



D1.2 Working Paper

Version 2 – 1 September 2026

Project Acronym: ARM
Project Full Title: ARM: The Long Arm of Authoritarian States
Call: HORIZON-CL2-2023-DEMOCRACY-01
Topic: Horizon-CL2-2023-DEMOCRACY-01-02
Type of Action: Horizon-RIA
Grant Number: 101132437
Project URL: <https://cordis.europa.eu/project/id/101132437>

DELIVERABLE 1.2	D1.2 WORKING PAPER
Related Work Package	WP1 Conceptualising Information Suppression
Deliverable Lead	CMI
Authors	Lovise Aalen (CMI) Pauline Lemaire (CMI) Gabriele de Seta (CMI)
Contact	media@arm-project.eu
Start date / Project Duration	1 Jan 2024 – 38 months
Type of Deliverable (R, DEM, DEC, Other)	R
Dissemination Level (PU, CO, CI)	PU
Date of Last Update	1 September 2026
Project Website	www.arm-project.eu



Information Suppression: Does it belong to FIMI?

Table of Contents

Abstract.....	2
1. Introduction.....	2
2. EU's FIMI countermeasures.....	4
2.1 EEAS Reports on FIMI threats	4
2.2 The Digital Services Act	6
2.3 The Democracy Shield	8
3. Revisiting the scholarship on information manipulation	9
3.1 Censorship: Domestic subtractive practices.....	10
3.2 Propaganda: Additive practices for persuasion or confusion	11
3.3 Sharp power and authoritarian image management	11
3.4 Transnational and practical: Defining information suppression	13
4. Information Suppression practices	14
4.1 Suppression of information production	14
4.2 Suppression of information dissemination.....	15
4.3 Information salience	15
4.4 The importance of context in identifying information suppression.....	17
5. Information suppression: An updated definition	18
6. Conclusions and recommendations	20
7. References	22

Abstract

This working paper offers a conceptualisation of information suppression, outlines its practices and suggests policies to address the phenomenon. It starts by examining how the EU addresses Foreign Information Manipulation and Interference (FIMI) and highlights its insufficient response to information suppression. It first reviews key EU instruments, the EEAS FIMI threat reports, the Digital Services Act and the Democracy Shield, arguing that the privilege of disinformation over silencing of information and the exclusive focus on China and Russia as perpetrator states is preventing the EU from addressing FIMI in an efficient manner. Based on scholarship on information manipulation and the four case studies of the ARM project, the working paper conceptualises information suppression across production, dissemination and salience, including transnational effects on diasporas. It warns against an overbroad “FIMI-isation” that risks blocking merely undesirable content and securitising diaspora communities, thereby undermining fundamental rights. It calls for integrating information suppression into the FIMI Toolbox through better awareness, cross-institutional coordination and attention to transnational repression, so that EU policy can simultaneously counter foreign threats and protect freedom of expression and democratic participation in Europe.

1. Introduction

A central part of authoritarian practices across regimes is to use information as a way of sustaining their power. Disinformation, widely discussed as the most direct way to manipulate and push forward information for political ends, is a well-researched phenomenon addressed by numerous policies and regulations. A less visible domain of information manipulation - *information suppression*, or the deliberate silencing and hiding of information - is much less researched and has gained little attention from policy and practice. Although specific practices of information suppression, such as censorship or astroturfing, are well-known parts of the authoritarian playbook, we still lack systematic knowledge on other forms of information suppression, as well a systematic theorization of this concept. The Horizon-funded research project *ARM: Research for Information Freedom*¹ is dedicated to conceptualising and exploring information suppression strategies, aiming at filling a gap that spans scholarship, policy and practice. ARM started its work in 2024 with a provisional definition of information suppression: *‘a set of actions to silence information with the purpose of muting dissenting voices or*

¹ ARM is funded by the 2024 EU Horizon call ‘Standing up for democracy’ within the research destination ‘Innovative research on democracy and governance’ (Cluster 2 Culture, Creativity and Inclusive Society). The call provided funding for research to be conducted with the explicit aim of both conceptualizing and documenting tactics and techniques of information suppression. In this call, Russia was explicitly mentioned in addition to China as a potential threat actor, and it was opening for other cases to be explored, with emphasis on diaspora groups in Europe. The ARM project was one of three projects which got funding, including analyses of Rwanda and Ethiopia in addition to China and Russia.

*narratives within and outside a country's borders, serving the interest of strengthening a regime's grip on power.'*²

This definition was formulated in conversation with what the European External Action Service (EEAS) is defining as Foreign Information Manipulation and Interference (FIMI), as '*a mostly non-illegal pattern of behaviour 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, by state or non-state actors, including their proxies inside and outside of their own territory.*'³ The starting point and rationale for EEAS's FIMI work is EU's interest in containing foreign influence 'in defence of fundamental rights and European values' (EEAS 2023). Since the launch of the concept in 2021, FIMI has been picked up by researchers and civil society working within the information field, and has been both criticised and hailed for its conceptual innovation.

In dialogue with the FIMI definition, the ARM team agreed that information suppression, while not always coordinated or coerced from above, serves the interest of regimes in preserving power. Information suppression can be either intentionally planned and enacted by governmental actors, or can result from social norms and cultural practices influencing what information should be suppressed or freely distributed by individuals or groups that act without direct pressure from state actors. In line with the FIMI definition, we emphasised its transnational character, highlighting the link between domestic and global tactics of information suppression, with diaspora groups as both agents and targets. In policy terms, we stressed the importance of avoiding labelling of diasporas as threats, as labelling can ultimately endanger their civil and political rights, thereby challenging the original objective of fighting FIMI – to protect the fundamental rights for all. Finally, we identified information suppression strategies operating within three different spheres: information production, information dissemination, and information salience. All these spheres reach across national borders, highlighting the links and overlaps between domestic and foreign information suppression. We considered transnational repression, how authoritarian regimes strive to control diasporas outside their borders, as an important element in all three spheres.

This working paper starts with a recap of EU's policies on FIMI and the (so-far) lacking European response to information suppression. It follows with a revisit of the scholarship relevant for information suppression as an authoritarian strategy. It then moves on to describe some of the main practices of the suppression of information production, dissemination and salience we found across the four case studies covered by the ARM project, including their respective diasporas, paving the way for a modified conceptualisation of information suppression. The working paper concludes with a set of recommendations: what our findings and the modified understanding of information suppression should mean for EU policy.

² ARM Policy Brief no 1 'Information Suppression' <https://www.arm-project.eu/publication/information-suppression/>

³ European External Action Services (2022) '1st EEAS Report on Foreign Information Manipulation and Interference Threats Towards a framework for networked defence February 2022', https://www.eeas.europa.eu/eeas/1st-eeas-report-foreign-information-manipulation-and-interference-threats_en

2. EU's FIMI countermeasures

EU's work against information manipulation and interference got traction with the Russian annexation of Crimea in 2014 (Proto et.al. 2025). Disinformation was conceptualised as a *foreign* threat and was therefore sorted as a responsibility of the European External Action Services (EEAS), EU's diplomatic corps and foreign service. From 2021, the EEAS launched the concept of Foreign Information Manipulation and Interference (FIMI), re-affirming the external dimension and widening its conceptual scope.

EEAS' FIMI definition has come under scrutiny from many different sides. Its security orientation and alignment with the concept of 'information warfare' and hybrid threats (Buvarp 2023) has been criticised for reducing complex communicative processes to binary notions of attack and defence (Wagnsson et.al. 2025), seeing communication as a unidirectional process, neglecting the interplay between sender and receiver (Proto et.al. 2025) and the importance of context (Aalen and Lemaire 2024). On the one hand, by including mostly *non-illegal* patterns of behaviour it has been accused of being too wide, opening for new restrictions on freedom of expression. By containing legal, but undesirable information in the name of fighting FIMI, this can create dangerous precedent (Vérter 2025). On the other hand, it has been blamed for being too narrow. In theory, FIMI is incorporating different kinds of manipulative behaviours that threaten democratic processes and public trust within the information field. But its practice has been continuing to focus on foreign disinformation, mostly in the online domain. While conceptually relevant for all kinds of actors, it has continued to concentrate on two authoritarian states, Russia and China, reflecting EU's geopolitical priorities (Henin 2023), paying little attention to other authoritarian actors, in both autocratic and democratic regimes.

This narrow application of FIMI, practically limiting it to the threats of online *disinformation* from two key actors - China and Russia - has in the last two years started to change. In the following sections, we will present key points from the EEAS's four reports on FIMI threats, released in the period from 2023 to 2026, illustrating a gradually widening approach to FIMI, explicitly including information suppression in addition to disinformation in its two latest reports. While their geopolitical focus on China and Russia has remained in place, the later reports have included analysis of Russian and Chinese FIMI campaigns beyond Europe, with examples from West-Africa and the Middle East. A challenge with a wider conceptual scope, however, is the risk of 'FIMI-ising' a much broader range of activities than before, thereby throwing suspicion on actors and potentially introducing undue restrictions on fundamental rights. With this challenge in mind, it is thus critical to carefully craft policies that can protect against FIMI while at the same time protecting the rights of all citizens in Europe.

2.1 EEAS Reports on FIMI threats

Since 2023, the EEAS has developed and expanded its FIMI framework through the publication of annual reports focused on FIMI threats. Starting with establishing basic analytical standards and methods on how to analyse FIMI with the first report (2023), the fourth and latest report (2026) includes an applied framework for deterring FIMI campaigns. Each report has attempts to answer core questions related to FIMI: 'How to analyse it?' (1st), 'How to respond to it?' (2nd), 'How to expose it?' (3rd), and finally 'How to deter it?' (4th). The four reports have

also tracked an important technological shift that has taken place within digital ecosystems over the course of the years. While social media platforms remain a constant core channel of dissemination, their relative relevance changes alongside shifts in governance and geopolitics - for example, Elon Musk's acquisition of Twitter is clearly reflected by an increasing centrality of X as a FIMI channel (EEAS 2025). Another important technological advancement emphasized by the reports is the popularisation of AI-powered tools such as Large Language Models (LLMs) and audiovisual generators, which were not even mentioned in the 2023 report (in spite of its recognition of fabricated images and impersonation as key FIMI strategies), then became recognized as emerging but "not (yet) the biggest threat" (EEAS 2024), acquired more relevance as they became more affordable and accessible (EEAS 2025) and were finally recognized as "the new norm" in FIMI (Kallas, in EEAS 2026). These technological shifts, resulting in phenomena like cross-platform coordination, mass-scale synthetic media dissemination and LLM grooming, have also prompted a reorientation of FIMI research away from a narrow focus on disinformation to other forms of information manipulation such as flooding, impersonation and distraction, and a gradual realisation that the suppression of information in various forms is also a key aspect of FIMI.

Informed by the DISARM framework to document and deter disinformation campaigns⁴, the FIMI framework is built to analyse manipulative behaviours regardless of who commits them. Using the DISARM methodology, it tracks how an operation is carried out through the identification of Tactics, Techniques, and Procedures (TTPs) rather than who is doing it. Tactics describe the operational goals that the actors try to achieve, the techniques are the actions depicting how they try to accomplish them, and the procedures are the specific combinations of techniques across multiple tactics that indicate intent.

While theoretically actor-agnostic, all four reports have practically continued to focus heavily on what EU defines as specific high-risk states, Russia and China, making the FIMI reports appear as strongly strategic and geopolitically driven. This is of course understandable, as the institution behind the reports, the EEAS, is the diplomatic arm of the EU, carrying out its foreign and security policy. One of its primary objectives is to counter the foreign adversaries actively trying to destabilize European democratic processes. Still, the exclusive focus on China and Russia may reduce EU's capacity to protect European citizens affected by FIMI from other regimes, something the ARM project draws attention to by including two additional cases into our investigations, Rwanda and Ethiopia. These two states have FIMI capacity and target their diasporas in Europe by transnational repression, even though they are not global actors comparable to China and Russia. Other studies have emphasised the role of Iran, with similar capacities to conduct FIMI operations as Russia and China (Calderon et.al. 2025).

The 3rd and 4th FIMI reports have however expanded the focus area of FIMI operations beyond the EU, to Russian operations in Ukraine, Moldova, Armenia, Syria, and the Sahel region in Africa. While this is useful for understanding the geographical spread of FIMI operations beyond Europe and how such operations in other continents may have an indirect effect on European interests and values, it is nevertheless continuing its narrow understanding of

⁴ DISARM Foundation, 2026 'DISARM helps identify and respond to malign information influence operations' <https://www.disarm.foundation/>

perpetrator states. Despite critical changes in the geopolitical situation with the second Trump administration and the wars in the Middle East, for example, none of the FIMI reports attribute information manipulation or interference to the United States, Israel, or any other Western countries. Instead, the United States and European states are discussed strictly within two categories: targets of foreign interference or strategic partners collaborating on a unified defence framework. For example, in the 4th Report, the data highlights how democratic societies are actively targeted by hostile networks to weaken transatlantic relationships and exploit domestic issues (EEAS 2026: 10).

Another change from the 1st report of 2023 to the 4th edition in 2026 is the increased focus on tactics and techniques that leverage artificial intelligence, to accelerate content production and scale up influence activities in a more cost-effective manner using for example bots/coordinated inauthentic behaviour and deepfakes. There is also an increased focus on digital infrastructure and the platforms and service providers used by threat actors, demonstrating a shift in view on platform companies from passive, opaque vehicles in 2023 to critical infrastructure intermediaries actively enabling FIMI by 2026. This development has been running in parallel with the regulatory and legal development within the EU, moving from addressing a lack of data transparency to demanding structural accountability for algorithmic amplification and AI weaponisation with the Digital Services Act (DSA) (see more on the DSA below).

While the EEAS definition of FIMI, consistent throughout its four yearly reports, encompasses a broad set of manipulative and deceptive behaviours, the majority of FIMI cases presented in all the four reports are examples of disinformation tactics and techniques. The concept of information suppression only appears in the 3rd and 4th reports. The 3rd report refers to information suppression as a key strategy for China, linking it to transnational repression, but offers no analysis of information suppression related to other states. The 4th report provides for the first time a definition of Transnational Information Suppression in the glossary of key terms related to FIMI:

The intentional action by threat actors and their proxies to suppress unwanted information with the aim to shape global narratives and norms in their favour. For this purpose, states apply a combination of technological, psychological, legal, and economic tactics. These tactics include active censorship measures and inducing self-censorship through systemic surveillance. (2026, 4)

While this general definition of transnational information suppression indicates an actor-agnostic understanding of the phenomenon, it hinges on the intentionality of “threat actors and their proxies”, something that is extremely difficult to assess. Further, it is only discussed in relation to China as a threat actor in the report, thereby limiting the reach of the definition, and missing the opportunity to engage with the phenomenon more critically, which in turns makes it more difficult to identify effective response strategies.

2.2 The Digital Services Act

The Digital Services Act (DSA), coming into force in November 2022, the European Union’s regulation of digital services is designed to make the online space transparent and safe for

users, protecting fundamental rights (DSA2022). While it was not designed solely as a countermeasure against FIMI, it is relevant as it focuses on the spread of disinformation and the societal risks with its dissemination (Hofman and Raue 2023). It imposes obligations on all online service providers in the EU, but the roles of Very Large Online Platforms (VLOPs) and Very Large Online Search Engines (VLOSEs) covering more than 45 million users per months in the EU, such as Meta, X, TikTok, and YouTube, are particularly highlighted (Art.33). The VLOPs and VLOSEs are made accountable for how their services may be used to disseminate or amplify misleading or deceptive content (Art. 34 and 45). They are therefore required to provide access to repositories of advertisements and manipulative content, including information about who paid for the advertisement (Art.39). Such repositories can facilitate the work of administrations, academics, and civil society organisations focusing on identifying and assessing foreign information manipulation and interference and uncovering potential perpetrators.⁵

The DSA, holding platform companies accountable for spreading disinformation and other malign content, has however led to worries of increased censorship and over-moderation in Europe, indirectly weakening the freedom of expression. This is parallel to the criticism of the broad definition of FIMI as *mostly non illegal*, which implies that not only illegal, but also undesirable content is removed through the imposition of the DSA. Describing this as the chilling effect of the DSA, the EU member states Ireland, Finland, and Sweden have during legal debates in the preparation of the DSA raised concerns regarding the broad, automated content-removal mechanisms of the regulation (Politico 2021). They have highlighted the risk that algorithmic filtering or automated content takedowns could result in over-blocking, where legal and legitimate speech is mistakenly removed to avoid compliance fines and advocated therefore for strict human and judicial review for content blocks, rather than relying on automated upload filters. This concern was also raised by ARTICLE 19, an international NGO working for digital rights and free speech. Because the FIMI framework directly feeds into the enforcement mechanisms of the DSA, ARTICLE 19's critiques focus on how the EU's approach altogether creates structural dangers for legitimate public speech (ARTICLE 19, 2026).

Some of worries of over-blocking is however mitigated by the DSA requiring platforms to notify users clearly and explain the reasons ('statement of reasons') whenever their content is removed or access is restricted (Art. 17a). It also requires that VLOPs must be transparent about their recommender systems. This is to curb unannounced algorithmic suppression or 'shadow banning' - restricting the visibility of a user's account or posts without notifying them (Art. 27). Implementing these articles requires a clear follow up, fining actors not only for the spread of undesirable information, but also for the removal or suppression of information. As pointed out in several analyses of the DSA implementation, there are some worrying signs as to how the platform companies will actually be held accountable and do what the DSA demands. Alphabet Inc (owner of Google and YouTube) has for instance opted out of parts of

⁵ In addition to the DSA, there are other relevant EU codes and acts that target FIMI. These are the European Media Freedom Act considering high quality media as a remedy against FIMI and offers specific protection of independent journalism (Bleyer-Simon 2025, RSF 2024) and the Artificial Intelligence Act, laying down harmonised rules for trustworthy and human-centric AI in the EU (Linera and Mauwese 2025).

the Code of Conduct on Disinformation as part of the DSA, parts that they deem as not relevant, proportionate or effective (Bleyer-Simon 2025).

2.3 The Democracy Shield

In November 2025, the EU Commission and the High Representative published a joint communication on the 'European Democratic Shield: Empowering Strong and Resilient Democracies'. The initiative, developed jointly by the European Commission and the EEAS, aimed at boosting the protection of democracy against attacks (Bentzen 2026). It includes three priority areas or pillars: 1. Reinforcing situational awareness and support response capacity to safeguard the integrity of the information space, 2. Strengthening democratic institutions, free and fair elections and free and independent media, 3. Boosting societal resilience and citizens' engagement (European Commission 2025).

The first pillar on safeguarding the integrity of the information space mentions foreign information manipulation and interference (FIMI) and disinformation as two of the main threats against democracy in the EU. The second pillar focuses on countering FIMI to protect electoral processes and independent media from both internal and external challenges to elections in Europe. Finally, the third pillar on societal resilience is mentioning basic skill support schemes for schools, including citizenship and digital skills; and a media resilience programme for all age groups across rural and urban areas - to bolster democracy and contain malign foreign influence.

In many ways, the Democracy Shield shares the same blueprint as the EEAS' FIMI reports and the DSA, with a similar scope and limitations: it focuses on online disinformation rather than addressing foreign interference more broadly. The document describes how a Blueprint for countering FIMI and Disinformation will be prepared, again indicating a focus on disinformation rather than other forms of FIMI, such as information suppression. A quantitative analysis of the content of the Democracy Shield document shows for instance that disinformation is mentioned 61 times in the document, while FIMI is mentioned 43 times. More problematically, Information suppression, an important aspect of FIMI, is not mentioned at all. Russia is the only identified threat actor, while China is not explicitly mentioned. While highlighting unspecified internal threats to democracy, the US and US based tech companies are not recognized as emerging FIMI actors. The Democracy Shield, as the EEAS FIMI threat reports and the DSA, must therefore be seen as a product of strategic manoeuvring by the EU in a world where the threat from Russia is seen as the most acute and the relationship to both China and the US should be kept warm.

The Democracy Shield recognises and describes the challenges coming from social media platforms and the way algorithmic systems contribute to FIMI, but is criticised for being vague on platform companies' specific responsibilities. It identifies how engagement-based ranking and manual manipulation pose a systemic risk to civic discourse and electoral processes, and offers strong proposals for fact-checking and media literacy initiatives. At the same time, it suggests little to force social media companies to act and mitigate issues (Stollmeyer and Geese 2026) and therefore fails to identify platform companies as enablers and actors in FIMI, especially in contrast to the accountability of VLOPs and VLOSEs imposed by the DSA. Instead, the Democracy Shield proposes a strengthening of voluntary coordination and

information-sharing structures as soft-law guidance, without providing much detail on how or when the EU plans to implement them (Quaritsch 2026). This could again be a result of strategic manoeuvring to balance the need to regulate international platform companies without disrupting their commercial presence in the region.

As part of the Democracy Shield, a European Centre for Democratic Resilience is launched to bring together expertise across member states, EU candidate countries and potential candidates, as well as EU institutions, offices and agencies including the EEAS. The Centre will host a stakeholder platform for dialogue with civil society, academic researchers, media providers, and a new European network of fact-checkers (Bentzen 2026), the latter indicating a continuing emphasis on disinformation as compared to other forms of FIMI. The establishment of this Centre has however been criticised for overlapping with the already existing EEAS Rapid Alert System, and it is not clear how the division of labour between these units will be structured (Quaritsch 2026). As it has only been recently established, it is yet unknown how the Centre will deal with FIMI threats in practice, and it remains to be seen whether the EEAS' recent inclusion of transnational information suppression as part of FIMI will be followed up through the Centre's operational cooperation to counter common threats.

3. Revisiting the scholarship on information manipulation

The knowledge gap on information suppression is not limited to EU policy and practice, but is also reflected in the scholarly literature on information manipulation. One exception is the suppression of *scientific* research, which has been extensively discussed in the field of social studies of science, highlighting important features of how information is suppressed by powerful actors (Delborne, 2016; Martin, 1999). These findings have not yet been expanded to the domain of transnational influence. It is not surprising that the deliberate suppression of information beyond borders is rarely discussed: as pioneering studies of suppression in science have argued, suppression is difficult to study as it is characterized by both discretion and contingency; its targets might not want or be in a position to report it, and its operations might not be visible to outside observers (Martin 1999, 122). In this working paper, we contribute to the study of suppression beyond scientific knowledge, underlining its impact on information and its transnational operation.

As we expand the analytical purchase of information suppression as a concept beyond the narrow domain of scientific knowledge production, we also emphasise the need to incorporate the interplay between its online and the offline dimensions. While the recent theorizations of concepts such as “digital authoritarianism” (T. Roberts and Oosterom 2024) have examined the control of online activities through the lens of authoritarian practices, these tend to focus solely on the digital domain and fail to consider other spheres such as traditional media, in-person interaction, hearsay, and other channels of suppression. There is, however, a longer scholarly tradition focusing on various ways of controlling domestic information environments such as censorship and propaganda, which we summarise in the following sections in order to ground our definition of information suppression.

3.1 Censorship: Domestic subtractive practices

Censorship can be defined as the restriction of public expression or of public access to information by an authority when the information is thought to have the capacity to undermine the authority by making it accountable to the public (M. E. Roberts 2018, 37). It involves a variety of mechanisms to ensure that information deemed damaging for the regime is subtracted from the public domain or does not circulate widely, thereby limiting the regime's accountability towards the citizenry, making coordination among citizens difficult, and facilitating regime survival (McMillan and Zoido 2004, 87).

Censorship targets both traditional media, for example by shutting down, regulating or restaffing newspapers and other media outlets (Gohdes 2024, 6), and the online realm, through website blockages or requesting content to be taken down. The latter offers a more centralized, low cost, and responsive way of controlling information, opening up possibilities for the simultaneous censorship of individuals and media outlets (Gohdes 2024, 6). Online censorship has been at the heart of recent scholarship on censorship, which has focused on classifying techniques (Deibert et al. 2010; M. E. Roberts 2018; Sanovich et al. 2018; Keremoğlu and Weidmann 2020) and identifying effects (Pearce et al. 2014; Hobbs and Roberts 2018; Falisse and Nkengurutse 2019; Pan and Roberts 2020; Lemaire 2024).

While that scholarship has proposed different ways to catalogue and classify the techniques used to control the online realm, including by considering offline activities that can restrict access to online content, there have been fewer efforts to consider censorship as a phenomenon that can occur online and offline simultaneously – that is, considering censorship of *information*, rather than censorship of a specific medium or activity. The framework proposed by Roberts (2018) to analyse the phenomenon – although mainly applied to online information – could be usefully deployed to analyse other types of information, including news media and academic research. Her typology differentiates between the mechanisms of fear, friction, and flooding (M. E. Roberts 2018, 41–44), enabling researchers to consider censorship as a system beyond the centralized vision of an information killswitch independent of the medium being targeted. For example, fear-based mechanisms include arresting researchers (Thomson 2011), passing legislation that considers a range of journalistic activities as cybercrime (Cross 2019), or imposing restrictive conditions to obtain research permits and visas on researchers (Jessee 2012). Friction consist in making information more difficult to access or produce, for example by blocking websites (M. E. Roberts 2018, 56–58), or by making data difficult to collect or inaccessible (M. E. Roberts 2018, 66–67) – practices in line with the phenomenon of evidence censorship (Shao et al. 2024). Lastly, flooding designates the phenomenon of diverting audiences from sensitive information by submerging it with other information less troubling for (or even supportive of) the censor (Roberts 2018, 80).

The typology of fear, friction and flooding offers the possibility to focus on mechanisms regardless of the media they are applied to – and in fact, concerns censoring both access to and sharing of information. It focuses on how mechanisms affect citizens, and a single mechanism can be understood as belonging to each of the categories. It also allows for exploring a variety of censorship actors, including states and non-state actors such as platform companies.

3.2 Propaganda: Additive practices for persuasion or confusion

Propaganda consists of “manipulating or misleading a target population by affecting its beliefs, attitudes, or preferences to obtain behaviour compliant with the political goals of the propagandist” (Benkler et al. 2018, 29). It has traditionally been seen to push information, not suppress it. Propaganda can involve pushing disinformation – that is, intentionally false or misleading information (Benkler et al. 2018, 32; Wardle and Derakhshan 2017, 5). Propaganda is often deployed in combination with censorship, to maximize its effect (Geddes and Zaller 1989, 319).

Recently, research has enriched the study of propaganda by identifying a different type: “hard propaganda”, understood as egregious, obvious propaganda, that is used by a regime to signal its strength to citizens (Huang 2015), showing that while such propaganda can deter protests in the short run, it also lowers regime legitimacy in the eyes of citizens (Huang 2018; Lutscher and Donnay 2024). Hard propaganda may fail to persuade its audience of its messages, induce scepticism, leading to a form of backlash (Rosenfeld and Wallace 2024).

By contrast, propaganda that tries to legitimize regime action can also be effective, particularly when the regime manages to set the agenda – that is, to shift political discussions from issues where it underperformed to issues it owns (Aytaç 2021). This strategy relies on distraction to other political issues (Boussalis et al. 2023), or even to non-political content (Morozov 2012, 70–72). This type of distraction leads a population to pay less attention to another subject, thereby suppressing information around it, as highlighted in work focusing on Chinese techniques to control online media (King et al. 2017). The distraction will then lead people to lose the capacity to develop a politically informed opinion (Benkler et al. 2018, 35). Propaganda can also disorientate – making it impossible for audiences to tell truth from non-truth. The aim is not necessarily to convince people, but to leave them in a state of confusion and passivity. It is important to note that propaganda has become cheaper with the Internet – as regimes can leverage social media to spread pre-packaged information much more cheaply, for example by using bots, or paying users to spread content (M. E. Roberts 2018, 88–92).

Thus, censorship and propaganda go hand in hand, and enable states to control the flow of information to ensure they contain threats to their survival (Converse 1985). It is important to note that both terms are pejorative – meaning that they are seen as inherently bad, and attribute bad intentions to the censor or the propagandist, even as, in some cases, these tools can be legitimately used (Wanless and Pamment 2019; Meserve and Pemstein 2019).

3.3 Sharp power and authoritarian image management

Most definitions of censorship and propaganda consider the control of information by states domestically, that is, within state borders. Other concepts need to be mobilized when considering censorship and propaganda in a transnational context. Indeed, states face threats to their survival from inside, but also from the outside – and this is particularly the case for

authoritarian regimes (Greitens 2016, 19). Controlling the flow of information on the international stage is at the heart of the concept of soft power: the ability for a state to leverage its cultural clout to influence other countries (Nye 1990, 168), which does not involve coercion such as propaganda or censorship (Nye 2019, 18). The concept of “sharp power”, however, developed in conversation with the soft power literature, encompasses state actions that “involve efforts at censorship, or the use of manipulation to sap the integrity of independent institutions” (Walker 2018, 11). The limit between soft and sharp power can however be porous, for example in the case of state-funded (dis)information channel *Russia Today*, which was originally launched to promote a positive image of Russia but became a tool for manipulating public opinion abroad with the aim of influencing domestic politics of other states (Elsawah and Howard 2020).

The neighbouring concept of “authoritarian image management” (Dukalskis 2021, 4–5), describes efforts targeted at foreign audiences to enhance the legitimacy of authoritarian regimes and ensure their survival. Such efforts can be promotional or obstructive, and diffuse (aiming at foreign citizens generally) or specific, i.e. targeted at specific types of individuals abroad (Dukalskis 2021, 40). The concept does exclude some forms of soft power – those that are not directly related to state politics, for example promoting tourism (Dukalskis 2021, 7–8), thereby risking to miss cases where content is produced to create diversion. It only considers activities conducted by state authorities and their proxies abroad or targeting foreigners.

Authoritarian image management thus covers many aspects of censorship and propaganda applied in a transnational setting, particularly by including cases of transnational repression – when a regime represses its citizens after they have emigrated, for example by threatening family members, withholding passports, by organizing assassinations of opponents abroad, or by leveraging digital tools (Moss 2016; Michaelsen 2018). But transnational repression is restricted to activities by states or their agents targeting that state’s diaspora (Dukalskis et al. 2022), particularly, but not only, human rights activists and journalists in exile (Schenkkan 2025).

The concept of authoritarian image management was developed to analyse the practices of authoritarian regimes, neglecting to focus on democracies. Transnational repression studies had the same point of departure, but has later come to argue that democratic states can also be perpetrators of transnational repression. Specifically, democratic states can facilitate authoritarian practices by creating new norms that enable transnational repression (for example, the war on terror) (Schenkkan 2025, 40) or by collaborating with perpetrating states. However, transnational repression focuses on those practices that target diaspora members. Authoritarian image management focuses most directly on how states control the flow of information beyond their borders – something akin to Foreign Information Manipulation and Interference and foreign influence operations. However, it differs from FIMI in that it presupposes that only authoritarian states engage in the behaviour, and it narrowly focuses on the central authorities managing how they are perceived. By contrast, the concept of FIMI is broader, as it includes activities that support state survival beyond simply projecting a positive image, and as it opens for less centrally coordinated activities (EEAS 2021; Hénin 2023).

3.4 Transnational and practical: Defining information suppression

As discussed above, scholarship has grappled with the questions on how states ensure their survival via censorship, propaganda, and repression, deployed domestically and transnationally. Most of the actions considered by this scholarship can be organized under different concepts: for example, the physical repression of journalists or activists does constitute a form of censorship, but it can also be used for propaganda purposes. Adopting the approach of studying authoritarian and illiberal practices makes it possible to overcome limitations stemming from the normative focus on authoritarian regimes, while also considering practices beyond those strictly deployed by states within territorial borders or towards their citizens (Glasius 2018), such as the suppressing practices of platform companies or regime loyal individuals or groups of activists, digital vigilantes and volunteers. This approach considers that actors disrupt accountability processes in a system by disabling access to information and disabling voice – which constitute authoritarian practices, and that they might do so by infringing on individuals' autonomy and dignity – defined as illiberal practices (Glasius 2018, 531). An underlying assumption is that by disrupting accountability processes, actors hope to ensure the system's survival. Information is central in these accountability processes (O'Donnell 1998; Glasius 2018).

In dialogue with interdisciplinary conceptualizations of censorship, propaganda, authoritarian image management and transnational repression, we proposed the concept of information suppression to make it possible to consider transnational practices geared towards the stifling of information and their effects in the contexts where they are deployed. In our definition, information suppression is a set of practices deployed to silence information with the purpose of muting dissenting voices or narratives outside a country's borders, and it covers a blind spot in current theorizations of foreign information manipulation and interference. By simply focusing on disinformation, this field has not managed to capture other critical means that states deploy to strengthen a regime's grip on power. In our initial definition, information suppression has two key characteristics: it is both *intentional* and *transnational*. By intentional, we meant that it results from a strategy deployed by a regime to serve its interests. However, this does not mean that information suppression is always coordinated or coerced from above. Rather, regime policies can also foster actions by private organizations and individuals that lead to information suppression. With transnational, we meant to highlight the link between domestic and global tactics of information suppression, with various social groups acting as both agents and targets.⁶ Here transnational does not simply refer to the repressive practices reaching a target across borders (often from an authoritarian regime into a democratic context), but also points to more complex chains of agency spanning grey areas between national jurisdictions and larger technological ecosystems operating at a supranational scale. Following our initial definition, which we developed from a detailed review of relevant literature across

⁶ these features are also highlighted in European External Action Services' definition of FIMI. See EEAS (2023) '1st EEAS Report on Foreign Information Manipulation and Interference Threats' www.eeas.europa.eu

fields, we identified and analyzed practices of information suppression across different national case studies, with the aim of updating our definition based on this empirical work.

4. Information Suppression practices

To identify information suppression, we centre our investigations on information, rather than on specific types of efforts deployed by states or their agents. This means that we focus on the information space, which is affected by suppression, in order to be able to identify suppression practices. To do so, we consider suppression at three different levels: production, dissemination, and salience of information. We understand the level of production as including all aspects linked to the production of information or knowledge, such as collecting evidence, conducting interviews, being able to travel, film or record. Typical producers of information are journalists as well as activists (for example human rights defenders) and academics (who produce knowledge). The dissemination level includes aspects related to sharing information (via publication in the media, including online, as well as through policy reports, scientific articles, and via more informal modes of sharing between individuals). Typical actors in information dissemination are journalists and activists, as well as publishers, communicators, or individuals who share information with others. Salience of information describes the extent to which information is visible. Typically, the salience of information can be manipulated by the public, by organized individuals who claim to be part of the public but who coordinate and act inauthentically, or by platforms who can make certain narrative more visible than others. The production, dissemination and salience of information all involve a transnational aspect for information to reach (or not) across borders, underlining the link between domestic and foreign suppression efforts. Looking into each level makes it possible to adopt a more holistic perspective, considering which combination of tactics are used at which level. It also makes it possible to understand how information suppression impacts the production, dissemination, and salience of future information.

4.1 Suppression of information production

Actors suppress the production of information by targeting either individuals or professionals within the media and academic sphere, or human rights defenders. At this stage, suppression of information includes techniques linked to evidence censorship (Shao et al. 2024). Making data unavailable to journalists, academics, or civil society, refusing to collect data, and / or hindering independent data collection efforts constitute friction-based tactics (M. E. Roberts 2018, 65–71).

Taking on a transnational lens, these types of suppression activities can take various forms, starting with restricting access to the country to outsiders. Visas and research permits can be extremely difficult to obtain, with long and complicated processes, for example in Rwanda (Jessee 2012; Thomson 2009, 110–11). Other examples include the heavy restrictions and constant surveillance foreign correspondents might face, unable to circulate freely, or to select interviewees in North Korea (Seo 2018) and across various authoritarian states in Southeast Asia (Morgenbesser and Weiss 2018). Such restrictions on access to a country do affect the kind of information that can circulate about it beyond its borders.

The production of information can also be suppressed by limiting access to specific types of data, or by manipulating data. For example, there are doubts concerning the validity of GDP data from China (Wallace 2016), or concerning official statistics on poverty in Rwanda (Ansoms et al. 2017) and several other African states (Jerven 2016). Access to archives – an important source material for scholars, journalists, and civil society – can also be denied (Greitens and Truex 2020, 355–56). Here again, the systems of visa and research permit can be used to restrict the type of data – both qualitative and quantitative – that can be collected and limit the production of information.

Additionally, threats and intimidation – fear-based tactics (M. E. Roberts 2018) – can be leveraged to influence the activities of public figures, journalists, activists, and academics, even when they are located beyond borders. For example, the need to secure access can lead actors to select topics of investigation that are more palatable for the regime – as is shown by the type of coverage the Associated Press in North Korea is able to provide, focusing mostly on soft issues (Seo 2018). Many aspects of suppressing the production of information include limiting access to the domestic territory to external actors. We do consider this as part of information suppression, and not only domestic censorship, because the aim is to suppress the production of critical information destined for a foreign audience. This is seen for example in the Ethiopian government's blockage of both internet and international media access to Tigray region during the war there in 2020-22 (Chala and Workneh 2025).

4.2 Suppression of information dissemination

Domestically, censorship as friction can target the dissemination of information, for example by subtractive practices such as closing down traditional and online news outlets, shutting down internet, or targeting private businesses by regulating/restricting digital technology companies. The media and individuals are diverted away from censored information, making certain social media posts, news articles or books difficult to obtain. In a transnational context, exercising surveillance or threatening those who produce information can also lead to the suppression of information at the dissemination stage. Researchers and journalists might be threatened with repercussions if they publish findings that do not fit with a specific narrative (Jessee 2013), leading to information not being disseminated.

Suppression of dissemination can also take the shape of Strategic Lawsuits Against Public Participation (SLAPPs), launched by states or their agents to disrupt the dissemination of critical reporting by journalists or civil society organizations, leveraging legislation of another country to do so (Chubb and Roberts Lye 2024). On a similar note, some regimes have proven that they are adept in using foreign media houses' own safeguard systems to stop the diffusion of material that present competing narratives (Reyntjens 2015), and influencing how academics are able to disseminate their findings (Guichaoua 2020).

4.3 Information salience

After information is produced and disseminated, what can be controlled is the salience of information. Techniques affecting information salience include burying information, diluting narratives, or promoting social norms on what should be talked about and not. The former is

akin to flooding (M. E. Roberts 2018), that is, creating distractions that heighten the relative costs of accessing competing (sensitive) information, or the coordinated production of information by an authority with the intent of competing with or distracting from information the authority would rather citizens not access. Flooding may not only involve complete burial of information, but rather a dilution of certain narratives, mildening its impact, as seen in the Ethiopian government's attempts of undermining the international community's understanding of the Tigray war (2020-22) (Tesfaye and Pohjonen 2025). Scholarship has shown how producing competing narratives can work – for example in the case of promoting a positive image of Rwanda in the United States (Dukalskis 2021, 148–51) or in the United Kingdom (Booth 2010) by using local (American or British) PR firms. These additive practices – where new content is produced – also constitute an example of information suppression, as they are used to bury other information. Providing pre-packaged information to the media is another example, as presented by Brazis and Dukalskis (2019, 569) in a study where they find that news outlets in cities where there is a Confucius Institute⁷ are more positive in their reporting on China.

Influencing the salience of information can also take the shape of coordinated attacks against critical coverage. This is a strategy often deployed online, where the individuals behind news reports, civil society efforts, or academic publications can be personally targeted and attacked, either by real individuals, or by relying on automated publications of content produced using artificial intelligence-based tools (Wack et al. 2024). This type of campaign aims at undermining and subtracting critical information by attacking the legitimacy or trustworthiness of those who produce information. The suppression of salience becomes even more important as technologies like Large Language Models – which are increasingly used to power products like search engines, chatbots, smart assistants, and so on – reproduce the biases intrinsic to their training data, which can be fine-tuned to privilege certain narratives or obfuscate sensitive outputs (Qiu, Zhou & Ferrara, 2026).

Overall, considering information suppression efforts based on the level of the information cycle at which they occur can be combined with Roberts' typology of censorship (2018) to facilitate identification efforts as shown in the examples above and summarized in figure 2. Tactics targeting one part of the information cycle can affect other parts, what we call recursive suppression. Efforts to suppress the dissemination of information or its salience are for example likely to also lead to the suppression of future information production. Similarly, intervening in the production of information leads to the suppression of dissemination and salience. It would also make sense that suppression efforts evolve over time, once information production has been suppressed in large parts, states can focus on the few remaining efforts to disseminate competing or sensitive information by simply targeting its salience stage in a more automated and cost-effective way.

⁷ Confucius Institutes are funded by China in universities abroad to facilitate language education and cultural exchanges.

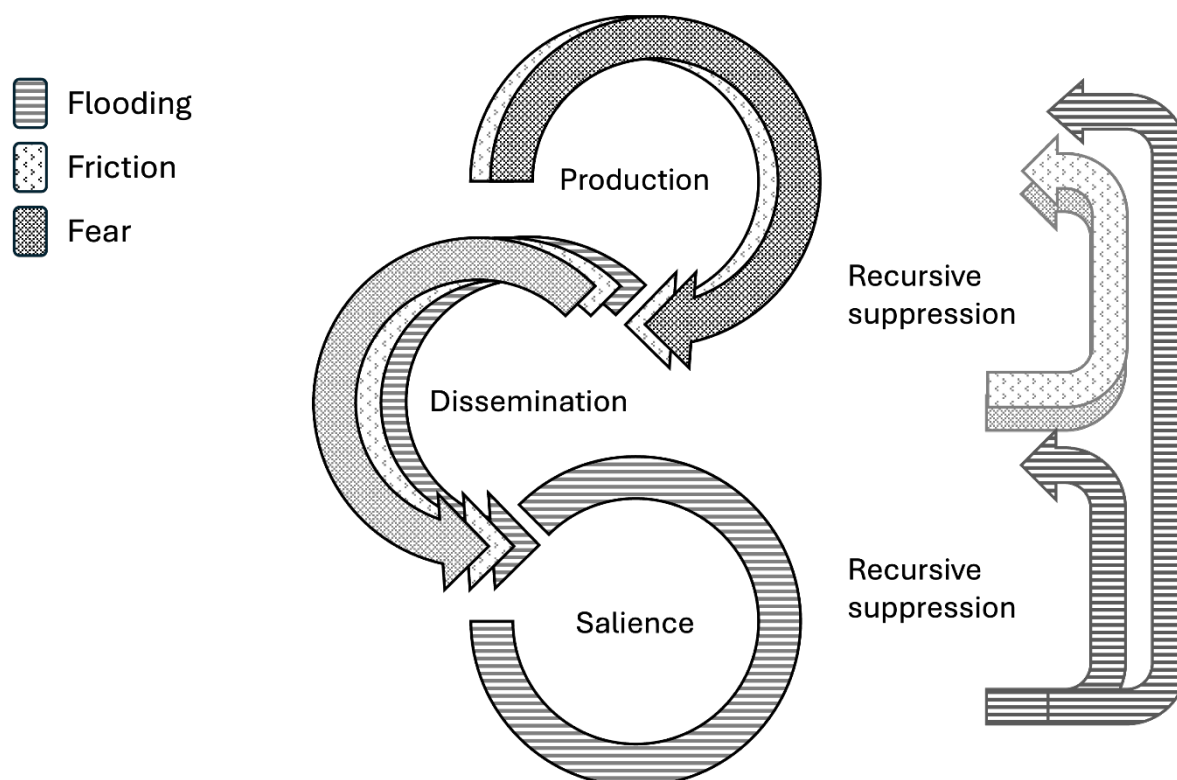


Figure 1 Information suppression practices and the information cycle

4.4 The importance of context in identifying information suppression

Practices suppressing information include a wide range of activities operating at different levels, making it difficult for external observers to identify them in a systematic manner, and for analysts to evaluate their effect on public opinion in targeted countries. We argue that methodological pluralism, combined with in-depth contextual knowledge, are needed to identify the tactics deployed to suppress information.

For example, efforts at suppressing the production of information have been identified through autoethnographic reflection about visa and administrative processes (Jessee 2012; Thomson 2009, 110–11), the combination of statistical analyses and in-depth in-country fieldwork used to demonstrate manipulation of official figures (Ansoms et al. 2017), and interviews of individuals targeted by threats. By contrast, some of the efforts deployed to suppress the dissemination of information can be more easily observed as they happen, as is the case for the closure of websites or media outlets, which can be quantified after they have happened (Lutscher 2023). Other tactics, such as the use of SLAPPs or the misuse of institutional safeguards to limit dissemination, can be identified using qualitative methods such as interviews and document analysis, but methods can be combined to more systematically map out how legal frameworks open up possibilities for these types of abuses (Schumann 2025).

Practices influencing the salience of information have to some extent been more documented, if one considers the blooming field of disinformation and misinformation studies to cover this ground. However, many of these studies focus on cases of flooding without identifying what information might have been buried by such efforts or might have gained more salience because of them. Exceptions come from case studies deploying quantitative tools to analyse campaigns aimed at specific critical reporting efforts (Wack et al. 2024) which are, again, prompted by contextual knowledge of where to look for information suppression.

Contextual knowledge is also needed to identify certain forms of information suppression that are deeply embedded in social pressure and norms, or in cultural practices and expectations about maintaining harmony among citizens or community members. A shared understanding about what should be talked about and not can make citizens both within the regime and in the diaspora actively disengage with certain information even if it is not actively censored, multiplying the effects of information suppression. In the digital domain, digital vigilantes and volunteers, not always acting as direct agents of the state, can be important actors in suppressing information through flooding, as is the case for China's "50-cent party" of paid commentators (Han 2015). This is equally important in the offline domain, which should be seen as contiguous to the online domain: virtual suppression and in-person suppression are often entangled and difficult to separate, with online intimidation leading to self-censorship in the public space, and in-person suppression leading to online self-censorship. This underlines the need to explore the intersection between online and offline arenas of information suppression.

As we have shown, information suppression practices are diverse and target a wide range of information (and knowledge) producers, including journalists, activists, members of diasporas, academics, and lay citizens in the targeted country. Comparative work is needed to be able to connect these practices together and identify them as part of a broader strategy of information suppression.

5. Information suppression: An updated definition

After our initial conceptualisation of information suppression as FIMI, the ARM team conducted in-depth case studies of information suppression practices of four authoritarian regimes, China, Ethiopia, Russia and Rwanda, and their diasporas in Europe. Based on both online sources and qualitative interviews, we identified the tactics and techniques of information suppression, presented in country case working papers and policy briefs and synthesised in a catalogue of Tactics and Techniques.⁸

⁸ See arm-project.eu for all these publications

Through the case studies, we were able to critically evaluate whether our initial conceptualisation of information suppression was still holding water or if it should be re-conceptualised.

- Our case studies reinforced our initial hunch that **offline dynamics and social and cultural norms** are key for how information suppression strategies are accepted, internalised and practised.
- While our initial definition emphasised intentionality as a key aspect of information suppression, we find that **intentionality is extremely difficult to demonstrate**, and does not account for information suppression that results from cultural norms or internalised practices. This is important as we also see that information suppression evolves over time, to focus less on the production of critical information and more on the salience of the little critical information that remains.
- In fact, information suppression can also be understood as **the result of illiberal practices including in non-authoritarian contexts**, and sometimes even as the intent is not necessarily to hide information or limit accountability.
- In the digital domain, we found that direct censorship is only one part of suppressing information. **Flooding and other forms of distraction** are equally important tactics and techniques, underlining the importance of studying information salience.
- A new key insight was the role played by **international platform companies as enablers** of information suppression strategies.
- Finally, while transnational repression was found in all the four case studies, we also identified that **non-coercive transnational campaigns with the aim of legitimisation more than repression** were crucial in the regimes' attempts of information control across borders.

Seen together, we argue that our initial conceptualisation still holds water, but the original emphasis on deliberate state action, coordination and coercion should be modified. While information suppression from authoritarian actors, be it regimes or private companies, should be seen as deliberate actions to sustain authoritarian power, the intermediation and reception of information suppression should *also* be understood as a result of non-coerced norm internalisation and self-censorship. We therefore define information suppression as

a set of actions to silence information with the purpose of muting dissenting voices or narratives outside a country's borders. It is transnational, highlighting the link between domestic and global tactics of information suppression, with various social groups acting as both agents and targets. Information suppression can also be the result of illiberal practices, targeting the autonomy and dignity of individuals.

Being aware of the dangers of conceptual stretching and the possible policy implications of a widening of the concept on fundamental rights and freedoms, we therefore propose a carefully crafted set of responses to information suppression with the aim of expanding, and not limiting the freedom of expression. These responses are lined up in the conclusions and recommendations below.

6. Conclusions and recommendations

Coming back to the different FIMI countermeasures that the EU has initiated, described in the outset of this working paper - the EEAS' FIMI threat reports, the Digital Services Act, and the Democracy Shield - we have already identified the need to step up the work against information suppression in addition to disinformation. It is not only manipulative information that is pushed, but also information that is hidden, buried or (self-)censored that should be addressed to protect democracy. The EU policy initiatives are on the right track in the fight against FIMI in terms of focusing on societal resilience and trust-building through media literacy. The DSA's attempt of also making platform companies accountable is an important step in realising how not only states, but also digital infrastructure and tech companies can be key enablers of FIMI.

In the review of EU's anti-FIMI initiatives, we have however noted the risks of 'FIMI'isation' of new types of behaviour. In the fight against foreign threats, not only illegal, but also undesirable information risks being blocked or diaspora groups labelled as security threats, ultimately undermining the fundamental rights that the fight against FIMI is supposed to protect. **Policies against FIMI therefore needs to balance the concern for protecting European governments from threat actors and the need to protect European citizens from undue limits on freedom of expression.**

EU's main action points against FIMI are summed up in **FIMI Toolbox** (Friedman and Boucher 2025): focusing on situational awareness (monitoring and detection, collection of evidence, investigation and information sharing), resilience building (strategic communication, capacity building), disruption and regulation (laws and policies aiming at preventing and deterring), and diplomatic responses (international cooperation and/or sanctions on media service providers).

Specifically, on information suppression – there is a **need to add to the FIMI Toolbox awareness creation and coordination on information suppression across institutions, agencies and policy domains**. While disinformation is a well-understood concept within FIMI, much remains to comprehend what information suppression is. This lack of understanding can create colliding policies, one action killing the other – ignoring for example the unintended consequences of regulations on freedom of expression or on alienation or further marginalisation of diaspora groups. Related to this, there is also a need to spread information about **transnational repression** – preventing diasporas from being targets and pressurised to become agents of FIMI (Antis and Michaelsen 2026). Addressing FIMI and transnational repression together enables EU to both combat hybrid threats from outside and to protect citizens from democratic vulnerabilities. The European Centre for Democratic Resilience can be one important arena for such awareness creation and policy coordination at the European level.

Being vocal and reactive about Western FIMI operations – from for example the USA or Israel - is a way of increasing the trustworthiness and credibility of EU as principled, consistent and actor-agnostic in their fight against FIMI and transnational repression. The emerging and possibly malign foreign influence from these two actors should not be silenced, but instead confronted and publicly debated.

One way of creating concrete and balanced policies is to focus on the three spheres where information suppression takes place, in the production, dissemination and salience of

information, and among diaspora groups in Europe. While much of the efforts should concentrate on Europe, some policies should also target the governments in which the information suppression operations are originating from, for example through development aid tailor-made for the information field.

To secure free **information production**, the independence of key media and civil society institutions should be supported. This includes:

- Providing legal and technical support to civil society and media organisations, including those working on fact-checking and digital literacy, both in Europe and in the countries where FIMI operations are originating from.
- Providing protection for journalists, offering asylum pathways, legal aid, and capacity building programs for exiled journalists, while condemning harassment and violence targeting media professionals.
- Strengthening academic and civil society collaboration, funding academic and civil society initiatives that promote independent research and reporting, while advocating against laws restricting CSO operations.

To secure free **information dissemination**, initiatives that contribute to transparent circulation of online and offline information should be supported. This includes:

- Pushing for clear rules for platform moderation and transparency in the decisions made.
- Tying European aid, especially technology-related development support, to transparency about the government's use of technology and AI.
- Addressing online harassment: partner with both European and overseas stakeholders to combat digital harassment, ensuring the safety of journalists and activists in online spaces.

To ensure that the management of **information salience** is not undermining freedom of information and expression, initiatives that hinder digital manipulation should be supported. This includes:

- Pressing major social media platforms to add additional resources and language capacity in smaller languages for their content moderation mechanism, to prevent the misuse of platform reporting mechanisms for political purposes and to honour transparency commitments.
- Tightening international export controls for different surveillance tools.

To protect **diasporas** from being co-opted as agents or becoming victims of information suppression in Europe, initiatives should acknowledge the fears that tie diaspora to authoritarian states. This includes:

- EU policy-makers should invest in understanding the country context so that EU/European countries do not take positions that are seen as paternalistic, undermining the trust from diasporas from these countries.
- Building expertise beyond Russia and China: there is a need for more Africa, Latin America and Middle East expertise in Europe, to continually assess and understand their foreign policies and engagement with their large diaspora.

- Diversifying sources of information: as conflicts in fragile contexts are complex, polarised, and highly contested, there is a need to consult diverse constituencies before taking a position on such conflicts.
- Consulting diasporas in decision making regarding countries, to have a more nuanced perspective and avoid taking positions that sideline and alienate the diaspora.

7. References

- Aalen, Lovise and Pauline Lemaire (2024) 'Information Suppression' ARM Policy Brief no.1 <https://www.arm-project.eu/publication/information-suppression/>
- Ansoms, An, Esther Marijnen, Giuseppe Cioffo, and Jude Murison. 2017. "Statistics versus Livelihoods: Questioning Rwanda's Pathway out of Poverty." *Review of African Political Economy* 44 (151): 47–65. <https://doi.org/10.1080/03056244.2016.1214119>.
- Article 19 (2026) 'EU: Principles for a Human Rights-Centred Application of the DSA' <https://www.article19.org/resources/eu-principles-for-a-human-rights-centred-application-of-the-dsa/>
- Aytaç, Selim Erdem. 2021. "Effectiveness of Incumbent's Strategic Communication during Economic Crisis under Electoral Authoritarianism: Evidence from Turkey." *American Political Science Review* 115 (4): 1517–23. <https://doi.org/10.1017/S0003055421000587>.
- Benkler, Yochai, Robert Farris, and Hal Roberts. 2018. *Network Propaganda: Manipulation, Disinformation, and Radicalization in American Politics*. Oxford University Press. <https://doi.org/10.1093/oso/9780190923624.001.0001>.
- Booth, Robert. 2010. "Does This Picture Make You Think of Rwanda?" Media. *The Guardian*, August 3. <https://www.theguardian.com/media/2010/aug/03/london-pr-rwanda-saudi-arabia>.
- Boussalis, Constantine, Alexander Dukalskis, and Johannes Gerschewski. 2023. "Why It Matters What Autocrats Say: Assessing Competing Theories of Propaganda." *Problems of Post-Communism* 70 (3): 241–52. <https://doi.org/10.1080/10758216.2021.2012199>.
- Brazys, Samuel, and Alexander Dukalskis. 2019. "Rising Powers and Grassroots Image Management: Confucius Institutes and China in the Media." *The Chinese Journal of International Politics*, November 13, poz012. <https://doi.org/10.1093/cjip/poz012>.
- Chala, Endalkachew H., and Téwodros W. Workneh. 2025. "Internet Shutdowns in Ethiopia: Discourses of Digital Sovereignty and Information Suppression amid Political Instability." *New Media & Society*, October 9, 14614448251378981. <https://doi.org/10.1177/14614448251378981>.
- Chubb, Andrew, and Kirsten Roberts Lyer. 2024. "Transnational Human Rights Violations: Addressing the Evolution of Globalized Repression through National Human Rights Institutions." *Journal of Human Rights Practice* 16 (3): 770–93. <https://doi.org/10.1093/jhuman/huae017>.

- Converse, Philip E. 1985. "Power and the Monopoly of Information." *American Political Science Review* 79 (1): 1–9. <https://doi.org/10.2307/1956115>.
- Cross, Charlotte. 2019. "Cybercrime and the Policing of Politics in Tanzania." In *Social Media and Politics in Africa: Democracy, Censorship and Security*, edited by Maggie Dwyer and Thomas Molony. Zed Books.
- Deibert, Ron, John Palfrey, Rafal Rohozinski, and Jonathan Zittrain, eds. 2010. *Access Controlled*. The MIT Press.
- Dukalskis, Alexander. 2021. *Making the World Safe for Dictatorship*. Oxford University Press.
- Dukalskis, Alexander, Saipira Furstenberg, Yana Gorokhovskaia, John Heathershaw, Edward Lemon, and Nate Schenkan. 2022. "Transnational Repression: Data Advances, Comparisons, and Challenges." *Political Research Exchange* 4 (1): 2104651. <https://doi.org/10.1080/2474736X.2022.2104651>.
- EEAS. 2021. *Stratcom Activity Report*. Strategic Communication Task Forces and Information Analysis Division, European External Action Service (EEAS).
- EEAS. 2023. *1st EEAS Report on Foreign Information Manipulation and Interference Threats. Towards a Framework for Networked Defence*. EU External Action Service. <https://www.eeas.europa.eu/sites/default/files/documents/2023/EEAS-DataTeam-ThreatReport-2023..pdf>.
- EEAS. 2024. *2nd EEAS Report on Foreign Manipulation and Interference Threats. A Framework for Networked Defence*. EU External Action Service. https://www.eeas.europa.eu/sites/default/files/documents/2024/EEAS-2nd-Report%20on%20FIMI%20Threats-January-2024_0.pdf.
- EEAS. 2025. *3rd EEAS Report on Foreign Information Manipulation and Interference Threats Exposing the Architecture of FIMI Operations*. <https://www.coe-civ.eu/kh/3rd-eeas-report-on-foreign-information-manipulation-and-interference-threats-exposing-the-architecture-of-fimi-operations>.
- EEAS. 2026. *EEAS 4th EEAS Report on Foreign Information Manipulation and Interference Dismantling the FIMI House of Cards*.
- Elsawah, Mona, and Philip N. Howard. 2020. "'Anything That Causes Chaos': The Organizational Behavior of Russia Today (RT)." *Journal of Communication* 70 (5): 623–45. <https://doi.org/10.1093/joc/jqaa027>.
- Falisse, Jean-Benoît, and Hugues Nkengurutse. 2019. "From FM Radio Stations to Internet 2.0 Overnight. Information, Participation and Social Media in Post-Failed Coup Burundi." In *Social Media and Politics in Africa: Democracy, Censorship and Security*, edited by Maggie Dwyer and Thomas Molony. Zed Books.
- Geddes, Barbara, and John Zaller. 1989. "Sources of Popular Support for Authoritarian Regimes." *American Journal of Political Science* 33 (2): 319. <https://doi.org/10.2307/2111150>.
- Glasius, Marlies. 2018. "What Authoritarianism Is ... and Is Not: A Practice Perspective." *International Affairs* 94 (3): 515–33. <https://doi.org/10.1093/ia/iyy060>.

- Gohdes, Anita R. 2024. *Repression in the Digital Age: Surveillance, Censorship, and the Dynamics of State Violence*. Disruptive Technology and International Security. Oxford University Press.
- Greitens, Sheena Chestnut. 2016. *Dictators and Their Secret Police. Coercive Institutions and State Violence*. Cambridge University Press.
- Greitens, Sheena Chestnut, and Rory Truex. 2020. "Repressive Experiences among China Scholars: New Evidence from Survey Data." *The China Quarterly* 242: 349–75.
- Guichaoua, André. 2020. "Counting the Rwandan Victims of War and Genocide: Concluding Reflections." *Journal of Genocide Research* 22 (1): 125–41.
<https://doi.org/10.1080/14623528.2019.1703329>.
- Han, Rongbin. 2015. "Manufacturing Consent in Cyberspace: China's 'Fifty-Cent Army.'" *Journal of Current Chinese Affairs* 44 (2): 105–34.
- Hénin, Nicolas. 2023. *FIMI: Towards a European Redefinition of Foreign Intefereence*. EU-DisinfoLab. https://www.disinfo.eu/wp-content/uploads/2023/04/20230412_FIMI-FS-FINAL.pdf.
- Hobbs, William R., and Margaret E. Roberts. 2018. "How Sudden Censorship Can Increase Access to Information." *American Political Science Review* 112 (3): 621–36.
<https://doi.org/http://dx.doi.org.pva.uib.no/10.1017/S0003055418000084>.
- Huang, Haifeng. 2015. "Propaganda as Signaling." *Comparative Politics* 47 (4): 419–37.
- Huang, Haifeng. 2018. "The Pathology of Hard Propaganda." *The Journal of Politics* 80 (3): 1034–38. <https://doi.org/10.1086/696863>.
- Jerven, Morten. 2016. "Research Note: Africa by Numbers: Reviewing the Database Approach to Studying African Economies." *African Affairs* 115 (459): 342–58.
<https://doi.org/10.1093/afraf/adw006>.
- Jessee, Erin. 2012. "Conducting Fieldwork in Rwanda." *Canadian Journal of Development Studies / Revue Canadienne d'études Du Développement* 33 (2): 266–74.
<https://doi.org/10.1080/02255189.2012.687356>.
- Jessee, Erin (Times Higher Education). 2013. "Rwanda's Subtle Forms of Intimidation." December 19. <https://www.timeshighereducation.com/comment/opinion/rwandas-subtle-forms-of-intimidation/2009974.article>.
- Keremoğlu, Eda, and Nils Weidmann. 2020. "How Dictators Control the Internet: A Review Essay." *Comparative Political Studies* 53 (10–11): 1690–703. Sage CA: Los Angeles, CA. <https://doi.org/10.1177/0010414020912278>.
- King, Gary, Jennifer Pan, and Margaret E. Roberts. 2017. "How the Chinese Government Fabricates Social Media Posts for Strategic Distraction, Not Engaged Argument." *American Political Science Review* 111 (3): 484–501.
<https://doi.org/10.1017/S0003055417000144>.
- Lemaire, Pauline. 2024. "Online Censorship and Young People's Use of Social Media to Get News." *International Political Science Review* 45 (4): 521–35.
<https://doi.org/10.1177/01925121231183105>.

- Lutscher, Philipp M. 2023. "When Censorship Works: Exploring the Resilience of News Websites to Online Censorship." *British Journal of Political Science*, January 25, 1–9. <https://doi.org/10.1017/S0007123422000722>.
- Lutscher, Philipp M., and Karsten Donnay. 2024. "A Difficult Test for Hard Propaganda: Evidence from a Choice Experiment in Venezuela." *Journal of Peace Research*, February 19, 00223433231220269. <https://doi.org/10.1177/00223433231220269>.
- Martin, Brian. 1999. "Suppression of Dissent in Science." In *Research in Social Problems and Public Policy*, edited by William R. Freudenburg and Ted I. K. Youn, vol. 7. JAP Press.
- McMillan, John, and Pablo Zoido. 2004. "How to Subvert Democracy: Montesinos in Peru." *Journal of Economic Perspectives* 18 (4): 69–92. <https://doi.org/10.1257/0895330042632690>.
- Meserve, Stephen A., and Daniel Pemstein. 2019. *Terrorism and Internet Censorship*. Working Paper No. 3. Digital Society Project (DSP).
- Michaelsen, Marcus. 2018. "Exit and Voice in a Digital Age: Iran's Exiled Activists and the Authoritarian State." *Globalizations* 15 (2): 248–64. <https://doi.org/10.1080/14747731.2016.1263078>.
- Morgenbesser, Lee, and Meredith L. Weiss. 2018. "Survive and Thrive: Field Research in Authoritarian Southeast Asia." *Asian Studies Review* 42 (3): 385–403. <https://doi.org/10.1080/10357823.2018.1472210>.
- Morozov, Evgeny. 2012. *The Net Delusion: The Dark Side of Internet Freedom*. PublicAffairs.
- Moss, Dana M. 2016. "Transnational Repression, Diaspora Mobilization, and the Case of The Arab Spring." *Social Problems* 63 (4): 480–98. <https://doi.org/10.1093/socpro/spw019>.
- Nye, Joseph S. 1990. "Soft Power." *Foreign Policy*, no. 80: 153. <https://doi.org/10.2307/1148580>.
- Nye, Joseph S. 2019. "Soft Power and Public Diplomacy Revisited." *The Hague Journal of Diplomacy* 14 (1–2): 7–20. <https://doi.org/10.1163/1871191X-14101013>.
- O'Donnell, Guillermo A. 1998. "Horizontal Accountability in New Democracies." *Journal of Democracy* 9 (3): 112–26. <https://doi.org/10.1353/jod.1998.0051>.
- Pan, Jennifer, and Margaret E. Roberts. 2020. "Censorship's Effect on Incidental Exposure to Information: Evidence From Wikipedia." *SAGE Open* 10 (1): 2158244019894068. <https://doi.org/10.1177/2158244019894068>.
- Pearce, Katy E., Deen Freelon, and Sarah Kendzior. 2014. "The Effect of the Internet on Civic Engagement under Authoritarianism: The Case of Azerbaijan." *First Monday* 19 (6). Nationally representative. <https://doi.org/10.5210/fm.v19i6.5000>.
- Reyntjens, Filip. 2015. "The Struggle over Truth – Rwanda and the BBC." *African Affairs* 114 (457): 637–48. <https://doi.org/10.1093/afraf/adv042>.
- Roberts, Margaret E. 2018. *Censored*. Princeton University Press.

- Roberts, Tony, and Marjoke Oosterom. 2024. "Digital Authoritarianism: A Systematic Literature Review." *Information Technology for Development* 0 (0): 1–25. <https://doi.org/10.1080/02681102.2024.2425352>.
- Rosenfeld, Bryn, and Jeremy Wallace. 2024. "Information Politics and Propaganda in Authoritarian Societies." *Annual Review of Political Science* 27 (Volume 27, 2024): 263–81. <https://doi.org/10.1146/annurev-polisci-041322-035951>.
- Sanovich, Sergey, Denis Stukal, and Joshua A. Tucker. 2018. "Turning the Virtual Tables: Government Strategies for Addressing Online Opposition with an Application to Russia." *Comparative Politics* 50 (3): 435–82. <https://doi.org/10.5129/001041518822704890>.
- Schenkkan, Nate. 2025. "The Golden Age of Transnational Repression." *Journal of Democracy* 36 (4): 36–50.
- Schumann, Maurice Phillip. 2025. "Legalizing Control: The Rise of Restrictive Internet Regulation in Sub-Saharan Africa." *Democratization* 0 (0): 1–26. <https://doi.org/10.1080/13510347.2025.2503370>.
- Seo, Soomin. 2018. "Covering the Hermit Regime: A Comparison of North Korea Coverage at the Associated Press and NK News." *Journalism* 19 (9–10): 1363–79. <https://doi.org/10.1177/1464884918776450>.
- Shao, Li, Dongshu Liu, and Fangfei Wang. 2024. "Suppression by Mobilization: How Information Control Strategies Contain Political Criticism in Autocracies." *Political Research Quarterly* 77 (3): 729–42. <https://doi.org/10.1177/10659129241242040>.
- Tesfaye, Amanuel, and Matti Pohjonen. 2025. "AI and Visual Propaganda Are Being Used to Stoke Tensions as Ethiopia Eyes Eritrea's Red Sea Port." *Aaawwwa. Global Voices*, October 9. <https://globalvoices.org/2025/10/09/escaping-the-geographic-prison-ai-and-visual-propaganda-in-ethiopias-red-sea-discourse/>.
- Thomson, Susan. 2009. "'That Is Not What We Authorised You to Do ... ': Access and Government Interference in Highly Politicised Research Environments." In *Surviving Field Research: Working in Violent and Difficult Situations*, edited by Chandra Lekha Sriram. Routledge.
- Thomson, Susan. 2011. "Reeducation for Reconciliation: Participant Observations on Ingando." In *Remaking Rwanda: State Building and Human Rights after Mass Violence*, edited by Scott Straus and Lars Waldorf. Critical Human Rights. The University of Wisconsin Press.
- Vériter, Sophie L (2025) 'The collective securitization of 'disinformation' and the EU's ban on *Russia Today* and *Sputnik*', in *International Affairs*, 101: 5, pp.1853–1876, <https://doi.org/10.1093/ia/iiaf139>
- Wack, Morgan, Darren Linvill, and Patrick Warren. 2024. *Old Despots, New Tricks - An AI-Empowered Pro-Kagame/RPF Coordinated Influence Network on X*. No. 5. Media Forensics Hub Reports. https://open.clemson.edu/mfh_reports/5/.
- Walker, Christopher. 2018. "What Is 'Sharp Power'?" *Journal of Democracy* 29 (3): 9–23. <https://doi.org/10.1353/jod.2018.0041>.

Wallace, Jeremy L. 2016. "Juking the Stats? Authoritarian Information Problems in China." *British Journal of Political Science* 46 (1): 11–29.
<https://doi.org/10.1017/S0007123414000106>.

Wanless, A., and J. Pamment. 2019. "How Do You Define a Problem Like Influence?" *Journal of Information Warfare* 18 (3): 1–14.

Wardle, Claire, and Hossein Derakhshan. 2017. *Information Disorder : Toward an Interdisciplinary Framework for Research and Policy Making*. DGI(2017)09. Council of Europe.