. 23) declared that the EU would "enhance its strategic communications, investing in and joining up public diplomacy across different fields, in order to connect EU foreign policy with citizens and better communicate it to our partners." In a 2019 report on the implementation of the EU Global Strategy, the EEAS emphasized that "public diplomacy and communication are critical" and suggested that the EU could invest more in "positively communicating who we are and what we seek to achieve in the world" (EEAS, 2019b, p. 26).

Therefore, we argue that by adopting the FIMI strategy, which considers all types of information exchanges, albeit from certain actors only, as potentially dangerous, the EU is severely endangering its ability to use public diplomacy and strategic communication (Szostek, 2020, makes this point for other responses to information warfare). Whereas it may be reasonably assumed that these channels are effectively locked in relation to geopolitical rivals, who control information channels in an authoritarian fashion, a key issue to consider is the reception of this message by other international partners. This is a further step in the direction of adoption since the geopolitical turn:

> From building policy on mutuality and reciprocity and attempting to co-create between equals, the EU has moved towards a communication approach that considers cultural relations as a tool in the above-mentioned EU StratCom's box, and local actors as rather passive recipients of a message that has already been drafted in Brussels. (Valenza, 2021, p. 4)

However, as Valenza anticipates, public diplomacy assumes reciprocity. Therefore, despite the EU's designation of Russia and China as its primary narrative rivals, the concept potentially undermines the ability of the EU to carry out public diplomacy successfully since any international actor attempting to manipulate the preferences of EU political actors in its favour could be targeted as an object of anti-FIMI measures and would therefore likely retort: "Problematically, however, this messaging approach disregards the fact that successful people-to-people contacts take place only when the principles of mutuality and reciprocity are fully reflected in the implementation of external action" (Valenza, 2021, p. 4).

Furthermore, the FIMI can also impact the polyphonic nature of EU public diplomacy narratives: Since the FIMI considers information a dangerous element to be channelled, it can endanger the organic ability to cast

a positive narrative of the EU. This is particularly important since the EU's public diplomacy is intermestic, as messages are sent to both the EU member states and the third states.

The EU turning to FIMI does not mean that it has renounced public diplomacy, as it still sees it as a fundamental tool of the EEAS and that the fight against disinformation can actually be reinforced. However, based on a case study by NATO, Olsson et al. (2019) state that information warfare strategies risk undermining public diplomacy efforts, as they foster adversarial behaviour instead of being open to genuine dialogue. Of course, EU FIMI efforts are not a form of aggressive information warfare against its rival, but they adopt an adversarial language that conceives of all information from some rivals as a potential bit of information, therefore fostering defensive information warfare and enhancing the already mentioned conceptual lack of clarity between information warfare and public diplomacy. As a result, it has been argued that, at least in relation to Eurasia, the EU can no longer be conceived as a normative but a defensive power (Zwolski, 2024, p. 134). The remaining questions are whether this turn is fully reflective and whether the EU has the means, tools, and will to achieve such a transformation.

5. Conclusions

The FIMI pivot is a logical evolution for an institution seeking to recalibrate and redefine its role within an increasingly hostile and multifaceted global environment. In this process, the actor responsible for driving the EU's external policy—the EEAS—has found ways to replicate the narrative strategies of its geopolitical rivals, adopting a more assertive posture in response to foreign threats. This is coherent with ongoing securitization and geopoliticisation in other fields but contributes to transforming the way in which the EU sees itself (Manners & Murray, 2016).

The shift towards viewing disinformation as a form of hybrid warfare may reflect an accurate reading of a global reality that the EU finds unfavourable but cannot fundamentally change. However, this article challenges more than just the adoption of FIMI or the reframing of disinformation as a broader issue requiring new regulatory frameworks. Returning to a question addressed by Szostek (2020), the issue is whether democracies can win information and at what cost. In terms of Wagnsson et al. (2024), the EU's approach has decidedly opted for confronting rival narratives, whereas the jury is still out as to its ability to do so while still promoting its own narratives abroad (Valenza, 2021) or assume a greater role in blocking, as evidenced in the exceptionality (both as a single case and as an application of an extraordinary measure) of the RT and Sputnik ban. Does this shift and its effects truly enhance the Union's standing, or does it risk eroding its main strengths, ultimately causing it to lose more than it gains?

As discussed in Section 4, the EU is still fundamentally an international actor with civilian capacities who can turn its market power into political influence by diplomatic means, including public diplomacy. Even though it is trying to accommodate itself to a diagnosis of an international environment where liberal norms weaken, the EU is only incorporating the information control rationale into its external policy toolbox incrementally, whereas it is still expected to be able to follow a rules-based normative logic in the fight against disinformation in the internal market (Casero-Ripollés et al., 2023). The dilemma is whether the EU has sufficient time and resources to develop new capacities and strategies in line with its new world vision.

The new world vision defining the world as a hostile environment for what the EU has traditionally been may become a consensual venue both for reformists and more radical critics of traditional EU policies. This

consensus works since rival visions are not there to be represented and, as noted in Section 3, it avoids some of the more polarising issues about the role of domestic politics, media, and platforms in the origin and circulation of disinformation. This has implications for the consolidation of a postcolonial worldview opposing an internal sphere where rules and norms can be applied and an external sphere dominated by securitised power politics, including information wars, and can potentially affect political pluralism internally (Wagnsson et al., 2024).

This article contributes to the emerging policy turn that FIMI represents in the EU policy toolbox on disinformation. This line of work will require further research in different directions. First, the EEAS is not a monolithic actor but is composed of different internal actors maintaining internal balance. The critical relationship between the interception of harmful foreign narratives and the ability to exert public diplomacy is likely to become an issue of internal contention. Additionally, research will be required if and when the case emerges of applying FIMI to actors who are internally more divisive than China and Russia, such as Israel or the Trump-led US. Finally, even though the EU regulatory response still maintains a clear distinction between foreign threats (to be addressed with FIMI) and internal phenomena (related to the EU market or national politics) where distinctions between legal and illegal and factually based or unverifiable contents apply, the RT/Sputnik sanctions demonstrate that geopolitical thinking can rapidly challenge this internal/external distinction and take decision-making down a slippery slope affecting internal freedom.

Conflict of Interests

The authors declare no conflict of interests. In this article, editorial decisions were undertaken by Jorge Tuñón Navarro (Universidad Carlos III de Madrid) and Alvaro Oleart (Université Libre de Bruxelles).

References

Abascal critica que la UE sea severa con Elon Musk y Donald Trump, pero no con Nicolás Maduro. (2024, August 13). *El Debate*. https://www.eldebate.com/espana/20240813/abascal-critica-ue-sea-severa-elon-musk-donald-trump-nicolas-maduro_219851.html

Borrell, J. (2019). *Hearing of Josep Borrell Fontelles, high representative/vice president—designate of the European Commission: Opening statement by Josep Borrell Fontelles*. European Parliament Multimedia Centre. https://multimedia.europarl.europa.eu/en/video/hearing-of-josep-borrell-fontelles-high-representativevice-president-designate-of-the-european-commission-opening-statement_I178140

Borrell, J. (2020). *EU HRVP Josep Borrell: The Coronavirus pandemic and the new world it is creating*. European Union External Action. https://www.eeas.europa.eu/eeas/eu-hrvp-josep-borrell-coronavirus-pandemic-and-new-world-it-creating_en

Bouza García, L. (2017). Introduction: A narrative turn in European studies. *Journal of Contemporary European Studies*, *25*(3), 285–290. https://doi.org/10.1080/14782804.2017.1348341

Butcher, P., & Neidhardt, A. H. (2021). *From debunking to prebunking: How to get ahead of disinformation on migration in the EU*. European Policy Center. https://www.epc.eu/content/PDF/2021/Disinformation___Migration_2021_final_single.pdf

Buvarp, P. M. H. (2023). The space of influence: Developing a new method to conceptualize foreign information manipulation and interference on social media. *Journal of Information Warfare*, *22*(2), 31–51.

Casero-Ripollés, A., Tuñón, J., & Bouza-García, L. (2023). The European approach to online disinformation: Geopolitical and regulatory dissonance. *Humanities & Social Sciences Communications*, *10*(1), Article 657. https://doi.org/10.1057/s41599-023-02179-8

Chaban, N., & Lucarelli, S. (2021). Reassessing external images of the EU: Evolving narratives in times of crisis. *European Foreign Affairs Review*, *26*(1), 177–196. https://doi.org/10.54648/eerr2021014

Connolly, K. (2024, December 20). Outrage as Elon Musk claims 'only AfD can save Germany.' *The Guardian*. https://www.theguardian.com/world/2024/dec/20/elon-musk-claims-only-afd-can-save-germany

Correyero-Ruiz, B., & Baladrón-Pazos, A. J. (2023). Antídotos contra la epidemia desinformativa: hacia un estado de la cuestión en la lucha contra la desinformación en España. *Espejo de Monografías de Comunicación Social*, *10*, 127–144.

Cull, N. J. (2009). *Public diplomacy: Lessons from the past*. Figueroa Press.

Datzer, V., & Lonardo, L. (2023). Genesis and evolution of EU anti disinformation policy: Entrepreneurship and political opportunism in the regulation of digital technology. *Journal of European Integration*, *45*(5), 751–766.

De Spiegeleire, S., Sweijs, T., & Zhao, T. (2011). *Contours of conflict in the 21st century: A cross-language analysis of Arabic, Chinese, English and Russian perspectives on the future nature of conflict*. Hague Centre for Strategic Studies. https://hcss.nl/wp-content/uploads/2011/03/Contours-of-Conflict-in-the-21st-Century.pdf

Dragomir, M., Rúas-Araújo, J., & Horowitz, M. (2024). Beyond online disinformation: assessing national information resilience in four European countries. *Humanities and Social Sciences Communications*, *11*, Article 101. https://doi.org/10.1057/s41599-024-02605-5

East Stratcom Task Force. (2015). *Action plan on strategic communication* (Ref. Ares (2015)2608242—22/06/2015). https://www.eeas.europa.eu/sites/default/files/action_plan_on_strategic_communication.docx_eeas_web.pdf

European Commission. (2018). *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Tackling online disinformation—A European approach* (COM(2018)236). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52018DC0236

European Commission. (2020). *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Commission work programme 2020 a union that strives for more* (COM(2020) 37 final). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0037

European Commission, & High Representative of the Union for Foreign Affairs and Security Policy. (2018). *Joint communication to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions: Action plan against disinformation* (Document 52018JC0036). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52018JC0036

European Commission, & High Representative of the Union for Foreign Affairs and Security Policy. (2021). *Joint communication to the European Parliament and the Council: The EU strategy for cooperation in the Indo-Pacific* (JOIN/2021/24 final, Document 52021JC0024). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52021JC0024

European Council. (2015). *European council meeting (19 and 20 March 2015)—Conclusions* (EUCO 11/15). https://www.consilium.europa.eu/media/21888/european-council-conclusions-19-20-march-2015-en.pdf

European Council. (2018, June 29). *European Council conclusions, 28 June 2018* [Press Release]. https://www.consilium.europa.eu/en/press/press-releases/2018/06/29/20180628-euco-conclusions-final/

European Union Agency for Cybersecurity, & European Union External Action Service. (2022). *Foreign information manipulation interference (FIMI) and cybersecurity—Threat landscape*. European Union Agency for Cybersecurity. https://www.enisa.europa.eu/publications/foreign-information-manipulation-interference-fimi-and-cybersecurity-threat-landscape

European Union External Action Service. (2015). *Action plan on strategic communication*. https://www.eeas.europa.eu/sites/default/files/action_plan_on_strategic_communication.docx_eeas_web.pdf

European Union External Action Service. (2016). *Shared vision, common action, a stronger Europe: A global strategy for the European Union's foreign and security policy*. https://www.eeas.europa.eu/sites/default/files/eugs_review_web_0.pdf

European Union External Action Service. (2019a). *Rapid alert system: Strengthening coordinated and joint responses to disinformation*. EUvsDisinfo. https://www.eeas.europa.eu/sites/default/files/ras_factsheet_march_2019_0.pdf

European Union External Action Service. (2019b). *The European Union's global strategy three years on, looking forward*. https://www.eeas.europa.eu/eeas/european-unions-global-strategy-three-years-moving-forward_en

European Union External Action Service. (2021). *Tackling disinformation: Information on the work of the EEAS Strategic Communication division and its task forces (SG.STRAT.2)*. https://www.eeas.europa.eu/eeas/tackling-disinformation-information-work-eeas-strategic-communication-division-and-its-task_en

European Union External Action Service. (2022). *A strategic compass for security and defence*. https://www.eeas.europa.eu/eeas/strategic-compass-security-and-defence-0_en

European Union External Action Service. (2024a). *2nd EEAS report on foreign information manipulation and interference threats*. https://www.eeas.europa.eu/eeas/2nd-eeas-report-foreign-information-manipulation-and-interference-threats_en

European Union External Action Service. (2024b). *EEAS Stratcom's responses to foreign information manipulation and interference (FIMI) in 2023*. https://euvsdisinfo.eu/uploads/2024/06/EEAS-Stratcom-Annual-Report-2023.pdf?swcfpc=1

EUvsDiSiNFO. (n.d.). *About*. https://euvsdisinfo.eu/about

Farkas, J., & Schou, J. (2019). *Post-truth, fake news and democracy: Mapping the politics of falsehood*. Routledge.

Fridman, O. (2024). Defining foreign influence and interference. *INSS Special Publication*, 1–12. https://kclpure.kcl.ac.uk/portal/en/publications/defining-foreign-influence-and-interference

García-Guitián, E., Bouza, L., & Haapala, T. (2024). What Is the EU's vision of democracy in the post-truth scenario? A conceptual analysis of the institutional narratives of the public sphere in the "democracy action plan." *Javnost-The Public*, *31*(3), 364–381. https://doi.org/10.1080/13183222.2024.2382662

Hedling, E. (2021). Transforming practices of diplomacy: The European External Action Service and digital disinformation. *International Affairs*, *97*(3), 841–859.

Hénin, N. (2023). *FIMI: Towards a European redefinition of foreign interference.* EU DisInfoLab. https://www.disinfo.eu/wp-content/uploads/2023/04/20230412_FIMI-FS-FINAL.pdf

Information Sharing and Analysis Centre. (n.d.). *Home.* https://fimi-isac.org

Mann, M. (2015, April 28). The European External Action Service and digital diplomacy. *Twidiplomacy.* https://www.twiplomacy.com/the-european-external-action-service-and-digital-diplomacy

Manners, I. (2002). Normative power Europe: A contradiction in terms? *JCMS: Journal of Common Market Studies*, *40*(2), 235–258. https://doi.org/10.1111/1468-5965.00353

Manners, I., & Murray, P. (2016). The end of a noble narrative? European integration narratives after the nobel peace prize. *JCMS: Journal of Common Market Studies*, *54*(1), 185–202. https://doi.org/10.1111/jcms.12324

Missiroli, A., Gaub, F., Popescu, N., & Wilkins, J. J. (2016, December). *Strategic communications: East and South* (European Issues Policy Paper no. 415). Fondation Robert Schuman Foundation.

Morača, T., Sicurella, F. G., Sekulić, T., Armanini, J., & Stella, F. A. (2023). *Feeling the pulse: Countering foreign information manipulation and interference in Africa and the Western Balkans* (Brief no. 18). European Union Institute for Security Studies.

Nye, J. S. (1990). Soft power. *Foreign Policy*, (80), 153–171. https://www.jstor.org/stable/1148580

Olsson, E.-K., Wagnsson, C., & Hammargård, K. (2019). The use of political communication by international organizations: The case of the EU and NATO. In C. Bjola & J. Pamment (Eds.), *Countering online propaganda and extremism: The dark side of digital propaganda* (pp. 66–80). Routledge.

Ördén, H. (2019). Deferring substance: EU policy and the information threat. *Intelligence and National Security*, *34*(3), 421–437.

Pamment, J. (2020a). *The EU's role in fighting disinformation: Taking back the initiative.* (Future threats, future solutions Working Paper no. 1). Carnegie Endowment for International Peace. https://carnegieendowment.org/research/2020/07/the-eus-role-in-fighting-disinformation-taking-back-the-initiative?lang=en

Pamment, J. (2020b). *The EU's role in fighting disinformation: Crafting a disinformation framework* (Future threats, future solutions Working Paper no. 2). Carnegie Endowment for International Peace. https://carnegieendowment.org/2020/09/24/eu-s-role-in-fighting-disinformation-crafting-disinformation-framework-pub-82720

Song, W., & Fanoulis, E. (2023). Global perspectives on European Union public diplomacy: an introduction. *Journal of Contemporary European Studies*, *31*(1), 1–7.

Splidsboel Hansen, F. (2017). *Russian hybrid warfare: A study of disinformation* (DIIS Report no. 2017:06). Danish Institute for International Studies.

Starcevic, S. (2024, August 12). EU's Breton warns Musk on hate speech ahead of Trump interview; receives profane response. *Politico.* https://www.politico.eu/article/eu-warns-elon-musk-hate-speech-donald-trump-interview-breton-x

Szostek, J. (2020). What happens to public diplomacy during information war? Critical reflections on the conceptual framing of international communication. *International Journal of Communication*, *14*, 2728–2748.

Szostek, J., & Orlova, D. (2024). Free speech versus defence of the nation? The media as sources of national insecurity in Ukraine. *European Security*, *33*(1), 82–106.

The White House. (2021). *U.S.–EU summit statement.* https://www.whitehouse.gov/briefing-room/statements-releases/2021/06/15/u-s-eu-summit-statement

Valenza, D. (2021). *The trap of geopolitics: Rethinking EU strategic communication* (College of Europe Policy Brief no. 3.21). College of Europe. https://www.coleurope.eu/sites/default/files/research-paper/valenza_cepob_3_2021_final.pdf_0.pdf

Van Raemdonck, N., & Meyer, T. (2024). Why disinformation is here to stay. A socio-technical analysis of disinformation as a hybrid threat. In L. Lonardo (Ed.), *Addressing hybrid threats: European law and policies* (pp. 57–83). Edward Elgar.

Wagnsson, C. (2020). What is at stake in the information sphere? Anxieties about malign information influence among ordinary Swedes. *European Security*, *29*(4), 397–415. https://doi.org/10.1080/09662839.2020.1771695

Wagnsson, C., & Hellman, M. (2018). Normative power Europe caving in? EU under pressure of Russian information warfare. *JCMS: Journal of Common Market Studies*, *56*(5), 1161–1177. https://doi.org/10.1111/jcms.12726

Wagnsson, C., Hellman, M., & Hoyle, A. (2024). Securitising information in European borders: How can democracies balance openness with curtailing Russian malign information influence? *European Security*, 34(1), 127–147. https://doi.org/10.1080/09662839.2024.2321906

Yuskiv, B., & Karpchuk, N. (2024). Russian Federation's FIMI prior to its intervention Ukraine. In M. Echeverría, S. García, & D. C. Hallin (Eds), State-sponsored disinformation around the globe (pp. 250–253). *Routledge.*

Zwolski, K. (2024). *Researching European security integration cham.* Springer.

About the Authors

Lucas Proto is a journalist in *El Confidencial* and a part-time lecturer in political science at the Universidad Autónoma de Madrid, where he is undertaking a PhD.

Paula Lamoso-González is an assistant professor at Universidad Loyola Andalucía. She holds a PhD in Law, government, and public policies from the Universidad Autónoma de Madrid.

Luis Bouza García is associate professor of political science at the Universidad Autónoma de Madrid.