COMMITTEE OF MINISTERS
COMITÉ DES MINISTRES

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

MINISTERS' DEPUTIES | Information documents | CM/Inf(2026)18 | 10 April 2026

135th Session of the Committee of Ministers **(Chișinău,** 14-15 May 2026)

Feasibility study on the possible elaboration of a legal instrument on foreign information manipulation and interference (FIMI), including disinformation

TABLE OF CONTENTS

EXECUTIVE SUMMARY

1. In line with the Terms of Reference of the Committee of Experts on Foreign Information Manipulation and Interference (PC-FIMI), this study aims to examine the feasibility of the elaboration of a Council of Europe legal instrument on foreign information manipulation and interference (FIMI), including disinformation.

2. The PC-FIMI recognises that FIMI constitutes a serious threat to democratic and national security, human rights and the rule of law, both in Europe and beyond. FIMI operations are designed to distort democratic debate, erode public trust in institutions and the media, and undermine the integrity of electoral and political processes. Addressing this phenomenon requires responses that are both effective and fully consistent with the European Convention on Human Rights and other Council of Europe standards.

3. The study is divided into eight chapters. After a brief introduction (Chapter 1), Chapter 2 examines the conceptual aspects of FIMI, including its defining characteristics and what sets it apart from other terms. Chapter 3 provides an overview of the existing international initiatives relevant for addressing FIMI, in particular those of the Council of Europe, the United Nations, the European Union, NATO, the OSCE and the OECD.

4. Chapter 4 delves into the various categories of responses to FIMI that are being applied by member States. These include resilience-building measures (such as media freedom, pluralism, and media and information literacy), governance and regulatory responses, detection and analytical capacities, accountability and enforcement mechanisms, network disruption, as well as national and international co-operation frameworks. The analysis underlines that no single category of response is sufficient in isolation, and that addressing FIMI effectively requires a holistic, whole-of-society and whole-of-government approach.

5. Chapter 5 examines how FIMI-related conduct may be criminalised as well as the risks such criminalisation may pose to human rights. It emphasises that criminal law must remain a measure of last resort, subject to strict requirements of legality, necessity and proportionality. The Chapter points out that overly broad or vague criminalisation risks undermining freedom of expression and democratic participation.

6. Whereas Chapters 2 – 5 are mainly descriptive in character, Chapter 6 contains an analysis of challenges and gaps in the experiences of member States in building resilience to, countering, and disrupting, FIMI operations. These challenges include differences in the conceptualisation of FIMI, uneven institutional capacities, fragmented policy approaches, challenges in detection and attribution, limited international co-operation, and emerging risks linked to - in particular - artificial intelligence and alternative financing mechanisms.

7. Building on the analysis contained in Chapter 6, Chapter 7 examines the feasibility of elaborating a Council of Europe legal instrument to address the identified gaps and challenges. Chapter 8 contains the conclusions which the PC-FIMI have reached regarding the feasibility of elaborating a Council of Europe legal instrument on FIMI.

8. The Committee of Experts finds that FIMI poses a direct risk to democratic institutions and processes, national security, human rights and the rule of law in Europe and globally. It also finds that there is added value in member States adopting a co-ordinated approach to countering FIMI and working together to prevent, build resilience against, detect and disrupt FIMI operations, as well as to ensure accountability, based on a shared set of principles grounded in human rights, democracy and the rule of law.

9. Furthermore, there is common ground between member States for further strengthening co-operation in areas such as digital governance, institutional resilience and addressing the challenges related to online service providers, artificial intelligence and other emerging digital technologies in the context of countering and disrupting FIMI.

10. The PC-FIMI notes that, at present, member States do not conceptualise the term FIMI in a uniform manner, and that further efforts aimed at clarifying and bringing together the various concepts of FIMI are needed. These differences partly reflect varying national experiences with, and levels of exposure to, FIMI operations.

11. Member States have differing positions on the feasibility of criminalising certain FIMI-related conduct. The PC-FIMI notes that this issue requires further careful consideration, if the Committee of Ministers decides to go ahead with the elaboration of a Council of Europe legal instrument on FIMI, in particular in light of the need to safeguard freedom of expression and other human rights.

12. The PC-FIMI observes that many issues relating to media are already the subject of substantive standards at the level of the Council of Europe. Any future legal instrument should therefore focus on specific related responses and build upon the existing acquis of the Council of Europe.

13. The feasibility study reflects the work of the Committee at the current stage and within the time available. The Committee agreed on the feasibility of a Council of Europe legal instrument addressing FIMI, with a particular focus on supporting resilience building, sharing of best practice and facilitating international co-operation and an emphasis on a shared set of principles grounded in human rights, democracy and the rule of law. However, the study should not be considered exhaustive or definitive as to the scope of issues that may need to be addressed. Further work would be required for a possible Council of Europe legal instrument, particularly in light of the rapidly evolving nature of FIMI-related challenges, which continue to pose a threat to democracy.

14. The PC-FIMI cannot pronounce itself on the type of legal instrument (recommendation or convention/framework convention) that would be most suitable for addressing FIMI, but notes that the range and characteristics of the measures that can be taken will vary depending on the type of legal instrument chosen. However, the PC-FIMI has drawn up a non-exhaustive list of elements that could be considered for inclusion in such an instrument.

CHAPTER 1 – INTRODUCTION

15. By decision of the Committee of Ministers of 18 November 2025, the Committee of Experts on Foreign Information Manipulation and Interference (PC-FIMI) was established under the European Committee on Crime Problems (CDPC). The Committee of Experts was composed of the following twelve members elected by the CDPC: Belgium, Estonia, Finland, France, Latvia, Malta, Republic of Moldova, Netherlands, Poland, Spain, Switzerland, and the United Kingdom, and chaired by Heini HUOTARINEN (Finland). The Vice-Chair was Agnieszka LEGUCKA (Poland). Moreover, the following member States, observers and participants attended the meetings of the PC-FIMI: Azerbaijan, Belgium, Czechia, Estonia, Finland, France, Georgia, Hungary, Latvia, Malta, Republic of Moldova, Monaco, Montenegro, Netherlands, Poland, Serbia, Spain, Switzerland, Türkiye, Ukraine, Japan, European Union (EU), Organization for Security and Co-operation in Europe (OSCE), Parliamentary Assembly (PACE), Congress of Local and Regional Authorities, Office of the Commissioner for Human Rights, Steering Committee for Human Rights (CDDH), Steering Committee on Media and Information Society (CDMSI), Steering Committee for New and Emerging Digital Technologies (CDNET), Cybercrime Convention Committee (T-CY), and Netherlands Helsinki Committee. The PC-FIMI held a total of four meetings from 27 January until 13 March 2026 with the task of preparing this feasibility study.

16. The elaboration of the feasibility study is part of the activities under the Council of Europe's New Democratic Pact for Europe[1]. This Pact aims to provide a collective response to the democratic backsliding, disinformation, impunity, and authoritarianism which is currently threatening democratic security[2] in Europe and beyond. The work of the PC-FIMI seeks to contribute to shaping a coherent and practicable response to FIMI in line with the Organisation's mandate.

---

[1] Council of Europe, New Democratic Pact for Europe (2024), political framework emphasising democratic security and the need for coherent, rights-based responses to democratic backsliding, including disinformation and other forms of interference affecting democratic governance.

[2] "Democratic security" is a concept formally articulated at the Council of Europe's first Summit of Heads of State and Government (Vienna, 1993). It reflects the understanding that Europe's long-term stability depends fundamentally on effective democracy, human rights and the rule of law, and forms part of the Organisation's core mandate, as reaffirmed in the framework of the New Democratic Pact for Europe.

17. This work is also in line with the Reykjavík Declaration[3] adopted at the 4th Summit of Heads of State and Government of the Council of Europe, which reaffirmed the Organisation's resolve to strengthen democratic security, uphold human rights and address emerging threats to democratic institutions[4].

18. Addressing the Parliamentary Assembly of the Council of Europe on 27 January 2026[5], the President of the Republic of Moldova and current president of the Committee of Ministers, Maia Sandu, underlined that European democracies are facing not only armed aggression, but also "a less visible hybrid war involving disinformation, cyberattacks and external interference". She emphasised that this form of confrontation erodes trust and seeks to undermine democratic institutions from within[6].

19. The Secretary General of the Council of Europe, Alain Berset, has similarly underlined the need to "draw clear boundaries between freedom of expression and imperative for truth, between legitimate critique and destabilisation" and called for Europe to "make democratic security its first line of defence"[7].

20. Foreign information manipulation and interference (FIMI)[8] undermines democratic debate and decision-making. FIMI operations are currently launched in Europe and worldwide to weaken trust in public institutions, undermine national security, affect electoral integrity, and erode public confidence in democratic processes[9].

21. These activities are often deployed alongside other hybrid threats. They may involve informational, political, economic, technological and cyber means. They are designed to remain below the threshold of armed conflict[10].

22. Apart from the manipulation of information, hybrid threats may also be expressed through interference with essential systems and facilities linked to the public safety, security, and economic stability of a State. These activities may include acts of sabotage, cyberattacks, signal jamming, unauthorised drone incursions and similar unlawful acts, sometimes carried out through individuals recruited or instrumentalised for this purpose, and aimed at testing, disrupting, or undermining the resilience of democratic societies.

23. Though FIMI and the accompanying hybrid threats are not *per se* new phenomena, digital technological advances have introduced a new dynamic. Online service providers, including social media, enable rapid and large-scale dissemination of manipulated content in ways which were not previously possible. Artificial intelligence (AI) further increases the speed, reach and sophistication of such activities.

24. These developments demonstrate that FIMI is not a marginal or short-term phenomenon, but a structural challenge to democratic and national security that requires careful legal, policy and institutional responses, grounded in respect for human rights, democracy and the rule of law.

---

[3] Reykjavík Declaration – United around our values, 4th Summit of Heads of State and Government of the Council of Europe, Reykjavík, 16-17 May 2023.

[4] "Democratic institutions" are understood as the constitutional and public authorities that ensure the functioning of democratic governance in accordance with the principles of democracy, human rights and the rule of law, including elected bodies, independent oversight institutions and judicial authorities, as reflected in the Statute of the Council of Europe (ETS No. 1) and reaffirmed in the Reykjavík Declaration (2023).

[5] The Republic of Moldova holds the Presidency of the Council of Europe (Committee of Ministers) from November 2025 until May 2026.

[6] Address by the President of the Republic of Moldova, Maia Sandu, to the Parliamentary Assembly of the Council of Europe, 27 January 2026, available at: https://pace.coe.int/en/news/10166/maia-sandu-two-wars-are-being-waged-against-european-democracy

[7] Article in Euronews by Secretary General Alain Berset on 22 May 2025, available at: https://www.euronews.com/my-europe/2025/05/22/democracy-is-europes-first-line-of-defence

[8] The understanding of FIMI used in this study is explained in Chapter 2.

[9] For the purposes of this study, "democratic processes" refer to the procedures and conditions through which the will of the people is formed and expressed, including electoral processes and political participation, as protected under Article 3 of Protocol No. 1 to the Convention. This notion also encompasses the conditions for free and pluralistic public debate, including the role of the media as a public watchdog under Article 10 of the Convention, as consistently recognised in the case-law of the European Court of Human Rights.

[10] NATO, Vilnius Summit Communiqué (2023), political declaration addressing hybrid threats and activities conducted below the threshold of armed conflict, including political interference, disinformation and malicious cyber activities (see in particular paras. 6, 18 and 64).

25. FIMI is particularly damaging where societies are already marked by inequality and discrimination. It deliberately exploits existing social fractures and polarisation, amplifying tensions and reinforcing narratives of division to further weaken social cohesion and democratic trust[11].

26. Certain groups are disproportionately harmed by FIMI. Women, LGBTI persons, Roma and Travellers, migrants and other minorities are frequently singled out, including through the instrumentalisation of migration and identity-based narratives, or distortions relating to gender equality norms[12]. In some instances, these narratives are designed to undermine the protection of the rights of specific groups, thereby challenging established human rights standards and democratic safeguards.

27. FIMI may also undermine free and pluralistic media, which are essential to democratic debate under Article 10 of the European Convention on Human Rights (the Convention).

28. Political events, such as electoral processes, referenda or major public debates, may constitute periods of heightened vulnerability to FIMI. During such periods, manipulation campaigns may have amplified impact on public trust, institutional stability and the free formation of political will.

29. In some cases, such operations may also adversely affect children and young people at early stages of individual and group formation. They may also deter marginalised groups or individuals from political participation. Such practices undermine human rights, equality and the ability of individuals to participate effectively in democratic life.

30. It is accordingly important to emphasise that, by their nature, FIMI operations do not constitute a legitimate exercise of human rights deserving of protection under international or domestic law. Because these operations are conducted under the cover of human rights, such as freedom of expression or peaceful assembly, a false dichotomy often occurs in public debate. This dichotomy opposes the protection of these rights to action against the serious, corrosive effects of FIMI operations. This false dichotomy not only risks weakening the resolve of democratic States to counteract FIMI operations but may de facto create the conditions for such operations to be carried out with virtual impunity in the name of the very freedoms they seek to undermine.

31. Democratic security and the protection of human rights are closely interconnected. Measures that fail to safeguard human rights risk undermining democratic legitimacy, while insufficient protection against foreign interference can weaken democratic institutions and public trust.

32. States have negative obligations to avoid undue interference with the exercise and enjoyment of the human rights and fundamental freedoms guaranteed by the Convention. In accordance with the Court's jurisprudence, they also have positive obligations to take the necessary measures to safeguard those rights and freedoms. Such obligations may arise when those rights and freedoms are threatened in the context of foreign interference. Article 17 of the Convention clarifies that human rights cannot be invoked to justify activities aimed at undermining those very rights[13]. Addressing FIMI therefore raises a fundamental challenge for democratic societies. Responses must be effective in protecting democratic systems against evolving forms of foreign interference, while fully preserving human rights.

[11] Council of Europe, Resisting disinformation: 10 building blocks to strengthen information integrity (CDMSI, 2025), policy document adopted by the Steering Committee on Media and Information Society, addressing the role of social inequalities, discrimination and polarisation in weakening social cohesion and democratic trust (see in particular pp. 6, 10 and 36).
[12] Council of Europe, Recommendation CM/Rec(2022)16 of the Committee of Ministers to member States on combating hate speech (2022), addressing the disproportionate targeting of women, LGBTI persons, Roma and Travellers, migrants and other minorities, including through identity-based and migration-related narratives (see in particular pp. 5–6, 16 and 18).
[13] Article 17 of the European Convention on Human Rights states: "Nothing in this Convention may be interpreted as implying for any State, group or person any right to engage in any activity or perform any act aimed at the destruction of any of the rights and freedoms set forth herein or at their limitation to a greater extent than is provided for in the Convention

33. In line with these considerations and the mandate given by the Committee of Ministers, the aim of this feasibility study is to assess the feasibility of elaborating a Council of Europe legal instrument on FIMI. The study does not seek to establish uniform positions across all thematic areas and, where relevant, reflects differing national approaches. Taking into account the various facets of the threat that FIMI poses to democratic and national security, it proposes legal and other measures to strengthen resilience against FIMI while protecting and respecting human rights, democracy and the rule of law.

CHAPTER 2 – UNDERSTANDING FIMI AND RELATED CONCEPTS

34. This chapter describes and frames the phenomenon of FIMI. It establishes the parameters for the discussions that follow. The explanations provided do not constitute legal definitions.

A. The concept of FIMI

35. Policy discussion and public debates on FIMI are marked by significant terminological confusion. Concepts such as “disinformation”, “information manipulation”, “foreign interference” are frequently used loosely, inconsistently, or as if they were interchangeable. These terms in fact refer to distinct but related dimensions of the same phenomenon, reflecting variations in actors, methods and objectives.

36. For this reason, a feasibility study should clarify how foreign information manipulation and interference, disinformation, and wider foreign interference relate to one another as a necessary step before examining the range of possible responses, including preventive, regulatory, or criminal-law options. This clarification will help avoid conflating legitimate and transparent forms of foreign influence with conduct that is co-ordinated, deceptive or covert.

37. In recent years, the European Union (EU) has developed a specific understanding of FIMI in response to the growing scale and sophistication of such activities. According to the European External Action Service, *“foreign information manipulation and interference (FIMI) refers to mostly non-illegal patterns of behaviour that threaten or have the potential to negatively impact democratic values and processes. Such activity is manipulative, intentional and co-ordinated, relies on deceptive practices, and is conducted by State or non-State actors and their proxies*[14]*.”*

38. A defining feature of FIMI is the direct or indirect involvement of a foreign State, whether State or non-State, including private entities and their proxies**.** This external dimension distinguishes FIMI from purely domestic forms of information manipulation and interference, even when similar techniques or narratives are used.

39. The EU approach situates FIMI within a broader set of activities that operate below the threshold of armed conflict. Information manipulation may interact with diplomatic, economic, cyber, technological or criminal means and form part of wider hybrid strategies. At the same time, the EU distinguishes FIMI from military operations governed by international humanitarian law[15].

40. For the purposes of this feasibility study, the EU understanding of FIMI serves as a starting point for analysis. Activities falling within the notion of FIMI involve the manipulation of the information environment in a covert, co-ordinated or deceptive manner. This information dimension may be combined with other forms of hybrid interference, such as diplomatic, economic, cyber or technological means. At the same time, the above framing analytical framework does not predetermine legal qualification or responses, nor does it imply that any conduct falling within the notion of FIMI is unlawful or requires coercive or punitive measures solely because it deliberately distorts the conditions of democratic debate, rather than contributing to it[16].

---

[14] European Union, European External Action Service, 3rd EEAS Report on Foreign Information Manipulation and Interference (FIMI) Threats, March 2025, p. 4 (Glossary).
[15] European Union, European External Action Service, 3rd EEAS Report on Foreign Information Manipulation and Interference (FIMI) Threats, March 2025, pp. 7–8.
[16] European Union, European External Action Service, 1st Report on Foreign Information Manipulation and Interference (FIMI) Threats, February 2023, p. 26, outlining a behaviour-centred analytical approach and indicators used to distinguish co-ordinated and covert manipulation from lawful expression.

41. The fact that certain expressions may echo narratives associated with FIMI operations does not automatically remove them from protection under the Convention[17].

B. Foreign interference

42. Foreign interference may take multiple forms, including political, economic, cyber and informational activities, or acts of sabotage. It is therefore not limited to the information domain and may involve a combination of tools and channels[18].

43. In legal terms, however, foreign interference does not constitute a formally defined legal category under international law[19]. It should be distinguished from the concept of unlawful intervention as developed in international law. The term is used in policy and analytical discourse in light of principles relating to State sovereignty and non-intervention[20]. While not all forms of foreign interference reach the threshold of unlawful intervention, certain activities may, depending on their nature and effects, amount to a violation of the principle of non-intervention.

44. In contemporary policy discourse, it commonly refers to non-transparent or deceptive actions by foreign actors that seek to influence or disrupt the internal political or democratic processes of another State, including electoral processes and broader public debate[21].

45. The involvement of foreign State or non-State actors, including their proxies acting on their behalf, may be direct or indirect. It may need to be assessed on the basis of patterns of behaviour and converging indicators[22]. These links may be concealed, mediated through intermediaries, or otherwise deliberately obscured[23].

46. The qualification of a domestic actor as acting "on behalf of" or as a "proxy" of a foreign power should be based on clear and strictly defined legal criteria.

47. These activities are aimed at disrupting or manipulating internal political, democratic or societal processes, and the functioning of free and independent media. The objective is not merely to shape opinions, but to affect the functioning, legitimacy or stability of democratic systems, including public trust in democratic institutions and media[24].

48. Foreign interference must also be clearly distinguished from legitimate and transparent foreign influence. Diplomatic engagement, public communication, lobbying or cultural exchange fall outside this concept when conducted openly and lawfully. International co-operation and the activities of civil society organisations likewise fall outside this concept when transparent and lawful. The threshold of interference is crossed where conduct becomes manipulative, deceptive, coercive or covert. This includes situations where actions are intended to improperly influence or corrupt decision-making processes, or to undermine the functioning, legitimacy or stability of democratic systems. For reasons of maintaining deniability, foreign

---

[17] European Court of Human Rights, *Handyside v. the United Kingdom*, no. 5493/72, judgment of 7 December 1976, para. 49, holding that freedom of expression protects not only information or ideas that are favourably received but also those that offend, shock or disturb. The Court also found (paras. 48-52) that contracting parties enjoy a margin of appreciation in assessing the scope of domestic restrictions, in order to protect societal interests, although later jurisprudence has narrowed State discretion when restrictions are overly broad or vague. See also *Delfi AS v. Estonia*, no.64569/09, judgment of 16 June 2016, and *Magyar Tartalomszolgáltatók Egyesülete And Index.Hu Zrt v. Hungary*, no. 22947/13, judgment of 2 May 2016.

[18] NATO, Strategic Concept 2022; Vilnius Summit Communiqué (2023), Hybrid Threats section.

[19] The prohibition of intervention is grounded in the Charter of the United Nations, notably Articles 2(1) and 2(4), which enshrine the principles of State sovereignty and non-intervention.

[20] United Nations General Assembly, Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations, Resolution 2625 (XXV), 1970, elaborating the principle of non-intervention, including indirect forms of coercive interference.

[21] United Nations, Charter of the United Nations, Articles 2(1) and 2(4), enshrining the principles of State sovereignty and non-intervention and United Nations General Assembly, Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations, Resolution 2625 (XXV), 1970, elaborating the principle of non-intervention, including indirect forms of interference.

[22] EEAS, 2nd Report on Foreign Information Manipulation and Interference Threats (2024), "Key Characteristics of FIMI"; 3rd FIMI Threat Report (2025).

[23] Parliamentary Assembly of the Council of Europe, Resolution 2326 (2020) "Democracy hacked? How to respond?", paras. 1-2, describing foreign interference and disinformation as co-ordinated and intentional campaigns aimed at misleading the public and undermining democratic processes.

[24] VIGINUM, Portal Kombat (February 2024), "Architecture of the Network", pp. 3-6; StratCom Moldova, Hybrid Threats Summary 2021–2024.

involvement and strategic objectives are often concealed, mediated through proxies, or otherwise deliberately obscured. The presence of foreign involvement may need to be assessed on the basis of patterns of behaviour and converging indicators.

49. These activities pursue a strategic objective, such as disruption or destabilisation, and are usually characterised by co-ordinated behaviour rather than isolated or spontaneous acts, and they rely on manipulative practices designed to shape the conditions under which information is received and acted upon, rather than individual opinions or beliefs.

C. Information manipulation

50. Information manipulation refers to a mode of action within the information domain. It covers intentional practices aimed at distorting or disrupting the way information is produced, disseminated or perceived. It does not describe a category of content. The focus is not on individual pieces of content taken in isolation, but on how the information space as a whole is shaped and steered.

51. While practices aimed at influencing information environments are not new in democratic societies, contemporary digital technologies have significantly increased their scale, speed and capacity for co-ordination, automation and targeted dissemination[25].

52. In this sense, information manipulation primarily concerns co-ordinated methods and techniques, the strategic use of narratives, and the alteration of the broader information environment. Its defining characteristics often include a strategic and co-ordinated approach, frequently operating across borders, and a reliance on manipulative practices such as concealment of origin, co-ordinated amplification and strategic repetition, rather than factual accuracy alone.

53. These practices may affect not only the content of communication but also its production, amplification, visibility and reception[26]. These practices may include, *inter alia*, deceptive or misleading content, the use of inauthentic or covert accounts and networks[27], co-ordinated amplification techniques, the concealment of origin or sponsorship, and the strategic use of algorithmic systems to influence information flows or to target specific audiences[28].

54. Importantly, information manipulation may rely on false, misleading, or even true information, depending on the objective pursued. What matters is not the truth value of the information as such, but the intentional and strategic manner in which it is deployed to shape how information circulates and is perceived within the information environment.

55. Information manipulation is also not inherently linked to foreign involvement. It may also occur in purely domestic contexts, without any participation by foreign State or non-State actors. For this reason, it should not automatically be equated with foreign information manipulation and interference. Furthermore, the fact that a message is co-ordinated or persuasive does not, in itself, render it manipulative.

56. Finally, information manipulation is a functional and descriptive concept. It serves to describe practices and patterns of behaviour, but it is not a legal category in itself and does not automatically imply illegality. It may involve lawful expression and should be assessed with care to avoid undue restrictions on freedom of expression.

[25] Council of Europe, Declaration on the manipulative capabilities of algorithmic processes (13 February 2019), paras. 6–9.
[26] European External Action Service, EEAS Reports on Foreign Information Manipulation and Interference (2023–2025).
[27] Certain policy and operational frameworks use the expression “co-ordinated inauthentic behaviour” to describe organised deceptive practices involving false identities or artificial amplification. The term captures one subset of manipulative techniques and does not exhaust the broader range of co-ordinated practices referred to in this study. Regulation (EU) 2022/2065 (Digital Services Act), recital 84 and EEAS FIMI Reports.
[28] Council of Europe, CDMSI(2025)17 – Resisting Disinformation: 10 Building Blocks; Regulation (EU) 2024/1689 (Artificial Intelligence Act), recitals on manipulative techniques and exploitation of vulnerabilities.

D. Disinformation

57. In public and policy discourse, disinformation is often used in a generic and imprecise way. It commonly serves as a catch-all term for false or misleading information, without clear conceptual limits. This broad usage contributes to confusion and weakens analytical and legal precision.

58. Within Council of Europe standards, the notions of misinformation, disinformation and malinformation are clearly distinguished:

- Misinformation refers to false or misleading information shared without intent to cause harm[29].
- Disinformation refers to verifiably false, inaccurate or misleading information deliberately created and disseminated to cause harm or pursue economic or political gain by deceiving the public[30].
- Malinformation refers to genuine information shared to cause harm, often by moving information designed to remain private into the public sphere[31].

59. This distinction is essential to ensure that lawful expression, journalism and political speech, error, satire or opinion are not improperly restricted.

60. This deceptive intent is pursued for a specific purpose namely, to cause harm or to obtain economic or other gain. The harm may affect individuals, groups, institutions, or democratic processes more broadly.

61. For legal and normative purposes, disinformation can therefore be analysed through two complementary dimensions. Objective elements relate to the falsity of the information and its potential to cause harm. Subjective elements concern the knowledge and intent of the actor involved in its creation or dissemination.

62. In the analytical framework of this study, disinformation is best understood as a specific tool within foreign information manipulation. While defined by falsity and intent, it does not encompass the full range of manipulative practices, many of which may rely on truthful content or operate through indirect means.

E. Some examples of FIMI-related conduct

63. The purpose of the following examples is illustrative rather than exhaustive. They are drawn from publicly documented cases analysed by EU institutions, national authorities and international mechanisms, as well as independent research bodies[32].They are presented to demonstrate how the analytical framework set out in this chapter may be applied in practice. The examples highlight different configurations of FIMI-related conduct, including cases of foreign information manipulation and interference, hybrid situations combining information and non-information means, and cases that fall outside the scope of FIMI despite producing information effects[33].

[29] Council of Europe, Steering Committee on Media and Information Society (CDMSI), Guidance Note on countering the spread of online mis- and disinformation through fact-checking and platform design solutions in a human rights compliant manner, p. 6, para. 3(a).
[30] Council of Europe, Committee of Ministers, Recommendation CM/Rec(2022)11 on principles for media and communication governance, Appendix, para. 4 ; Recommendation CM/Rec(2022)12 on electoral communication and media coverage of election campaigns, Appendix, para. 7.
[31] Wardle C. and Derakhshan H. (2017), Information Disorder: Toward an interdisciplinary framework for research and policymaking, Strasbourg, Council of Europe, available at https://go.coe.int/lmtTh, p. 5.
[32] Including public analyses by the European External Action Service, the G7 Rapid Response Mechanism, NATO and other international monitoring bodies, as well as national authorities such as the Strategic Communication and Countering Disinformation Centre of the Republic of Moldova and VIGINUM (France).
[33] European External Action Service, How to Detect and Analyse Foreign Information Manipulation and Interference (FIMI): A Practical Guide, 2023, p. 2, clarifying the analytical and illustrative purpose of case examples and the non-legal nature of the FIMI framework.

1. Information manipulation operations

(a) Impersonation of trusted media and institutions

64. The operation commonly referred to as “Doppelgänger[34]” illustrates a paradigmatic case of FIMI. The activity involved the creation of large numbers of websites and social media accounts impersonating trusted media outlets and public institutions in several EU member States. These assets were used in a co-ordinated manner to disseminate misleading and selectively framed narratives concerning elections, public institutions and support for Ukraine. The operation combined a clear foreign nexus, covert and deceptive practices, and systemic manipulation of the information environment[35].

65. Comparable structural features have been identified in other documented FIMI operations, including the use of cloned media portals, synchronised publication chains and shared technical infrastructure designed to simulate independent sources while concealing central co-ordination[36].

(b) Strategic narrative construction

66. Certain documented cases illustrate how FIMI operations may involve the construction and dissemination of strategic narratives designed to delegitimise institutions, undermine accountability processes or reshape perceptions of international events. Such campaigns may combine selective factual distortion, co-ordinated amplification and cross-platform dissemination to influence both domestic and international audiences[37].

67. Such narratives may also draw on historical, cultural, linguistic or religious references to cultivate a sense of shared identity beyond existing State borders. In some cases, these narratives form part of broader influence campaigns in which identity-based themes are strategically promoted to reinforce perceived cultural or political affinities across borders. When amplified through co-ordinated media ecosystems and online networks, such narratives may be used to mobilise identity-based communities, shape perceptions of political or social developments, undermine trust in democratic institutions or legitimise political influence over populations in other States.

68. A documented example concerns the reuse of apparently credible “external” sources to legitimise hostile narratives in the domestic information space. Public reporting in the Republic of Moldova has described cases in which materials produced by foreign-based outlets were amplified locally as “external validation” in order to portray EU-related reforms as censorship or political control[38].

69. Another documented example concerns the laundering of fabricated narratives through third-party media before wider amplification. Investigations have described operations in which staged or manipulated content was first published by external outlets and then relayed across platforms to increase credibility and obscure co-ordination[39].

(c) Exploitation of social and identity-based vulnerabilities

70. Some co-ordinated FIMI campaigns strategically exploit identity-based narratives and socially sensitive issues in order to increase polarisation and societal division. In documented electoral contexts, narratives targeting vulnerable groups have been amplified in a co-ordinated manner, contributing to heightened tensions and erosion of trust[40].

---

[34] The so-called “Doppelgänger” operation, consisting of a co-ordinated network of fake websites impersonating established European media outlets in order to disseminate pro-Kremlin narratives, has been publicly attributed by European authorities to actors linked to the Russian Federation, including entities such as the Social Design Agency, as documented in the European External Action Service, Reports on Foreign Information Manipulation and Interference (FIMI) Threats (2023–2025).
[35] European External Action Service, 3rd Report on Foreign Information Manipulation and Interference (FIMI) Threats, 2025, pp. 25-26, documenting the “Doppelgänger” operation as a co-ordinated foreign information manipulation campaign based on impersonation of media outlets and systemic narrative amplification.
[36] VIGINUM, Portal Kombat: A structured and co-ordinated pro-Russian propaganda network, “Architecture of the Network”, pp. 3-6.
[37] GRC, Manufacturing Impunity: Russian Information Operations in Ukraine, Executive Summary.
[38] Strategic Communication and Countering Disinformation Centre of the Republic of Moldova, public reports on information manipulation and hybrid threat patterns (2021–2026).
[39] European External Action Service, Reports on Foreign Information Manipulation and Interference (FIMI) Threats (2023–2025).
[40] GENDERDOC-M, Report on Disinformation, Hate Speech and Incitement against LGBTI+ People in the Republic of Moldova (2025).

71. Public reporting has documented co-ordinated campaigns targeting socially sensitive issues in order to increase polarisation. In the Republic of Moldova, narratives concerning language policy, minority rights and European integration were amplified during electoral periods. These narratives portrayed reforms as threats to national identity and sovereignty[41].

72. Other cases have involved the exploitation of identity-based tensions in overseas territories. Co-ordinated online narratives framed episodes of social unrest as evidence of systemic repression. Independence-related themes were amplified across platforms in order to weaken institutional legitimacy and deepen divisions[42].

73. International monitoring bodies have also documented operations targeting religious and cultural cleavages in several European States. These campaigns relied on emotionally charged content and selective framing. The objective was to reinforce existing distrust and to fragment public debate[43].

74. Documented cases have also highlighted attempts to mobilise diaspora communities, youth networks, and cultural or educational initiatives as channels for influence aligned with foreign State objectives. Such activities may combine identity-based narratives, community outreach, and cross-border organisational support. While cultural and educational exchanges constitute legitimate and valuable forms of international engagement, their covert instrumentalisation for strategic interference purposes may fall within the scope of FIMI.

2. Hybrid and multi-domain FIMI operations

75. Some documented cases illustrate hybrid operations in which non-informational acts are deliberately used as triggers for subsequent information manipulation. Campaigns targeting elections in Eastern Europe have shown how cyber intrusions, data leaks or acts of intimidation were followed by co-ordinated narrative amplification across online platforms.

76. A concrete and recent example of how online information manipulation is often combined with physical criminal acts concerns damage to a railway track in a member State as result of acts of sabotage. Responsibility was attributed by the national authorities in question to nationals of another member State acting on behalf of foreign intelligence services. The sabotage acts were exploited to disseminate disinformation narratives by the foreign intelligence services. The resulting online campaign generated substantial engagement across platforms[44].

77. Another such example is the violation of the airspace of a member State by foreign drones accompanied by intensified disinformation activity conducted by foreign intelligence services. This activity was characterised by a high volume of co-ordinated online posts and significant audience reach[45].

3. Domestic disinformation without a foreign nexus

78. By contrast, large-scale domestic disinformation campaigns conducted by political actors or commercial entities, even when highly co-ordinated and misleading, do not in themselves constitute FIMI in the absence of a foreign nexus. Several cases documented in EU member States involve the spread of false or manipulative content aimed at influencing public opinion or electoral outcomes, but without any evidence of foreign State involvement. Such cases may raise serious concerns under electoral law, media regulation or criminal law, but they fall outside the scope of FIMI[46].

---

[41] Strategic Communication and Countering Disinformation Centre of the Republic of Moldova, Hybrid Threats Summary 2021-2024; 2026 Report: Information Manipulation and Democratic Resilience.
[42] VIGINUM (France), Un-notorious BIG: A digital information manipulation campaign targeting French overseas departments, regions, territories and Corsica (2024).
[43] European External Action Service, Reports on Foreign Information Manipulation and Interference (FIMI) Threats (2023–2025).
[44] According to information provided by the authorities of the member State concerned during the Committee’s discussions, the sabotage-related campaign generated at least 1.84 million views and an estimated reach of approximately 4.25 million users on the X platform.
[45] According to information provided by the authorities of the member State concerned during the Committee’s discussions, the drone-related case involved 63,953 disinformation posts reaching at least 7.9 million users.
[46] Parliamentary Assembly of the Council of Europe, Resolution 2326 (2020) “Democracy hacked? How to respond?”, paras. 1-2, distinguishing foreign interference from domestic disinformation and underlining that not all disinformation activities are attributable to foreign actors.

79. Similarly, certain commercially motivated “clickbait” networks have generated large volumes of misleading content for advertising revenue. These operations may distort public debate. Yet they do not qualify as FIMI where no foreign nexus is established[47].

CHAPTER 3 – EXISTING INTERNATIONAL INITIATIVES RELEVANT TO ADDRESSING FIMI

80. This chapter examines existing international and regional initiatives relevant to addressing FIMI. It identifies how different organisations and institutional frameworks approach issues related to disinformation, information manipulation and foreign interference. The explanations provided do not assess effectiveness or prejudge the desirability of new legal instruments.

A. Introduction

81. This chapter provides an overview of existing international initiatives relevant to FIMI, building on the conceptual framework set out in Chapter 2. Its purpose is to map how different international and regional institutions address issues related to disinformation, information manipulation and foreign interference, in light of their respective mandates and instruments.

82. FIMI intersects with several policy domains, including human rights, democratic governance, security, digital regulation and international relations. A purely thematic categorisation of initiatives would risk creating overlaps and blurring institutional responsibilities. For this reason, the chapter adopts an institutional approach, examining initiatives organisation by organisation, while applying a common analytical framework across institutions.

83. The initiatives reviewed in this chapter differ significantly in their legal nature and normative effect. Some establish binding legal obligations, while others consist of non-binding standards, policy orientations or analytical and operational frameworks. These instruments are not treated as equivalent. Instead, attention is paid to how their normative character reflects institutional mandates, risk perceptions and the sensitivity of regulating the information environment, particularly in relation to freedom of expression.

84. The limited presence of binding norms specifically addressing FIMI should not be understood solely as a normative gap. In many cases, it reflects a deliberate reliance on a combination of soft law instruments, policy guidance, operational co-ordination mechanisms, regulatory frameworks and analytical tools, aimed at managing risks to democratic systems while preserving freedom of expression and democratic pluralism. On this basis, the chapter clarifies what existing frameworks do and do not cover, without anticipating conclusions on the desirability or form of future legal instruments.

B. Council of Europe: Human Rights, Democracy and Rule of Law

85. Within the international landscape, the Council of Europe addresses issues related to foreign information manipulation and interference through its mandate to protect human rights, democracy and the rule of law[48]. Its standards do not define FIMI as a separate legal category. They establish the legal instruments within which information-related risks, including those involving foreign actors, must be addressed by public authorities.

86. The Council of Europe approach focuses on the effects of disinformation and manipulation on individuals, public debate and democratic institutions. It does not centre on the identification of hostile actors or on the classification of manipulation techniques. Priority is given to safeguarding democratic processes and fundamental freedoms, while preventing responses that could unduly restrict lawful expression or political participation[49].

---

[47] European External Action Service, Reports on Foreign Information Manipulation and Interference (FIMI) Threats (2023–2025), sections addressing economically motivated disinformation networks.
[48] Council of Europe, Statute of the Council of Europe, 1949, Articles 1 and 3, defining the organisation’s mandate in human rights, democracy and the rule of law.
[49] Council of Europe, Committee of Ministers, Declaration on the manipulative capabilities of algorithmic processes (2019), emphasising an effects-based and rights-compliant approach to information-related risks, with particular attention to their impact on individual autonomy, opinion-forming processes and democratic environments (see in particular paras. 3, 7 and 9).

87. This set of conventions, standards and policy instruments forms a coherent rights-based framework. It provides safeguards and guidance across distinct policy areas relevant to democratic resilience. It remains sectoral in scope and does not constitute an integrated framework addressing FIMI as a single phenomenon, as it does not combine, within one instrument, the foreign dimension, manipulation practices and strategic interference.

1. European Convention on Human Rights and case-law

88. The European Convention on Human Rights (the Convention) constitutes the binding legal framework applicable to FIMI-related situations in Council of Europe member States. Depending on the context, several Convention rights may be engaged when information manipulation affects democratic life or when States adopt measures in response to such practices[50].

89. Article 10 of the Convention plays a central role. It protects freedom of expression and the right to receive and impart information, including in political contexts and on matters of public interest. The case-law of the European Court of Human Rights (the Court) subjects any restriction on expression to strict requirements of legality, necessity and proportionality. It further recognises that Article 10 entails positive obligations for States to safeguard the right to receive and impart information. States may also be required to secure an enabling environment for pluralistic and effective freedom of expression. Council of Europe standards further underline the importance of protecting media pluralism and journalistic independence in the digital information environment[51]. These standards are directly relevant where measures targeting disinformation or manipulation risk affecting public debate[52].

90. Other Convention provisions may also be relevant. Article 3 of Protocol No. 1 to the Convention is engaged where information manipulation undermines the integrity of electoral processes or the free formation of the opinion of the electorate. Article 8 of the Convention may apply where manipulation involves intrusive data practices, harassment or targeted attacks on individuals, including where members of specific groups are individually targeted. Articles 11 and 14 of the Convention may be implicated where collective participation, association or equality considerations are affected. The applicability of these rights depends on the nature and impact of the conduct concerned.

91. In addition, Article 17 of the Convention, which prohibits the abuse of rights, may be relevant where activities seek to undermine the foundations of democratic society. The Court has applied Article 17 of the Convention in relation to claims of a violation of Article 10 where the views expressed had involved, for example, threats to territory and the constitutional order[53], promotion and justification of terrorism and war crimes[54], incitement to violence[55], promotion of totalitarian ideologies[56], and incitement to hatred[57].

92. The case-law of the Court provides general guidance on the Convention safeguards applicable to measures addressing election interference, media freedom, and related risks to democratic processes. The Court's jurisprudence under Articles 10 and 11 of the Convention, as well as Article 8 of the Convention and Article 3 of Protocol No. 1 to the Convention, is particularly relevant. When measures to tackle FIMI consist of legal provisions on conduct which give rise to criminal liability, the Court's jurisprudence on Articles 5

[50] Council of Europe, Convention for the Protection of Human Rights and Fundamental Freedoms (1950, ETS No. 5).
[51] Committee of Ministers, Recommendation CM/Rec(2022)4 on promoting a favourable environment for quality journalism in the digital age (adopted on 17 March 2022).
[52] European Court of Human Rights, *Handyside v. the United Kingdom*, judgment of 7 December 1976, para. 49, setting out the fundamental principles governing freedom of expression in a democratic society, including the requirements of legality, necessity and proportionality.
[53] European Court of Human Rights, *Romanov v. Ukraine*, no. 63782/11, judgment of 16 July 2020.
[54] European Court of Human Rights, *Roj TV A/S v. Denmark*, no. 24683/14, decision of 17 April 2018.
[55] European Court of Human Rights, *Hizb ut-Tahrir and Others v. Germany*, no. 31098/08, decision of 12 June 2012; *Belkacem v. Belgium*, no. 34367/14, decision of 27 June 2017; *Romanov v. Ukraine*, no. 63782/11, judgment of 16 July 2020; *Lenis v. Greece*, no. 47833/20, decision of 27 June 2023.
[56] European Commission on Human Rights, *German Communist Party (KPD) v. Germany*, Commission decision, no. 250/57, 20 July 1957; European Court of Human Rights, *Ayoub and Others v. France*, nos. 77400/14 and 2 others, judgment of 8 October 2020; *Kasymakhunov and Saybatalov v. Russia*, nos. 26261/05 and 26377/06, judgment of 14 March 2013.
[57] European Commission on Human Rights, *Glimmerveen and Hagenbeek v. the Netherlands*, decision, 1979; European Court of Human Rights, *Ayoub and Others v. France*, cited above; *Vona v. Hungary*, no. 35943/10, judgment of 9 July 2013; *Pavel Ivanov v. Russia*, no. 35222/04, decision of 20 February 2007; *Association of Citizens "Radko" and Paunkovski v. the former Yugoslav Republic of Macedonia*, no. 74651/01, judgment of 15 January 2009; *Garaudy v. France*, no. 65831/01, decision of 24 June 2003.

and 7 of the Convention may also be relevant. The case-law on any matters on recent FIMI operations is still sparse. The following is a snapshot of cases that however are of relevance in the present context.

93. In *Bradshaw and Others v. the United Kingdom*[58] (2025), concerning alleged foreign interference in democratic processes, the Court examined the complaint under Article 3 of Protocol No. 1 to the Convention (right to free elections). It reiterated that this provision requires States to organise elections “under conditions which will ensure the free expression of the opinion of the people in the choice of the legislature”. The Court accepted that, where there is a real risk that interference by a hostile State could impair the very essence of electors’ rights and deprive them of their effectiveness, Article 3 of Protocol No. 1 may require the adoption of positive measures to protect the integrity of the electoral process. It further recognised that States must not remain passive in the face of sufficiently established threats and that the legal and institutional framework, taken as a whole, must be capable of safeguarding electoral integrity. At the same time, States enjoy a wide margin of appreciation in the choice of means adopted to address such risks. Finding no violation, the Court held that the respondent State’s response fell within that margin and did not disclose a manifest failure to secure the free expression of the people’s will.

94. The Court has consistently held that while member States enjoy a wide margin of appreciation in imposing conditions on the right to vote and to stand for election, they should not curtail the rights in question to such an extent as to impair their very essence and deprive them of their effectiveness. In *Political Party “Patria” and Others v. the Republic of Moldova* (2020)[59], the Court held that the disqualification of a party from elections which used campaign funds from abroad and/or undeclared funds in considerable amounts constituted an interference both with the rights of the party and of the individual applicants under Article 3 of Protocol No. 1 to the Convention. The applicant party’s disqualification from participating in the elections was not based on sufficient and relevant evidence, the procedures of the electoral commission and the domestic courts did not afford the applicant party sufficient guarantees against arbitrariness, and the domestic authorities’ decisions lacked reasoning and were thus arbitrary.

95. Other cases illustrate the Court’s approach to restrictions of freedom of expression in the context of electoral and political debate as well as restrictions of freedom of association. In *Salov v. Ukraine*[60] (2005), concerning the criminal conviction of an individual for disseminating false information during a presidential election campaign, the Court found a violation of Article 10 of the Convention. While accepting that protecting voters from misinformation constituted a legitimate aim, it stressed that criminal sanctions in the context of electoral discourse call for particularly careful scrutiny and must respond to a “pressing social need” and remain proportionate. In *Kita v. Poland*[61] (2008), which concerned the fining of a Polish citizen by a national court in a civil procedure for publicly spreading allegedly false statements during an election campaign, the Court accepted that protection of the reputation or rights of others constitutes a legitimate aim. However, taking into account the context of the political debate on matters of public interest and, *inter alia*, the fact that some statements lacking a factual basis were made in good faith, the Court considered that the applicant had not exceeded the acceptable limits of criticism and found a violation of Article 10 of the Convention[62]. In *Kwiecień v. Poland*[63] (2007), concerning civil liability for circulating a defamatory open letter about a public official standing for election, the Court found a violation of Article 10. It reiterated that the limits of acceptable criticism are wider with regard to public officials and that sanctions imposed in the context of public-interest electoral debate must be proportionate. In *Ecodefence and Others v. Russia* (2022), concerning various measures, including dissolution, imposed on the applicant associations under the Foreign Agents Act, the Court found a violation of Article 11 of the Convention taking into account that the Act as applied fell short of the foreseeability requirement and judicial review failed to provide adequate and effective safeguards against the arbitrary and discriminatory exercise of the wide discretion left to the executive[64].

---

[58] European Court of Human Rights, *Bradshaw and Others v. the United Kingdom*, no. 15653/22, judgment of 22 July 2025.
[59] European Court of Human Rights, *Political Party “Patria” and others v. the Republic of Moldova*, nos. 5113/15 and Others, judgment of 4 August 2020, paras. 32-38.
[60] European Court of Human Rights, *Salov v. Ukraine*, no. 65518/01, judgment of 6 September 2005.
[61] European Court of Human Rights, *Kita v. Poland*, no. 57659/00, judgment of 8 July 2008.
[62] In February 2025, the Commission and the European Board for Digital Services endorsed the integration of the 2022 Code of Practice on Disinformation as a Code of Conduct on Disinformation into the framework of the DSA.
[63] European Court of Human Rights, *Kwiecień v. Poland*, no. 51744/99, judgment of 9 January 2007.
[64] European Court of Human Rights, *Ecodefence and others v. Russia*, nos. 9988/13 and 60 others, judgment of 14 June 2022, para. 118.

96. The Court has also examined security-related contexts involving information measures. In *Gaponenko v. Latvia*[65] (2023), it declared inadmissible complaints relating principally to detention on remand in criminal proceedings concerning alleged offences directed against national independence, sovereignty and territorial integrity, linked to a series of social-media posts; the decision illustrates the Court's Article 5 approach to "reasonable suspicion" and justification requirements in a context framed domestically as involving hostile information campaigns and hybrid threats. In *Rotaru v. Romania*[66] (2000), the Court found a violation of Article 8 of the Convention in respect of the storage and use of personal information by the intelligence services, holding that domestic law must indicate with reasonable clarity the scope and manner of exercise of discretion and provide adequate safeguards against abuse; in the absence of such safeguards, the interference was not "in accordance with the law".

97. Finally, the Court has consistently reaffirmed the central importance of political pluralism and democratic debate. In *Castells v. Spain*[67] (1992), it found a violation of Article 10 of the Convention in respect of the criminal conviction of an opposition senator for insulting the Government. The Court reiterated that freedom of expression constitutes one of the essential foundations of a democratic society and that interferences with the freedom of expression of an opposition member of parliament call for the closest scrutiny, noting that the limits of acceptable criticism are wider with regard to the Government than to private individuals. In *Eğitim ve Bilim Emekçileri Sendikası v. Turkey*[68] (2012), concerning dissolution proceedings against a trade union because its statutes defended education in the "mother tongue", the Court found violations of Articles 10 and 11 of the Convention. It emphasised that pluralism, tolerance and broadmindedness are hallmarks of a democratic society and that restrictions on freedom of association and expression require relevant and sufficient reasons; in the absence of incitement to violence or a genuine threat to territorial integrity, compelling the union to amend its statutes was not necessary in a democratic society.

98. Taken together, this case-law indicates that, in addressing challenges such as election interference, threats to media freedom, and other risks to democratic processes - including those arising from organised crime, cybercrime, corruption or the malign use of digital technologies - States may legitimately pursue aims such as protecting national security, public order and the integrity of electoral systems. At the same time, any restrictive measures must be prescribed by law, pursue a legitimate aim and be necessary in a democratic society, including by being proportionate. The Court applies heightened scrutiny where political expression, media activity and democratic participation are concerned, while recognising the margin of appreciation afforded to States in complex and sensitive contexts. In certain circumstances, the Court has found that restricting a statement without a factual basis violated the freedom of expression guaranteed by Article 10 of the Convention[69].

2. Council of Europe Conventions of sectoral relevance

99. In addition to the Convention system, several Council of Europe conventions establish binding sectoral frameworks that may be relevant to specific aspects of information manipulation. These instruments are open to non-member States and reflect areas in which States have agreed on common legal standards.

100. The Convention on Cybercrime provides binding rules concerning offences against computer systems and data, procedural powers and international co-operation. Although it does not address information manipulation in the context of FIMI-related activities, it may be relevant where influence operations rely on cyber-enabled practices or affect digital infrastructures[70].

[65] European Court of Human Rights, *Gapoņenko v. Latvia*, no. 30237/18, decision of 23 May 2023.
[66] European Court of Human Rights, *Rotaru v. Romania*, no. 28341/95, Grand Chamber judgment of 4 May 2000.
[67] European Court of Human Rights, *Castells v. Spain,* no. 11798/85, judgment of 23 April 1992.
[68] European Court of Human Rights, *Eğitim ve Bilim Emekçileri Sendikası v. Turkey*, no. 20641/05, judgment of 25 September 2012.
[69] European Court of Human Rights, *Salov v. Ukraine*, no. 65518/01, judgment of 6September 2005; *Kita v. Poland*, cited above.
[70] Council of Europe, Convention on Cybercrime (2001, ETS No. 185), establishing binding rules on offences against computer systems and data (see in particular Articles 2, 4 and 5), procedural powers (Article 14) and international co-operation (Article 23).

101. The Second Additional Protocol to the Convention on Cybercrime further strengthens cross-border co-operation in relation to electronic evidence and co-operation with service providers. These instruments provide an established procedural framework that may be applicable where FIMI-related conduct involves cyber elements. They may also facilitate early investigative action where attribution remains complex[71].

102. The Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law establishes binding principles for the governance of AI systems. It addresses risks related to automated decision-making, transparency and accountability, including where such systems may affect democratic processes or fundamental rights. The Framework Convention covers technological vectors that may be used in information manipulation, while remaining grounded in a rights-based approach[72].

3. Soft-law instruments and intergovernmental policy work

103. Binding conventions are complemented by a substantial body of soft-law instruments adopted by the Committee of Ministers and developed through intergovernmental co-operation[73]. These instruments provide guidance on how convention standards can be implemented in practice by States and relevant stakeholders.

104. In addition to its binding standards, the Council of Europe has developed a substantial body of non-binding instruments and intergovernmental policy work, including recommendations adopted by the Committee of Ministers, that can support democratic resilience to disinformation and FIMI by promoting and supporting media freedom and pluralism, journalism media and information literacy and information integrity. Through policy documents, recommendations, guidelines and intergovernmental co-operation, these initiatives address structural vulnerabilities in the information environment and seek to reinforce the conditions for it to be free and pluralistic supportive of an informed public debate, in full respect of freedom of expression and other human rights[74].

105. Work conducted under the Steering Committee on Media and Information Society (CDMSI) has contributed to the development of relevant Council of Europe standards and policy instruments aimed at strengthening media freedom and information integrity, supporting independent journalism and promoting pluralism and transparency in the media environment[75]. In this context, information integrity is used as policy concept. It is understood as safeguarding the conditions for accurate, reliable and pluralistic information ecosystems, in line with freedom of expression standards. Parallel initiatives on media and information literacy address long-term resilience by enhancing individuals' capacity to engage critically with information[76].

---

[71] Council of Europe, Second Additional Protocol to the Convention on Cybercrime on enhanced co-operation and disclosure of electronic evidence (2022, CETS No. 224). The Protocol enhances cross-border co-operation, including direct co-operation with service providers, expedited disclosure of subscriber information and traffic data, and reinforced safeguards for human rights and data protection (see in particular Articles 6–10 and 13–14).

[72] Council of Europe, Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law (2024, CETS No. 225), establishing binding principles for the governance of AI systems, including safeguards relating to human rights, democratic processes, transparency and accountability (see in particular Articles 1, 3 and 5).

[73] This includes work carried out under the auspices of several intergovernmental committees of the Council of Europe, including the Steering Committee on Democracy (CDDEM), in particular its work on the application and implementation of the Reykjavík Principles; the Steering Committee on Media and Information Society (CDMSI); the Steering Committee for Human Rights (CDDH); the European Committee on Crime Problems (CDPC); the Steering Committee on New and Emerging Digital Technologies (CDNET); the Committee on Artificial Intelligence (CAI); and other relevant sectoral bodies dealing with democratic governance, media freedom, electoral integrity, digital transformation and human rights safeguards.

[74] Council of Europe, Resisting Disinformation: 10 Building Blocks to Strengthen Information Integrity and National Media and Information Literacy (MIL) Strategies – Practical Steps and Indicators, policy documents adopted by the Steering Committee on Media and Information Society (CDMSI), addressing information integrity, media pluralism and media and information literacy as complementary components of democratic resilience, in a manner consistent with freedom of expression and other fundamental rights.

[75] Recommendation CM/Rec(2012)1 on public service media governance (15 February 2012); Recommendation CM/Rec(2007)3 on the remit of public service media in the information society (31 January 2007); Recommendation no. R(96)10 on the guarantee of the independence of public service broadcasting (for an overview, see Digest: Council of Europe Standards on Public Service Media, 2022). Recommendation CM/Rec(2022)4 on promoting a favourable environment for quality journalism in the digital age (17 March 2022), see also the Report on Good practices for sustainable news media financing, CDMSI/MSI-REF, 2023; Recommendation CM/Rec(2018)1 on media pluralism and transparency of media ownership (7 March 2018). Recommendation CM/Rec(2007)2 on media pluralism and diversity of media content (31 January 2007); Guidance note on countering the spread of online mis- and disinformation through fact-checking and platform design solutions in a human rights compliant manner, (29 November-1 December 2023), CM(2024)9-add1.

[76] Council of Europe, Steering Committee on Media and Information Society (CDMSI), National Media and Information Literacy (MIL) Strategies – Practical Steps and Indicators (2025), providing policy guidance on the development of national MIL strategies aimed at strengthening individuals' capacity to engage critically with information as a component of long-term democratic resilience.

106. Other Council of Europe bodies contribute through thematic standards addressing democratic participation and equality. The Parliamentary Assembly and the European Commission for Democracy through Law (Venice Commission) have developed guidance related to electoral integrity, democratic processes and political participation[77].

107. Council of Europe bodies have consistently addressed the links between information manipulation, social inequalities and polarisation. Their work recognises that disinformation and manipulation are particularly effective in societies marked by existing social fractures and discrimination. Such practices deliberately exploit identity-based tensions, amplify narratives of division and weaken social cohesion and democratic trust[78].

108. Specific attention has been given to groups that are disproportionately targeted by disinformation and manipulation campaigns. Council of Europe standards and policy work highlight the recurrent targeting of women, LGBTI persons, Roma and Travellers, migrants and other minorities, including through the instrumentalisation of migration and identity-based narratives. These practices undermine equality, dignity and the ability of individuals to participate effectively in democratic life [79].

109. Council of Europe work has also underlined the particular vulnerability of children and young people in the information environment. Exposure to manipulative narratives at early stages of individual and group formation may have lasting effects on socialisation, political participation and trust in democratic institutions. Relevant standards therefore link information integrity with the protection of children's rights and inclusive approaches to education and participation[80].

C. United Nations system: sovereignty, non-intervention and information integrity

110. Within the United Nations (UN) system, issues relevant to FIMI are primarily addressed through general principles and obligations of international law governing State conduct. The UN framework does not conceptualise FIMI as a distinct phenomenon. Its relevance lies in the regulation of cross-border conduct such as through the principles of non-intervention and international co-operation[81].

111. The principle of non-intervention occupies a central place in this framework. It prohibits States from intervening in matters within the domestic jurisdiction of another State through coercive means. This principle applies across political, economic and other domains, and constitutes a cornerstone of the international legal order.

112. The scope of the prohibition of intervention has been clarified by the International Court of Justice (ICJ) in its judgment in Military and Paramilitary Activities in and against Nicaragua[82]. The ICJ held that intervention is unlawful where it involves coercion with regard to matters in which a State is permitted to decide freely, such as its political, economic or social system.

113. This jurisprudence illustrates the challenges involved in applying existing principles of international law to contemporary information-related and digital practices. Influence activities, including those conducted through information channels, do not in themselves amount to prohibited intervention unless they reach a threshold of coercion, as traditionally interpreted. The application of international law to digital activities, including the interpretation of the principle of non-intervention, continues to be discussed in international

[77] Venice Commission, Code of Good Practice in Electoral Matters (2002, CDL-AD(2002)023), setting standards for democratic elections, including principles of free suffrage, voter autonomy and the free formation of the opinion of the electorate.
[78] Parliamentary Assembly of the Council of Europe, Resolution 2326 (2020), Report "Democracy hacked? How to respond?", paras. 11–13, highlighting the links between disinformation, social polarisation and the erosion of democratic trust.
[79] Council of Europe, Committee of Ministers, Recommendation CM/Rec(2019)1 on preventing and combating sexism (2019), highlighting the disproportionate targeting of women through discriminatory narratives and practices that undermine equality, dignity and effective participation in democratic life.
[80] Council of Europe, Committee of Ministers, Recommendation CM/Rec(2018)7 on Guidelines to respect, protect and fulfil the rights of the child in the digital environment (2018), addressing children's particular vulnerability in the information environment and linking information integrity with the protection of children's rights, education and participation.
[81] Charter of the United Nations (1945), in particular Articles 1 and 2, establishing the principles of sovereign equality, non-intervention and international co-operation governing State conduct.
[82] Charter of the United Nations, Article 2(7); International Court of Justice, Military and Paramilitary Activities in and against Nicaragua (*Nicaragua v. United States of America*), judgment of 27 June 1986, paras. 202–205.

fora. As a result, many practices commonly associated with FIMI may fall outside the scope of non-intervention as it is currently understood in international law[83].

114. In addition to non-intervention, international law recognises obligations of due diligence, requiring States to take reasonable measures to prevent significant harm originating from their territory. While this obligation has been developed primarily in other contexts, it may be relevant where information-related activities produce cross-border effects.

115. Binding treaty provisions may also be relevant in specific contexts. In particular, Article 20 of the International Covenant on Civil and Political Rights requires States to prohibit propaganda for war and advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence[84].

116. Alongside these general principles, the UN has developed non-binding initiatives addressing the integrity of the information environment. These initiatives focus on freedom of expression, access to information and the role of independent media, and seek to promote international co-operation and shared standards rather than legal obligations[85].

117. Within this broader framework, specialised agencies of the UN also address aspects of information integrity.

118. The United Nations Educational, Scientific and Cultural Organization (UNESCO) addresses disinformation and information manipulation within its mandate on freedom of expression, media development and education. Its work promotes media pluralism, supports independent journalism and strengthens media and information literacy as long-term responses to manipulation.

119. UNESCO initiatives are framed as guidance and capacity-building tools. They aim to support rights-based approaches to information governance without establishing binding legal standards or enforcement mechanisms[86].

120. The UN approach thus remains largely principled and does not establish a specific legal framework addressing FIMI. It provides a universal framework for assessing state conduct and for promoting co-operation. This framework is grounded in binding human rights treaties and general principles of international law. It nevertheless offers limited guidance for addressing information manipulation practices operating below the threshold of coercive intervention. This reflects both the broad scope of the UN mandate and the sensitivity of regulating information-related activities at the international level.

D. European Union: political, operational, regulatory and judicial approaches

121. Within the international landscape, the European Union (EU) has developed and institutionalised a dedicated operational concept of FIMI. Its approach combines external action, internal market regulation and fundamental rights protection. It does not rely on a single legal instrument addressing FIMI as a whole, but on a set of complementary and sector-specific frameworks.

---

[83] United Nations General Assembly, Resolution 2625 (XXV), Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States (1970), and International Court of Justice, Military and Paramilitary Activities in and against Nicaragua (Nicaragua v. United States of America), Judgment of 27 June 1986, paras. 202–209, clarifying the prohibition of intervention and the central role of coercion as its defining element.

[84] International Covenant on Civil and Political Rights (ICCPR), adopted by UN General Assembly resolution 2200A (XXI), 16 December 1966, entered into force 23 March 1976, Article 20.

[85] United Nations, Global Principles for Information Integrity – Recommendations for Multi-stakeholder Action (2024), setting out non-binding principles on information integrity, freedom of expression and international co-operation.

[86] UNESCO, Windhoek+30 Declaration: Information as a Public Good (2021), and Guidelines for Regulating Digital Platforms (2023), promoting freedom of expression, media pluralism, independent journalism and media and information literacy through non-binding, rights-based guidance and capacity-building approaches.

1. Political co-ordination and strategic orientation

122. At the political level, the EU has articulated a cross-cutting approach to protecting democratic systems through the European Democracy Shield[87], under which a series of actions are to be progressively rolled out in 2026–2027. Building on the existing legal and policy framework, this initiative encompasses new measures in three priority areas: reinforcing situational awareness and response capacities to safeguard the integrity of the information space; strengthening democratic institutions, including through free and fair elections and free and independent media; and boosting societal resilience and citizens' engagement.

123. In this context, the European Centre for Democratic Resilience provides a framework for gathering expertise and facilitating the sharing of information and best practices to strengthen situational awareness, democratic resilience and response capacity.

2. Conceptual and operational framework on FIMI

124. The EU is the only international organisation to have developed and institutionalised a dedicated operational concept of FIMI. This work has been carried by different actors within the European External Action Service, which uses FIMI as an analytical and operational category to describe co-ordinated, intentional and foreign-linked information activities[88].

125. The EU FIMI framework is based on an analytical methodology focusing on patterns of behaviour, co-ordination and intent, rather than on the falsity or legality of individual content. It is designed to support the identification, analysis and exposure of foreign information manipulation activities across different contexts.

126. This analytical approach relies largely on open-source intelligence and structured monitoring. It is supported by shared taxonomies, indicators and data models intended to ensure consistency and comparability across cases and to facilitate information-sharing among EU institutions and member States[89].

127. On the basis of this analytical work, the EU has developed a comprehensive FIMI Toolbox. This toolbox brings together a wide range of preventive, responsive and deterrent measures. These include strategic communication aimed at supporting access to reliable information and media diversity, public attribution, diplomatic engagement, co-operation with platforms and civil society, capacity-building, and, where appropriate, restrictive measures under the Common Foreign and Security Policy. It also encompasses measures designed to enhance the resilience and integrity of the digital information environment.

128. The FIMI Toolbox is conceived as an evolving and non-exhaustive set of instruments. It includes early-warning mechanisms, co-ordinated responses through international partnerships, exposure of information manipulation operations, support for independent media, media and information literacy initiatives, and co-operation with third countries and international organisations. These tools are applied in a context-specific manner and are not based on automatic or content-based triggers.

129. EU operational work on FIMI has also expanded through thematic and contextual analysis. Dedicated reporting has addressed FIMI targeting electoral processes, vulnerable groups and specific geographic regions, as well as the use of emerging technologies.

---

[87] Joint Communication to the European Parliament, the Council the European Economic and Social Committee and the Committee of the Regions, European Democracy Shield: Empowering Strong and Resilient Democracies, JOIN/2025/791 final.
[88] European External Action Service (EEAS), Report on Foreign Information Manipulation and Interference Threats (1st Report 2023; 2nd Report 2024; 3rd Report 2025), establishing an operational and analytical framework for identifying and analysing co-ordinated, intentional and foreign-linked information manipulation activities, based on behavioural patterns rather than content assessment.
[89] European Union, EU FIMI Toolbox, consolidating preventive, responsive and deterrent measures, including strategic communication, public attribution, diplomatic engagement and international co-operation, as a non-exhaustive and context-specific set of tools for addressing foreign information manipulation activities.

130. Methodological guidance has complemented this operational framework. Guidance on open-source investigations has been developed to support responsible evidence-gathering, with attention to ethical standards, data protection and the protection of vulnerable groups. This reflects the EU emphasis on evidence-based and rights-aware analysis[90].

3. Regulatory instruments affecting the information environment

131. Alongside its operational approach, the EU has adopted binding regulatory instruments governing the functioning of the online information environment. These instruments do not define FIMI as such and do not focus directly on foreign interference. They address systemic risks affecting civic discourse, democratic processes and political communication, including risks that may be exploited by FIMI activities[91].

132. The Digital Services Act (DSA) introduces due-diligence obligations for online platforms, with enhanced requirements for very large online platforms and very large online search engines. Articles 34 and 35 require such platforms to assess and mitigate systemic risks affecting civic discourse and electoral processes, including risks linked to the dissemination and amplification of manipulative information[92].

133. The DSA also establishes transparency obligations relating to recommender systems, content moderation and online advertising. These provisions are relevant where information manipulation exploits algorithmic amplification, opaque distribution mechanisms or monetisation pathways to increase reach and impact.

134. To support compliance with the obligations under the DSA, the European Commission has adopted guidelines on the mitigation of systemic risks for electoral processes and co-operates with national authorities of EU member States regarding their preparedness ahead of elections. The Code of Conduct on Disinformation also provides a set of commitments and detailed measures aimed at mitigating disinformation-related risks[93].

135. The Artificial Intelligence Act (Regulation (EU) 2024/1689) establishes a horizontal regulatory framework for AI systems and general-purpose AI models. While it does not address foreign interference as such, it introduces binding obligations relevant to the information environment, including transparency requirements for AI-generated content, obligations for providers of general-purpose AI models and safeguards for high-risk systems. These provisions are particularly relevant where information manipulation is facilitated or amplified through AI-driven systems[94].

136. In addition, Regulation (EU) 2024/900 on the transparency and targeting of political advertising establishes harmonised rules on the identification, transparency and targeting of political advertisements, including in cross-border contexts. It applies irrespective of whether political communication originates from domestic or foreign actors[95].

---

[90] European External Action Service (EEAS), Guidelines on Open-Source Investigations, providing methodological guidance for evidence-based analysis of information manipulation, with attention to ethical standards, data protection and the protection of vulnerable groups.

[91] Relevant EU instruments include, inter alia, the Digital Services Act; the Artificial Intelligence Act; Directive (EU) 2022/2555 (NIS2 Directive); Directive (EU) 2022/2557 on the resilience of critical entities (CER Directive); Regulation (EU) 2024/900 on the transparency and targeting of political advertising; the European Media Freedom Act; and Directive 2010/13/EU on Audiovisual Media Services (as amended). While pursuing distinct objectives within digital, media and democratic governance frameworks, these instruments contribute to strengthening transparency, media freedom, platform accountability, cybersecurity and institutional resilience in areas that may intersect with FIMI-related risks.

[92] Regulation (EU) 2022/2065 of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act), in particular Articles 34 and 35, introducing due-diligence obligations for very large online platforms to assess and mitigate systemic risks affecting civic discourse and electoral processes.

[93] In February 2025, the Commission and the European Board for Digital Services endorsed the integration of the 2022 Code of Practice on Disinformation as a Code of Conduct on Disinformation into the framework of the DSA.

[94] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act), OJ L 2024/1689, 12 July 2024.

[95] Regulation (EU) 2024/900 of the European Parliament and of the Council on the transparency and targeting of political advertising, establishing harmonised transparency and disclosure requirements applicable to political advertising, irrespective of the origin of the communication.

137. The regulation on political advertising limits certain targeting techniques, strengthens disclosure requirements and introduces obligations for political advertising publishers and intermediaries. These measures seek to reduce opaque influence practices and protect the integrity of democratic processes[96].

138. The European Media Freedom Act and the Audiovisual Media Services Directive establish frameworks aimed at reinforcing media freedom, transparency of media ownership and safeguards for pluralism within the audiovisual sector. While not designed specifically to address FIMI, these instruments contribute to strengthening the resilience of the media environment in contexts where manipulation and interference may occur.

139. A wide range of other EU acquis, co-operation frameworks and policy tools relevant to addressing FIMI is also in place[97].

4. Judicial interpretation at EU level

140. The interpretation and application of EU regulatory instruments affecting the information environment fall within the jurisdiction of the Court of Justice of the European Union (CJEU). The CJEU ensures compliance with the Charter of Fundamental Rights of the European Union, which includes the protection of freedom of expression and information[98].

141. The CJEU has recognised that measures aimed at safeguarding democratic processes and ensuring fair political competition may justify certain limitations on expression, provided that they respect the essence of fundamental rights and comply with proportionality requirements.

142. The CJEU has also examined restrictive measures adopted in response to systematic disinformation and propaganda activities linked to armed conflict. In *RT France v. Council*, the General Court upheld the temporary suspension of broadcasting activities of a State-controlled media outlet and considered that such measures pursued legitimate objectives linked to the protection of public order and Union values[99].

143. The EU approach therefore combines political co-ordination, operational tools, co-operation frameworks, sectoral binding regulation, and judicial oversight.

E. Other international organisations

144. Beyond the frameworks examined above, a number of international organisations and political formats address issues related to foreign interference and information manipulation within the limits of their respective mandates. These approaches do not establish binding legal standards governing FIMI as such. They operate primarily through political commitments, co-operative mechanisms, policy guidance or capacity-building, and contribute to awareness, preparedness and co-ordination rather than to legal regulation[100].

---

[96] Regulation (EU) 2024/900 of the European Parliament and of the Council of 13 March 2024 on the transparency and targeting of political advertising, in particular Articles 5(2), 11–13 and 18–19, OJ L 2024/900, 20 March 2024.

[97] Existing EU acquis includes, for example, a number of instruments that may be relevant for addressing certain aspects of FIMI. These include the Counterterrorism Directive (Directive (EU) 2017/541), the Directive defining criminal offences and penalties for the violation of EU restrictive measures (Directive (EU) 2024/1226), the EU Foreign Direct Investment (FDI) Screening Regulation (Regulation (EU) 2019/452), the Critical Entities Resilience Directive (Directive (EU) 2022/2557), the NIS2 Directive (Directive (EU) 2022/2555), the Cyber Resilience Act (Regulation (EU) 2024/2847), and the anti-SLAPP Directive (Directive (EU) 2024/1069). EU co-operation frameworks and policy tools also include, for example, the European Co-operation Network on Elections, the Commission Recommendation on inclusive and resilient elections, the Compendium on Elections Cybersecurity and Resilience, the Commission Recommendations on anti-SLAPP and on the safety of journalists, and the European Digital Media Observatory.

[98] Charter of Fundamental Rights of the European Union (2000), in particular Articles 11 and 52, providing the constitutional framework for judicial review of measures affecting freedom of expression and information, including proportionality requirements.

[99] General Court of the European Union, *RT France v. Council*, Case T-125/22, judgment of 27 July 2022, ECLI:EU:T:2022:483.

[100] OECD, Recommendation on Information Integrity, 2022, recognising the role of non-binding, co-operative and policy-based approaches in addressing risks to the information environment.

1. North Atlantic Treaty Organisation

145. The North Atlantic Treaty Organization (NATO) addresses information-related challenges within its broader approach to hybrid threats[101]. In this framework, information manipulation, characterised as "information threats" is analysed as one component of co-ordinated actions combining political, cyber, economic and, where relevant, military means. The emphasis lies on collective security, resilience and preparedness, rather than on the regulation of expression or information flows[102].

146. NATO's work in this area focuses on situational awareness, strategic communication and the strengthening of societal and institutional resilience. It includes analytical frameworks, training activities and co-operation mechanisms designed to support Allies in detecting, understanding and responding to hostile information activities, particularly in crisis and conflict contexts[103].

147. The NATO approach is operational and doctrinal in nature. It does not seek to establish legal standards governing information manipulation, nor does it address the human rights implications of responses to such activities. Questions relating to freedom of expression, proportionality and safeguards therefore fall outside NATO's mandate and are addressed in other international frameworks[104].

2. Organization for Security and Co-operation in Europe

148. The Organization for Security and Co-operation in Europe (OSCE) addresses risks related to foreign interference through its comprehensive concept of security, which integrates political, military, economic and environmental, and human dimensions. Its approach to information manipulation is grounded in political commitments adopted by participating States, with a strong focus on democratic institutions, electoral processes and media pluralism[105].

149. OSCE activities relevant to information manipulation include election observation missions, support for independent and pluralistic media, and dialogue among participating States on emerging security risks. These measures aim to identify vulnerabilities, promote confidence-building and prevent destabilisation through co-operative means. They rely on peer engagement and political consensus rather than on binding legal obligations or enforcement mechanisms[106].

150. Within the OSCE framework, specific attention is given to media freedom and the safety of journalists through the work of the OSCE Representative on Freedom of the Media. This mandate focuses on monitoring media-related developments, responding to threats against journalists and independent media, and addressing disinformation, hate speech, and intimidation affecting the media ecosystem[107].

151. The OSCE approach combines electoral support, media-related commitments and security dialogue within a non-binding framework. It contributes to early warning and prevention in relation to FIMI, while remaining based on political commitments adopted by participating States rather than enforceable legal standards.

---

[101] NATO's approach to counter information threats, updated 3 February 2025, defining information threats as "intentional, harmful, manipulative and co-ordinated activities conducted by State and non-State actors", including hostile information operations, information manipulation and interference by foreign actors, and disinformation.
[102] NATO, Strategic Concept (Madrid, 2022), identifying information manipulation and disinformation as elements of hybrid threats affecting Allied security, within a framework focused on collective defence, resilience and preparedness.
[103] NATO, NATO's approach to countering hybrid threats, updated 3 February 2025, describing operational, analytical and resilience-based measures to detect, understand and respond to hybrid activities, including hostile information activities.
[104] NATO, Strategic Concept, adopted at the Madrid Summit, 29 June 2022; NATO, "NATO's approach to countering information threats", updated 3 February 2025; NATO, "Countering hybrid threats", updated 29 January 2026.
[105] OSCE, Charter for European Security (Istanbul, 1999), articulating the OSCE's comprehensive concept of security and its emphasis on co-operative, preventive and confidence-building approaches to emerging security risks.
[106] OSCE, Document of the Copenhagen Meeting of the Conference on the Human Dimension (1990), setting out political commitments on democratic elections, pluralism, free expression and electoral integrity.
[107] OSCE, Ministerial Council Decision No. 3/18 on Safety of Journalists (Milan, 2018), reaffirming political commitments to media freedom, the safety of journalists and the protection of independent media in the digital environment.

3. Organisation for Economic Co-operation and Development

152. The Organisation for Economic Co-operation and Development (OECD) approaches information manipulation through governance and policy frameworks aimed at strengthening information integrity. Its work focuses on the functioning of information ecosystems and on policy responses to systemic risks affecting trust and democratic governance[108].

153. OECD instruments are non-binding and programmatic. They provide analytical guidance and comparative policy analysis intended to inform national policy-making, without defining foreign interference or information manipulation as legal categories.

4. Group of Seven (G7)

154. The Group of Seven (G7) addresses foreign interference and disinformation through political co-ordination among its members. Its approach focuses on information-sharing, situational awareness and co-ordinated responses, without creating legal standards or binding obligations[109].

155. The G7 Rapid Response Mechanism facilitates voluntary co-operation to identify and respond to foreign interference activities, including co-ordinated disinformation campaigns. While established within the G7 framework, it also engages non-G7 Associate Members in its co-ordination activities[110]. It operates through consensus and diplomatic co-ordination rather than through enforcement mechanisms.

156. The G7 Leaders' Communiqué adopted in Hiroshima reaffirmed the political commitment of G7 members to counter foreign interference and disinformation. It situates these efforts within a broader commitment to democratic values and open societies, without creating new legal obligations or definitions[111].

CHAPTER 4 – CATEGORIES OF RESPONSES TO FIMI

157. This chapter sets out the main categories of responses to FIMI. It classifies these responses according to their primary function.

A. General considerations

158. Responses to FIMI form a heterogeneous set of measures that differ in their objectives, legal nature, level of intrusiveness and institutional setting. These responses may pursue different purposes in addressing FIMI: strengthening democratic resilience; regulating relevant democratic and information environments; detecting and analysing co-ordinated manipulation[112] and interference; ensuring accountability and disruption; and enhancing co-operation and co-ordination at national and international level.

159. This chapter adopts a functional approach to these responses. Rather than organising them by institutional actor, legal instrument or geographical level, it classifies them according to the primary institutional function they perform in addressing FIMI. These categories describe what different types of responses seek to achieve and how they operate, irrespective of whether they are implemented at national or international level, or through legal, policy-based or operational means. This list is not exhaustive and may evolve as FIMI tactics continue to develop and responses adapt accordingly.

[108] OECD, Recommendation of the Council on Information Integrity (OECD/LEGAL/0505, 2024), establishing a non-binding governance and policy framework to strengthen information integrity and address systemic risks affecting trust and democratic governance, through analytical and programmatic guidance to support national policy-making.
[109] Group of Seven (G7), Rapid Response Mechanism (2018), establishing a voluntary and non-binding co-ordination mechanism to facilitate information-sharing, situational awareness and co-ordinated responses to foreign interference activities.
[110] The G7 Rapid Response Mechanism (RRM) was established in 2018 by G7 members (Canada, France, Germany, Italy, Japan, the United Kingdom and the United States), together with the European Union. In addition to its core members, the RRM engages a number of non-G7 Associate Members in its co-ordination activities.
[111] Group of Seven (G7), Charlevoix Commitment on Defending Democracy from Foreign Threats (2018), and Hiroshima Leaders' Communiqué (2023), reaffirming political commitments to counter foreign interference and disinformation as part of a broader commitment to democratic values and open societies, without establishing legal standards or binding obligations.
[112] For the analytical understanding of co-ordinated manipulation, including deceptive and inauthentic practices, see Chapter 2 (section on "Information manipulation").

160. The categories presented in this chapter are analytical and non-hierarchical. They should not be understood as sequential stages or as implying that one type of response should precede or replace another. They are not mutually exclusive and may operate in parallel or in combination. Each category may encompass a wide variety of measures and practices, implemented by different actors and adapted to specific national or contextual circumstances. Certain responses may be time-limited or situation-specific, including in periods of heightened vulnerability such as electoral processes.

161. References to concrete national or international examples are used solely for illustrative purposes, to clarify the functional logic of each category. They are neither exhaustive nor intended to constitute an assessment of effectiveness or a set of recommended practices.

162. Addressing FIMI requires a whole-of-society approach engaging public authorities, independent institutions, civil society, academia and researchers, media actors and private-sector actors, including online service providers. It also requires a whole-of-government approach ensuring co-ordination across relevant public authorities and policy domains. No single category of response is sufficient in isolation. In periods of heightened vulnerability, including electoral processes or major public debates, certain responses may require particular co-ordination, visibility or timely activation.

B. Resilience and strengthening responses

163. Resilience and strengthening responses focus on reinforcing the structural conditions that enable democratic societies to withstand manipulation and interference. Their primary objective is to strengthen democratic resilience by addressing structural vulnerabilities within democratic societies and information environments.

164. Democratic processes and public debate increasingly rely on the secure and reliable functioning of digital infrastructures and information systems. The protection of these systems against cyberattacks, sabotage or other forms of malicious interference contributes to broader democratic resilience. Strengthening preparedness, risk management and response capacities in this field may therefore complement efforts aimed at reinforcing the integrity of the information environment[113].

165. These responses do not focus on individual pieces of content or on the identification of specific perpetrators. Instead, they address the underlying conditions that enable FIMI to resonate, spread or persist. They aim to reinforce the capacity of democratic systems, institutions and societies to withstand manipulation while preserving open debate and fundamental freedoms.

166. These responses operate primarily through long-term and medium-term measures. They are typically continuous rather than reactive in nature and seek to enhance trust, pluralism, critical capacities and social cohesion. They generally rely on enabling and supportive measures and do not depend on coercive or punitive tools.

167. This category of responses is inherently cross-cutting. It may be implemented at national, regional or local level, and may involve public authorities, independent institutions, civil society, media actors, educational bodies and private stakeholders. Similar functional approaches can also be observed at international level, where frameworks, standards and co-operative initiatives aim to support democratic resilience without directly regulating expression or imposing binding obligations on States.

168. Strengthening resilience may also involve structured public oversight and sustained co-operation with civil society, academia and independent experts in order to enhance transparency and informed public awareness of manipulation risks, while fully respecting fundamental rights.

169. Resilience and strengthening responses address several interrelated dimensions of democratic life and the information environment. These include, in particular, the protection of media freedom and pluralism, the promotion of quality journalism, the development of education and media and information literacy, and broader efforts to strengthen social inclusion and trust in democratic institutions.

[113] Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements (Cyber Resilience Act), the notion of “cyber resilience” generally referring to risk assessment, prevention, preparedness, response and recovery capacities in relation to digital infrastructures and information systems.

170. A defining feature of this category of responses is its close relationship with freedom of expression. By focusing on enabling conditions rather than prohibitions, this approach seeks to reinforce the quality and resilience of public debate without restricting lawful expression or political participation. At the same time, their effectiveness depends on sustained implementation and on co-ordination across sectors, as their impact is often gradual and difficult to measure in the short term.

1. Media freedom, pluralism and quality journalism

171. Media freedom, pluralism and quality journalism constitute a core component of resilience and strengthening responses to FIMI. Independent and diverse media ecosystems reduce the effectiveness of manipulative interference by ensuring that public debate is informed by a plurality of sources, perspectives and editorial lines[114].

172. Media freedom enables journalists and other media actors to investigate, contextualise and expose attempts at manipulation and covert interference. Where media operate without undue political, economic or regulatory pressure, they are better positioned to inform the public in an independent and reliable manner. They can identify co-ordinated interference efforts and provide the public with reliable information about their nature and objectives.

173. Media pluralism further strengthens resilience by limiting the risk of narrative capture. A diverse and sustainable media landscape, including public service media, commercial outlets and community-based media, reduces dependency on a narrow set of information sources and mitigates the impact of co-ordinated FIMI campaigns seeking to dominate public discourse[115].

174. Quality journalism plays a specific preventive role through professional standards of accuracy, verification and accountability. These standards help limit the unintended amplification of manipulated narratives, including in highly polarised or emotionally charged contexts. Conversely, economic precarity, concentration of ownership or systematic harassment of journalists may weaken the capacity of media to fulfil this function and increase vulnerability to interference. Public authorities can strengthen this resilience through support of independent and effective self-regulatory mechanisms and transparent and regular communication, including planned media briefings.

175. The safety of journalists constitutes an essential component of democratic resilience. Threats, harassment, intimidation and strategic litigation targeting journalists may significantly weaken the capacity of media to investigate and expose manipulation and interference. Ensuring a safe and enabling environment for journalism is therefore a key element in strengthening resilience to FIMI-related activities[116].

176. Particular vigilance is required in contexts of heightened democratic sensitivity, including electoral periods, public demonstrations and situations of crisis. In such contexts, threats or pressures against journalists may have a disproportionate chilling effect on public debate and democratic participation and undermine democratic resilience[117].

177. Specific concerns arise where media outlets are owned or controlled by a foreign State and operate as instruments of co-ordinated interference. While media freedom remains a cornerstone of democratic societies, member States may adopt lawful and proportionate measures in response to clear evidence of systematic manipulation, subject to effective judicial oversight and safeguards.

[114] Council of Europe, Resisting Disinformation: 10 Building Blocks to Strengthen Information Integrity, policy document adopted by the Steering Committee on Media and Information Society (CDMSI), identifying media freedom, pluralism and quality journalism as core elements of democratic resilience.
[115] Recommendation CM/Rec(2018)1 of the Committee of Ministers to member States on media pluralism and transparency of media ownership, addressing risks related to concentration and undue influence in the media landscape (7 March 2018).
[116] Recommendation CM/Rec(2016)4 of the Committee of Ministers to member States on the protection of journalism and safety of journalists and other media actors (13 April 2016); Recommendation CM/Rec(2024)2 of the Committee of Ministers to member States on countering the use of strategic lawsuits against public participation (SLAPPs) (5 April 2024); see also the Council of Europe Platform for the Protection of Journalism and Safety of Journalists and the Council of Europe “Journalists Matter” Campaign for the Safety of Journalists.
[117] Recommendation CM/Rec(2016)4 of the Committee of Ministers to member States on the protection of journalism and safety of journalists and other media actors (13 April 2016), in particular the guidelines concerning protection in contexts such as elections, public demonstrations and crisis situations.

2. Education, media and information literacy

178. Education and media and information literacy constitute a second key dimension of resilience and strengthening responses. These measures address the cognitive and behavioural aspects of FIMI by strengthening individuals' capacity to access, analyse, evaluate and contextualise information across different media and platforms[118].

179. Media and information literacy initiatives aim to enhance critical engagement with information rather than to promote specific viewpoints. They support understanding of how information is produced, distributed and amplified, including the role of algorithms, emotional framing and co-ordinated dissemination practices commonly used in manipulation campaigns[119].

180. Preventive approaches in this area extend beyond the identification of false information. They encompass media and information literacy aimed at creating awareness of as well as the capacity to detect and understand manipulative techniques and inauthentic behaviours. These may rely on partially true, decontextualised or selectively framed content, as well as tactics designed to exploit identity, fear or polarisation. Clear public communication and appropriately timed resilience campaigns can further support these efforts.

181. Education and literacy measures are typically long-term in nature and require continuity across formal education, non-formal learning and lifelong education. They should reach all segments of society, considering different needs and specific contexts, including media professionals and journalists. Their impact is cumulative and often difficult to measure in the short term. Over time, they strengthen individual autonomy, informed participation in public life, and the capacity to detect manipulation.

182. For such measures to be effective, they should be embedded in a coherent and sustained public policy framework. This includes structured multi-stakeholder engagement, regular assessment of media and information literacy levels, and evaluation of the impact of initiatives over time. Where appropriate, co-operation at international level may further support the exchange of experience and good practices[120].

3. Societal resilience, inclusion and trust

183. Resilience responses to FIMI also encompass broader efforts aimed at strengthening societal resilience, inclusion and trust in democratic institutions. FIMI frequently exploits existing social tensions, inequalities and experiences of marginalisation to amplify division and undermine social cohesion[121].

184. Inclusive societies characterised by equal participation, non-discrimination and trust in public institutions are generally less susceptible to manipulative interference. Where segments of society experience systematic exclusion or distrust, manipulative narratives are more likely to resonate and spread.

185. Resilience approaches in this area do not seek to securitise social policy or public debate. Rather, they recognise that democratic resilience depends on the effective enjoyment of human rights, social inclusion and the credibility of democratic governance. Measures addressing discrimination, polarisation and institutional trust therefore contribute significantly to limiting the impact of FIMI.

---

[118] Council of Europe, Steering Committee on Media and Information Society (CDMSI), National Media and Information Literacy (MIL) Strategies – Practical Steps and Indicators (2025), providing policy guidance on the development of national MIL strategies aimed at strengthening individuals' capacity to engage critically with information as a component of long-term democratic resilience.

[119] UNESCO, Media and Information Literacy: Policy and Strategy Guidelines, outlining approaches to understanding information production, distribution and amplification processes in contemporary information environments.

[120] Council of Europe, Steering Committee on Media and Information Society (CDMSI), National Media and Information Literacy (MIL) Strategies – Practical Steps and Indicators (CDMSI(2025)09, adopted on 4 December 2025); and Resisting disinformation: 10 building blocks to strengthen information integrity (CDMSI(2025)17-rev, adopted on 4 December 2025).

[121] Recommendation CM/Rec(2022)16 of the Committee of Ministers to member States on combating hate speech, recognising the exploitation of social divisions and discrimination as vectors for harmful information practices (20 May 2022).

186. Societal resilience is closely linked to the protection of groups that are disproportionately harmed by manipulation campaigns, including women, minorities and young people. Efforts to counter stigmatisation, harassment and identity-based manipulation strengthen the overall resilience of the information environment by reducing the entry points through which interference operates.

C. Governance and regulatory responses

187. Governance and regulatory responses organise and regulate relevant democratic and information environments. Their purpose is to foster information integrity, and specifically trust, transparency and resilience and reducing vulnerabilities to manipulation and interference.

188. These responses address systemic risks and concrete vulnerabilities within the information environment without resorting to criminal sanctions. They typically involve the use of regulatory, administrative or governance tools that can be applied in a targeted and proportionate manner, in accordance with applicable legal frameworks.

189. Regulatory responses may operate at different stages of the information lifecycle. They may address dissemination, amplification or monetisation of content, as well as transparency of actors and processes.

190. Their common objective is to reduce systemic exposure to manipulation while preserving open debate and lawful expression.

1. Platform-related measures

191. Platform-related measures form an important component of governance and regulatory responses in contemporary information environments. Digital platforms play a central role in the distribution, amplification and visibility of information, and their design and governance choices can influence the reach and impact of manipulative activities.

192. Measures in this area increasingly focus on systemic risks affecting the functioning of the information environment and democratic processes rather than on individual items of content[122]. They may include obligations relating to risk assessment, transparency of content curation and recommendation systems, detection of co-ordinated inauthentic behaviour, and the disruption of artificial amplification practices. They may also include transparency and responsibility measures relating to false or misleading AI-generated content[123].

193. Platform-related regulatory responses are generally framed in a content-neutral manner. By concentrating on behaviours, processes and systemic effects, they seek to limit manipulation without requiring public authorities to assess the truthfulness or legitimacy of specific viewpoints. Notification mechanisms, including notifications by users and, where applicable, trusted flaggers[124], may support the identification of co-ordinated manipulation while reinforcing freedom of expression, participation and democratic debate.

194. The effectiveness and legitimacy of such measures depend on the existence of clear legal bases, independent oversight and procedural safeguards. Proportionality, transparency and access to redress are essential to ensure that regulatory measures do not result in undue restrictions on freedom of expression or arbitrary interference with lawful activity.

195. Where appropriate, regulatory approaches may also contribute to limiting the ability of co-ordinated networks engaged in manipulative practices to operate effectively, without relying on criminal law.

---

[122] [draft] Recommendation of the Committee of Ministers to member States on online safety and empowerment of content creators.
[123] Regulation (EU) 2022/2065 on a Single Market for Digital Services (Digital Services Act), in particular Articles 34 and 35, introducing obligations for very large online platforms to assess and mitigate systemic risks affecting civic discourse and electoral processes.
[124] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services (Digital Services Act), Article 22, which provides for the designation by Digital Services Co-ordinators of entities with demonstrated expertise and independence to submit notices of illegal content, whose notifications are to be treated with priority by online platforms.

196. Transparency obligations may extend to the identification and labelling of synthetically generated or AI-assisted content, particularly where such content may mislead users as to its origin or authenticity. Enhanced transparency in relation to political advertising and algorithmic amplification may further contribute to safeguarding the integrity of democratic processes, provided that such measures remain lawful, necessary and proportionate.

2. Transparency and integrity measures

197. Transparency and integrity measures constitute a further dimension of governance and regulatory responses. These measures aim to reduce covert influence by increasing visibility over the sources, funding and sponsorship of information and political communication.

198. Such measures may apply to a range of actors and contexts, including political advertising, issue-based campaigning, lobbying activities and media ownership structures. By clarifying who is behind particular messages or campaigns, transparency mechanisms seek to enable informed public debate and accountability[125].

199. Integrity-related measures may also address conflicts of interest, undue influence or the misuse of resources in ways that facilitate manipulation. These responses are typically preventive in intent but operate at the point where specific risks have already been identified.

200. As with other mitigation responses, transparency and integrity measures must be carefully calibrated. Overly broad or poorly defined obligations may have chilling effects on lawful expression or association, while insufficient safeguards may undermine trust in their application.

3. Safeguards and oversight

201. A defining characteristic of governance and regulatory responses is the need for robust safeguards and oversight mechanisms. This approach is consistent with existing Council of Europe standards concerning the roles and responsibilities of internet intermediaries and platform governance, which emphasise public oversight of systemic risk management processes and safeguards for freedom of expression[126]. Given their potential impact on the information environment and on human rights, such responses require clear allocation of responsibilities and effective accountability frameworks.

202. Independent oversight bodies play a central role in ensuring that mitigation measures are applied consistently and proportionately. Judicial review, procedural guarantees and access to remedies contribute to the legitimacy and sustainability of regulatory interventions.

203. Safeguards are particularly important where mitigation responses involve co-operation with private actors or rely on automated systems. Human oversight, transparency of decision-making processes and mechanisms for contesting decisions help prevent error, bias or abuse.

204. Certain regulatory or administrative responses may include restrictions targeting specific media outlets or distribution channels, including within the framework of sanctions regimes or audiovisual regulation. These measures may have significant implications for media freedom and freedom of expression. Where they are applied, they require a clear legal basis, strict proportionality, effective judicial review and robust safeguards to prevent arbitrary or politically motivated interference[127].

---

[125] Regulation (EU) 2024/900 on the transparency and targeting of political advertising, establishing disclosure and transparency requirements applicable to political advertising and related communication activities.

[126] Recommendation CM/Rec(2018)2 of the Committee of Ministers to member States on the roles and responsibilities of internet intermediaries (7 March 2018); Draft Recommendation of the Committee of Ministers to member States on online safety and empowerment of content creators.

[127] Relevant opinions and guidance adopted within the Council of Europe framework concerning restrictions affecting media outlets and freedom of expression, as well as documented practice under sanctions and audiovisual regulatory regimes in member States.

D. Detection and analytical responses

205. Detection and analytical responses focus on identifying, analysing and understanding FIMI activities. They aim to generate visibility over the information environment and to support informed and timely responses. These responses identify patterns of co-ordinated activity, assess their scope and potential impact, and support timely understanding of evolving tactics. These functions may be carried out by public authorities as well as by independent researchers, civil society organisations and other relevant actors.

206. They combine technical analysis, contextual assessment and strategic interpretation. They rely on the collection and examination of signals[128] across media, platforms and communication channels, often using open-source information, data analysis and qualitative assessment.

1. Monitoring, analysis and early warning

207. Monitoring and analysis are central components of situational awareness in relation to FIMI. These activities seek to identify co-ordinated patterns of information manipulation, including artificial amplification, inauthentic behaviour and the concealment of origin or intent.

208. Analytical approaches in this area focus on behaviours and dissemination patterns rather than on the truthfulness of individual items of content. By concentrating on patterns of co-ordination, amplification and concealment, this enables the identification of manipulative practices while reducing the risk of content-based interference with lawful expression[129].

209. Early warning mechanisms form an important aspect of detection-oriented responses. By identifying emerging campaigns or shifts in narratives at an early stage, they enable timely awareness and co-ordination among relevant actors.

210. In periods of heightened risk, early warning mechanisms may also support crisis-response arrangements[130]. They can facilitate rapid information-sharing between competent authorities and relevant platforms or other stakeholders.

211. Detection and early warning activities must operate with clear mandates and safeguards. Transparency of methodology, proportionality in data use and respect for privacy and freedom of expression are essential to maintain legitimacy and public trust in such mechanisms. They must not entail generalised or indiscriminate monitoring of online communications. Any monitoring must remain strictly limited to what is necessary and proportionate in a democratic society.

2. Analytical capacities and information-sharing mechanisms

212. Detection and situational awareness functions rely on appropriate analytical capacities, including technical expertise, data analysis, contextual assessment and strategic interpretation. They require the ability to identify and characterise interference activities, assess risks to democratic processes and communicate findings in a timely and accessible manner.

213. These analytical activities must operate within clear legal mandates and safeguards. Clear boundaries must be maintained between analytical functions, regulatory responsibilities and law enforcement activities in order to preserve proportionality, protect fundamental rights and maintain public trust.

E. Accountability, enforcement and disruption responses

214. Accountability, enforcement and disruption responses address situations in which FIMI-related conduct give rise to legal or regulatory consequences. They seek to establish responsibility, to apply appropriate consequences where legal thresholds are met, and to limit the operational capacity of co-ordinated manipulation networks.

---

[128] European External Action Service, EEAS Reports on Foreign Information Manipulation and Interference (2023–2025), referring to observable indicators of co-ordinated activity, such as patterns of amplification, synchronised dissemination, network behaviour or recurring narrative structures.
[129] European External Action Service, Information Integrity and Countering Foreign Information Manipulation and Interference (FIMI), describing an analytical framework focusing on co-ordinated behaviour and dissemination patterns rather than content assessment.
[130] Regulation (EU) 2022/2065 on a Single Market for Digital Services (Digital Services Act), in particular Article 36 and Article 48, providing for crisis-response mechanisms and structured co-operation, including the designation of contact points and rapid information-sharing arrangements with very large online platforms and search engines.

215. These responses may take different forms depending on the nature and seriousness of the conduct concerned. They may include administrative and regulatory measures, restrictive or targeted measures, financial investigation and anti-corruption measures and, where appropriate, criminal law measures[131].

1. Administrative and regulatory measures

216. Administrative and regulatory measures are triggered by identified conduct or failures to comply with applicable obligations. Unlike governance responses, which primarily address systemic risks and vulnerabilities within the information environment, these measures concern case-specific enforcement and may result in corrective orders or sanctions[132].

217. These measures may include fines, compliance orders, corrective obligations, suspension of specific services or functionalities, or other sanctions provided for under domestic law. They are applied by competent supervisory or regulatory authorities following established procedures and subject to safeguards ensuring legality, proportionality and due process[133].

2. Restrictive and targeted measures

218. Restrictive and targeted measures aim to limit the operational capacity of actors involved in FIMI-related activities. They are directed at specific individuals, entities or networks and may include asset freezes, prohibitions on certain transactions, travel bans or other restrictive measures provided for under domestic or international sanctions regimes.

219. The adoption of restrictive and targeted measures must be grounded in a clear legal basis and comply with applicable human rights standards. They should be subject to appropriate procedural safeguards, including transparency of designation criteria, access to review or appeal mechanisms and periodic reassessment where relevant.

220. In certain contexts, measures affecting media outlets have been adopted within sanction regimes or audiovisual frameworks. Given their implications for media freedom, these measures require a clear legal basis, strict proportionality and effective judicial review under Article 10 of the Convention.

221. Public attribution and exposure of co-ordinated manipulation activities may also form part of disruption strategies, reducing their credibility, limiting amplification and increasing accountability.

222. Their purpose is to prevent further harmful activity and to protect the integrity of democratic processes, not to restrict lawful expression.

3. Financial investigation and anti-corruption measures

223. Financial investigation and anti-corruption measures aim to identify, trace and, where appropriate, interrupt financial flows that enable FIMI-related activities. By addressing the economic structures, they seek to reduce the sustainability and reach of FIMI networks.

224. These measures may include parallel financial investigations, asset tracing, enhanced transparency obligations and the application of anti-money laundering or anti-corruption frameworks. This includes the tracing of transactions involving digital financial instruments such as crypto-assets, in accordance with domestic and international law.

225. Financial disruption, including the tracing and freezing of assets, the interruption of funding streams and the exposure of financial networks, may significantly reduce the sustainability and reach of co-ordinated FIMI operations.

226. In some cases, actors involved in FIMI-related activities may be motivated by financial incentives. Addressing the financial flows used to fund such activities or remunerate individuals involved may therefore play an important role in disrupting FIMI operations and networks. This may include enhanced financial

---

[131] The criminal law aspects of these phenomena are examined in greater detail in Chapter 5.
[132] Regulation (EU) 2022/2065 (Digital Services Act), notably Articles 34–35 on systemic risk assessment and mitigation, and Article 52 on penalties
[133] Regulation (EU) 2022/2065 (Digital Services Act), in particular Articles 52–54 on penalties and enforcement mechanisms

investigations and co-ordination between competent authorities, particularly where transactions involve digital financial instruments such as crypto-assets.

4. Criminal law measures

227. Criminal law measures may be applicable where FIMI-related activities meet the thresholds of existing offences under domestic law. These measures are subject to strict legality, necessity and proportionality requirements. Their scope, conditions and safeguards are examined in Chapter 5.

F. Co-operation and co-ordination responses

228. Co-operation and co-ordination responses play a central role in addressing FIMI. Given the cross-border, multi-actor and often simultaneous nature of information manipulation and interference, isolated or purely domestic responses are frequently insufficient. This category of responses focuses on enabling alignment, information-sharing and joint action across institutions and jurisdictions.

229. These responses do not primarily introduce new substantive measures. They connect existing capacities, reduce fragmentation and improve the timeliness and coherence of responses. They operate as enabling mechanisms that enhance the effectiveness of resilience, governance, detection and accountability responses.

230. This layer is particularly relevant where FIMI activities affect several States or information environments simultaneously, or where the actors, infrastructures or impacts involved extend beyond national borders. In such contexts, co-ordination contributes to situational awareness, consistency of responses and mutual support.

1. National co-ordination mechanisms

231. At national level, co-ordination mechanisms aim to bring together relevant public authorities and stakeholders involved in addressing FIMI. These may include bodies responsible for media regulation, electoral integrity, cybersecurity, strategic communication, foreign policy, and the protection of fundamental rights.

232. National co-ordination responses typically seek to clarify roles and responsibilities, facilitate information-sharing and support coherent decision-making. By improving internal co-ordination, they reduce the risk of fragmented or contradictory responses to FIMI activities.

233. Effective national co-ordination often requires structured interfaces between public authorities and non-State actors, including independent media, civil society organisations and academic experts. Such co-operation can enhance analytical capacity and responsiveness, while preserving the independence of participating actors.

234. Public authorities may not always be perceived as the most trusted voice in public communication. Effective co-ordination should therefore involve independent and credible actors, while fully respecting media freedom and institutional responsibilities.

235. Various institutional models have emerged across member States to strengthen national responses to FIMI. These include specialised executive units focused on the detection of foreign digital interference, independent agencies dedicated to psychological or societal resilience, and strategic communication structures tasked with co-ordinating analysis and public communication.

236. France, for instance, has established VIGINUM as a dedicated service for the detection of foreign digital interference. Sweden has created the Psychological Defence Agency with a broader mandate on resilience against information influence. The Republic of Moldova has developed strategic communication structures aimed at co-ordinating institutional responses to information manipulation. These models reflect differing constitutional traditions, threat perceptions and administrative arrangements. Poland has also established dedicated governmental structures tasked with monitoring, analysing and co-ordinating responses to foreign information manipulation within the information space.

2. International and cross-border co-operation

237. International and cross-border co-operation responses address the transnational dimension of FIMI. They facilitate the exchange of information, analysis and alerts between States and relevant international partners, including through early warning mechanisms, and support a shared understanding of emerging patterns and tactics.

238. Co-operation may take multiple forms, including bilateral exchanges, regional co-ordination frameworks and participation in multilateral platforms. It may also involve technical assistance, joint training initiatives, peer-to-peer exchanges and the sharing of good practices between neighbouring or partner States, including in preparation for electoral processes. These mechanisms aim to reduce duplication, improve comparability of analysis and enable co-ordinated responses where appropriate. In certain contexts, co-operation may involve expedited or structured channels for information-sharing, where appropriate, the designation of contact points to facilitate timely co-ordination, in accordance with applicable legal safeguards.

239. International co-operation responses are typically non-binding and rely on mutual trust, voluntary participation and political commitment. Their flexibility allows adaptation to evolving threats but may also result in uneven levels of engagement or capacity across participating States.

240. As with other categories of responses, co-operation mechanisms must operate within clear legal and human rights boundaries. Respect for national legal frameworks, data protection requirements and freedom of expression standards is essential to ensure legitimacy and sustainability of cross-border co-ordination.

241. Civil society organisations, independent researchers, journalists, academic institutions and other relevant non-State actors also play an important role in analysing manipulation patterns, sharing methodologies and strengthening resilience across borders.

CHAPTER 5 – ACCOUNTABILITY, CRIMINAL LAW AND HUMAN RIGHTS SAFEGUARDS

242. This chapter examines the potential role of criminal law in addressing conduct related to foreign information manipulation and interference (FIMI), along with the applicable human rights safeguards. It reviews the general conditions under which criminalisation may be warranted and the existing criminal law frameworks relevant to certain FIMI-related conduct.

A. General conditions for criminalisation

243. Criminal law may play a specific role in responses to FIMI and should be treated as a measure of last resort, used only where resilience, governance or other less intrusive measures are clearly insufficient. Its use raises sensitive concerns particularly for democratic States, given the direct impact of criminal sanctions on the enjoyment and exercise of human rights and the rule of law.

244. Any criminal law response must comply strictly with the principle of legality, requiring offences to be clearly defined and foreseeable. Vague or open-ended formulations risk legal uncertainty and may lead to arbitrary or disproportionate enforcement, especially in politically sensitive contexts.

245. Criminalisation should therefore be limited to conduct that meets a high threshold of seriousness. Only the most harmful and severe forms of FIMI-related behaviour, capable of causing serious damage to democratic processes or fundamental rights, can justify the use of criminal law.

246. A further core requirement concerns the subjective elements, including intent and knowledge. Liability should be based on clear evidence that the actor was aware of the nature of the conduct and its harmful effects and acted covertly and with the intention to manipulate information, interfere and cause serious harm.

247. Attribution and evidentiary challenges are particularly acute in FIMI cases. Linking conduct to identifiable individuals or entities, often operating across borders through covert means, raises complex questions of proof and due process that must be addressed.

248. Criminal law measures must maintain a clear distinction vis-à-vis lawful activity. Legitimate expression, political debate, advocacy and dissent must remain fully protected. Any criminal law framework must include robust safeguards to ensure that responses to FIMI do not encroach upon lawful democratic participation or chill freedom of expression[134], in particular of the media, journalists and other public watchdogs.

249. According to the jurisprudence of the Court, freedom of expression guaranteed by Article 10 of the Convention is applicable not only to “information” or “ideas” that are favourably received or regarded as inoffensive or as a matter of indifference, but also to those that offend, shock or disturb[135]. The Court has repeatedly upheld the right to impart, in good faith, information on matters of public interest, even where this involved damaging statements about private individuals[136]. There is little scope under Article 10, paragraph 2 of the Convention for restrictions on political speech or on the debate of questions of public interest[137]. Appropriate safeguards to protect against possible abuse of criminal law provisions in a political context must be in place.

250. An additional benefit of identifying minimum common denominators would be that they could provide a basis for co-operation among States despite differences in legal traditions, criminalisation thresholds and enforcement models.

251. Finally, any possible framework must respect national legal systems and the principle of subsidiarity. The objective is not to harmonise criminal law structures or impose uniform offences, but to offer shared reference points that can be adapted to diverse constitutional and criminal-law traditions.

B. Human rights principles and obligations in relation to criminalisation

252. When a State takes measures to guarantee the stability and effectiveness of a democratic system which result in interference with individual rights, it must ensure that a balance is achieved between the defence of democratic society and protecting individual rights[138].

253. Obliging individuals or organisations to disclose personal information, or affecting their capacity to express themselves freely and/or to associate with individuals/entities of their choice, may engage different provisions of the Convention, including the right to respect for private and family life (Article 8), freedom of expression (Article 10), freedom of thought, conscience and religion (Article 9 in conjunction with Article 10), and/or the right to freedom of assembly and association (Article 11, alone or in conjunction with Article 10). These measures may also engage Article 14 of the Convention (prohibition of discrimination).

254. These considerations must also be understood in light of States’ obligations under the Convention. States have both negative obligations to avoid undue interference with the exercise of the rights it guarantees and positive obligations, in accordance with the Court’s jurisprudence, to safeguard those rights when they are threatened, including in the context of foreign interference. Article 17 further states that Convention rights cannot be relied upon to justify activities aimed at undermining those same rights. Convention rights may regularly be restricted only if the three conditions of legality, legitimacy and necessity in a democratic society set out in the relevant Convention provisions are met cumulatively. The condition of legality is met, when the restriction is prescribed by law – i.e. it has a clear, precise and foreseeable legal basis, enabling individuals/organisations to regulate their conduct and foresee the consequences of their actions. To meet the second condition, restrictions must pursue one of the legitimate aims laid down by the relevant provision of the Convention. To meet the third condition, restrictions must be responded to a pressing social need to achieve the legitimate aim and must be proportionate to that aim.

---

[134] The European Court of Human Rights has found that even fairly light criminal measures (a fine or even a conviction without any sanction) have the potential of “discouraging open discussion of matters of public concern”; *Thorgeir Thorgeirson v. Iceland*, no. 13778/88, judgment of 25 June 1992; *Nikula v. Finland*, no. 31611/96, judgment of 21 March 2002, para. 54.

[135] European Court of Human Rights, *Janowski v. Poland*, no. 25716/94, judgment of 21 January 1999, para. 30, and cited case law; *Kita v. Poland*, cited above, para. 36.

[136] European Court of Human Rights, *Kita v. Poland*, cited above, para. 37.

[137] European Court of Human Rights, *Brzeziński v. Poland*, cited above, para. 53; *Feldek v. Slovakia*, no. 29032/95, judgment 12 October 2001, para. 74.

[138] European Court of Human Rights, *Bradshaw and Others v. the United Kingdom*, cited above, paras. 114 and 115.

255. In matters of freedom of expression, States must exercise restraint in using criminal proceedings and in imposing custodial sentences. Criminal conviction constitutes one of the most serious forms of interference with freedom of expression, in particular when imposed in the context of political debate; recourse to it will be justified only when other fundamental rights are seriously infringed upon[139].

256. Measures to tackle election interference engage the right to free elections under Article 3 of Protocol No.1 to the Convention. To ensure compliance with this provision, such measures must be lawful, pursue a legitimate aim, and be proportionate. They may also interfere with Articles 10 and 11 of the Convention.

257. Criminalisation of FIMI-related conduct engages Article 5 (right to liberty and security), Article 6 (right to a fair trial) and possibly Article 7 (no punishment without law) of the Convention. To meet the conditions of lawfulness under Article 5, criminal law measures must be in conformity with the principles of the rule of law, legal certainty, proportionality and protection against arbitrariness. When criminal charges are brought against an individual, the rights and procedural guarantees of Article 6 of the Convention must be respected.

258. It should be noted that Council of Europe treaties concerned with the establishment and application of criminal offences, provide explicit safeguards for freedom of expression, freedom of association and freedom of religion in compliance with the Convention[140].

259. Criminal legislation aimed at countering the risk of foreign election interference arising from co-ordinated and intentional information manipulation, including through the dissemination of disinformation[141] and the running of influence campaigns, is likely to interfere with the right to freedom of expression, notably the right to receive and impart information under Article 10 of the Convention. Legislation that does not lay down clear and precise definitions of the relevant conduct such as “disinformation” or “false and misleading information” and provide precise criteria for assessing intent and the seriousness of harm that it may cause to the public risks failing the Article 10 requirements on legal certainty[142]. The use of overly broad concepts risks capturing legitimate expression of opinions or quotations of others’ opinions (e.g. by journalists). Council of Europe standards do not support broad criminalisation of disinformation as such. Criminal law measures in this area, if acceptable at all, must remain exceptional and used only as a measure of last resort. It must be limited to clearly defined conduct involving intent and serious harm, in line with Article 10 of the Convention, including as regards avoidance of a chilling effect on freedom of expression[143].

260. Criminalising certain forms of co-ordinated and intentional information manipulation may be disproportionate where other remedies are available and effective. Alternative responses may include counter-speech, including public refutation of false claims, encouraging individuals and organisations to post corrections of information, or introducing social media obligations to remove illegal content promptly upon complaint.

261. During elections, recourse to criminal law in relation to co-ordinated and intentional information manipulation risks engaging a State’s obligations under Article 3 of Protocol No. 1 to the Convention to organise elections under conditions which will not thwart the free expression of the people in the choice of legislature. Member States must maintain the integrity and effectiveness of an electoral procedure aimed at identifying the will of the people through universal suffrage. They must also ensure the circulation of political opinions and information in a period preceding an election. In this context, the need to safeguard freedom of expression is heightened. Equal opportunity must be afforded to candidates. A State has the duty to adopt positive measures to secure pluralism[144].

---

[139] European Court of Human Rights, *Rouillan v. France*, no 28000/19, judgment of 23 June 2022, para. 74 (and cited case-law).
[140] E.g. Council of Europe Convention on the Prevention of Terrorism, Article 12, or its Additional Protocol, Article 8.
[141] See Chapter 2, section D, for the analytical definition of disinformation used in this study, including reference to co-ordinated and inauthentic behaviour.
[142] In this connection, the Court considers that a distinction needs to be made between statements of fact, whose existence can be demonstrated, and value judgments. The requirement to prove the truth of a value judgment is impossible to fulfil and infringes freedom of opinion itself, which is a fundamental part of the right secured by Article 10 of the Convention. The classification of a statement as a fact or as a value judgment is a matter which in the first place falls within the margin of appreciation of the national authorities. However, even where a statement amounts to a value judgment, the proportionality of an interference may depend on whether there exists a sufficient factual basis to support it, failing which the statement may be excessive: see *Kita v. Poland*, no. 57659/00, judgment of 8 July 2008, para. 40, and *Jerusalem v. Austria*, no. 26958/95, judgment of 27 February 2001, para. 43.
[143] European Court of Human Rights, *Nikula v. Finland*, no. 31611/96, judgment of 21 March 2002, para. 54.
[144] European Court of Human Rights, *Bradshaw and Others v. the United Kingdom*, cited above, paras. 118–120 and 131.

C. Criminal law frameworks relevant to FIMI-related conduct

1. Existing categories of criminal conduct intersecting with FIMI

262. The paragraphs below describe categories of conduct already addressed in the criminal law of several member States that may intersect with FIMI-related conduct. They do not suggest the creation of new offences.

263. Certain forms of conduct already addressed under existing criminal law frameworks may be relevant in FIMI-related contexts, provided that strict legal thresholds and safeguards are met. These offences do not target FIMI as such but may apply where FIMI-related conduct overlaps with clearly criminal conduct.

264. Espionage-related conduct may be relevant in certain FIMI-related contexts. This is for example the case where covertly obtained information is subsequently used as part of FIMI activities.

265. Sabotage, including cyber-enabled sabotage, covers the intentional disruption or damage of systems, infrastructure or democratic processes. Where such acts are linked to foreign interference, they may intersect with FIMI-related conduct.

266. Foreign interference offences, where they exist in domestic law, capture deliberate actions carried out by, or on behalf of, foreign actors with the aim of undermining democratic institutions, public authorities, or societal cohesion. They are not designed to criminalise FIMI as such but may apply where FIMI-related conduct overlaps with such offences.

267. Electoral interference offences address conduct targeting voting processes, political campaigns or political financing. These provisions are particularly relevant where manipulation is designed to distort electoral outcomes or undermine trust in democratic legitimacy.

268. In several member States, FIMI-related conduct is not treated as a separate offence. They may instead fall under existing offences against the security or interests of the State when they form part of malicious, systematic and co-ordinated influence operations conducted on behalf of, or under the direction or control of, a foreign actor. Criminal liability requires clearly established elements, including awareness of the nature of the conduct and intent to cause serious harm to a specifically identified public interest. Broad or content-based criminalisation may carry significant risks for freedom of expression.

269. Finally, speech or incitement provisions may become relevant where such expression is deliberately instrumentalised as part of FIMI operations, particularly where it targets specific groups and contributes to broader strategies of destabilisation, exclusion, or democratic erosion[145].

270. In addition, some member States provide that violations of sanctions regimes adopted in response to foreign interference or hybrid threats may constitute criminal offences rather than administrative infringements. Such approaches reflect the gravity of breaches linked to foreign interference and their potential implications for national security.

2. Examples of existing criminalisation in Council of Europe member States

271. A limited number of States have introduced standalone offences specifically addressing foreign interference. These provisions explicitly criminalise certain forms of foreign-linked interference, reflecting a legislative choice to name and target the foreign element more directly[146].

272. More commonly, States rely on the application of existing offences to address FIMI-related conduct, where the factual elements of such offences are met. Criminal law responses may operate through

[145] Article 20 of the International Covenant on Civil and Political Rights requires States to prohibit propaganda for war and advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence.
[146] For example, Norway introduced in 2024 criminal provisions (Sections 130 and 130a of its Criminal Code) addressing influence from foreign intelligence actors. Other examples include Estonia, Latvia and Lithuania.

established security-related or public order categories, which are applied to new interference patterns when the legal thresholds are satisfied[147].

273. Some legal systems also provide for electoral interference and foreign funding offences, which may become relevant where conduct targets voting processes, political campaigns or political financing, and meets the applicable legal thresholds[148]. Examples mentioned in the comparative inputs include France, Italy and Spain.

274. In addition, cybercrime-related offences may become relevant to FIMI, especially where information manipulation is enabled by hacking, unlawful access, data interference or disruption of digital services, provided that the applicable legal elements are satisfied[149].

275. Another recurring legislative technique provides for aggravating circumstances linked to foreign involvement, allowing courts to increase penalties where an offence is committed on behalf of, or under the direction or control of, a foreign actor[150].

276. Some member States have introduced more specific criminal provisions targeting intentional influence on public authorities or democratic decision-making. These provisions may apply where the conduct affects essential State interests or the democratic and constitutional order. For example, Belgium has introduced criminal provisions targeting the transmission of false or misleading information to public authorities with the intention to affect the democratic order. It also criminalises intentional influence on democratic decision-making for the benefit of a foreign State or a foreign-controlled entity, through illegal methods.

3. Adjustment of existing criminal law concepts

277. In some member States, existing offences have been interpreted or adapted to encompass FIMI-related elements within established categories of criminal law. This approach enables harmful conduct to be addressed without creating entirely new categories of offences.

278. In this context, the use of aggravating circumstances can be considered relevant. Elements such as foreign involvement, co-ordination, or the pursuit of a strategic objective can justify more severe penalties while preserving the core structure of existing offences.

279. This method also supports the avoidance of duplication. Where adequate legal tools already exist, adapting them is often preferable to creating overlapping offences that may create confusion or enforcement challenges.

4. Criminal responsibility of legal persons

280. The potential role of legal persons also requires careful consideration. FIMI-related conduct may involve companies, organisations or other intermediaries. While FIMI is characterised by a foreign nexus, the actors involved may include both State and non-State entities, as well as their proxies. This section therefore examines the possible criminal responsibility of legal persons in this context.

281. This is particularly relevant in relation to platform-related involvement, where services or infrastructures may be used to amplify, facilitate or monetise manipulative campaigns without necessarily being at the origin of them. Any legal response in this area must clearly distinguish between intentional participation and mere passive or technical involvement.

282. Approaches in this field should remain compatible with Council of Europe standards, notably existing principles on corporate liability, freedom of expression and intermediary responsibility. This implies avoiding automatic or strict liability models that could undermine legal certainty or innovation.

[147] Examples include France, Germany and the Netherlands.
[148] Examples include France, Italy and Spain.
[149] Examples include Romania and the United Kingdom.
[150] Examples include France, Germany, the Netherlands, Norway, Sweden and the United Kingdom.

283. Measures involving legal persons must respect proportionality, ensure due process, and provide effective remedies, particularly given the indirect and complex role that organisations may play in information ecosystems.

5. Aiding and abetting, proxies and indirect participation

284. Attention should also be given to forms of assistance that may support FIMI-related conduct. This can include financial, technical or logistical support that enables or sustains influence operations without directly engaging in the core manipulative acts.

285. The use of proxies is a recurrent feature of FIMI operations, with intermediaries, front organisations or service providers acting on behalf of foreign actors in order to conceal origin, intent or co-ordination. Such arrangements complicate attribution and blur the lines between direct and indirect involvement.

286. Recognising these dynamics is relevant for capturing indirect contributions to FIMI-related offences, while maintaining clear thresholds for intent, knowledge and material contribution. Any criminalisation should therefore be narrowly framed and supported by strong evidentiary requirements to avoid overreach.

6. International co-operation and mutual legal assistance in criminal matters

287. The cross-border nature of FIMI operations is a central challenge for any legal response, as relevant activities often span multiple jurisdictions and involve actors, infrastructure and victims located in different States. This creates significant difficulties for evidence gathering, including access to data held abroad, attribution of conduct and identification of responsible actors.

288. Effective responses therefore require international co-operation and, where appropriate, mutual legal assistance between States. Existing Council of Europe instruments provide important foundations in this regard, in particular the Convention on Cybercrime, which facilitates co-operation on electronic evidence, and the Convention on Mutual Legal Assistance in Criminal Matters and its additional Protocols, which supports cross-border investigative and procedural co-operation. These tools can play a supporting role in addressing FIMI-related conduct, even though they were not designed specifically for this purpose.

D. Human rights issues in relation to certain other counter-FIMI measures

289. This section outlines the human rights issues raised by certain legal measures adopted across member States to address FIMI. The relevant principles and obligations under the Convention, discussed earlier in this report, also apply in this context.

290. Measures affecting political participation, party financing or electoral processes may engage the right to free elections under Article 3 of Protocol No. 1 to the Convention. Not every regulatory measure amounts to an interference with this right. While States enjoy a margin of appreciation in regulating electoral matters, any interference must be justified, pursue a legitimate aim and remain proportionate.

1. Prohibition of foreign financing of political parties and candidates

291. The prohibition of donations to political parties and electoral campaigns from foreign donors or States would, in principle, be in line with Council of Europe standards. Some member States have introduced legislation prohibiting loans to political parties from any legal entity other than political parties and banks in the European Economic Area (EEA). Other measures include reserving third-party campaign spending to domestic based groups or individuals, or to registered overseas electors. One member State prohibits, in addition to political parties, candidates from receiving foreign support and applies criminal penalties for doing so[151].

[151] Hungary, Criminal Code Article 350/A “Illegal influence of the will of voters”.

292. To be justified under Article 11 of the Convention, a prohibition on foreign financing of political parties and candidates must meet the condition of necessity in a democratic society. This may be the case when such financing is used to pursue aims not compatible with the constitution and the laws of the respective member State. It may also be justified where it undermines the fairness or integrity of political competition, distorts the electoral process, threatens national territorial integrity, or inhibits responsive democratic development. To establish whether a prohibition is justified, each case must be assessed in light of the overall legislative framework governing party financing and the State's international obligations, including, where applicable, its obligations as a member of the EU[152].

293. Where legal prohibitions do not put in place safeguards to permit donations from nationals of the State concerned living abroad, there is a risk of unjustified interference with their rights under Article 11 of the Convention. The absence of exemptions to prohibitions for legitimate co-operation of parties active at international level may infringe their right to association under Article 11 of the Convention[153].

294. Prohibiting candidates from receiving and using foreign funding interferes with the right to stand for election under Article 3 of Protocol No. 1 to the Convention. When the prohibition is couched in broad terms, capturing funding from individuals or political parties, or funding received outside electoral processes, it potentially infringes on the free association of political forces and may fail the necessity/proportionality test[154].

2. Exclusion of a party from elections

295. The disqualification of a party from elections on grounds of using undeclared foreign funds interferes with Article 3 of Protocol No. 1 to the Convention. Although, such measure may pursue the legitimate aim of rule of law and the protection of democracy's functioning, it risks violating the right to free elections if it is not based on sufficient and relevant evidence of illegal activity and is not accompanied by sufficient procedural safeguards against arbitrariness[155].

3. Sanctions relating to foreign influence registration obligations: examples and approaches

296. Legislation introducing obligations to register foreign influence arrangements, e.g. political influence activities, carried out at the direction of a foreign power, such as communications to senior decision makers, election candidates, MPs and senior civil servants, may be accompanied by criminal sanctions for failure to register or acting without registration. Registration obligations may extend to communication to the public of funds collection under the direction or control of a foreign entity and with the aim of promoting the latter's interest[156].

297. Lobbying organisations may be required to register with relevant authorities and publicly disclose financial statements, which should also apply mutatis mutandis to lobbying natural or legal persons who act under the direction or control of a foreign principal. Sanctions may be envisaged for breaches of reporting obligations.

298. Transparency obligations imposed on individuals and entities may restrict their freedom of association (Article 11 read in conjunction with Article 10 of the Convention). However, concepts such as "foreign power", "foreign principal" or "agent of foreign principal" should be avoided due to their potential stigmatising effect, as well as the difficulty of defining them. If they are used and not defined with sufficient precision in law, this impacts foreseeability and legal certainty and there may be a risk of arbitrary

---

[152] European Commission for Democracy through Law (Venice Commission), Opinion on the Prohibition of Financial Contributions to Political Parties from Foreign Sources, CDL-AD(2006)014, 31 March 2006.
[153] European Commission for Democracy through Law (Venice Commission) and OSCE/ODIHR, Joint Opinion on the Draft Law on Financing Political Activities of the Republic of Serbia, CDL-AD(2010)048, 17–18 December 2010; European Commission for Democracy through Law (Venice Commission) and OSCE/ODIHR, Joint Opinion on the Draft Act to Regulate the Formation, the Inner Structures, Functioning and Financing of Political Parties and Their Participation in Elections of Malta, CDL-AD(2014)035, 10-11 October 2014.
[154] European Commission for Democracy through Law (Venice Commission), Opinion on Act LXXXVIII of 2023 on the Protection of National Sovereignty (Hungary), CDL-AD(2024)001, 15–16 March 2024.
[155] European Court of Human Rights, *Political Party "Patria" and Others v. the Republic of Moldova*, nos. 5113/15 and others, judgment of 4 November 2020, paras. 32-38.
[156] Law no.2024-850, 25 July 2024 aiming to prevent foreign interference in France, Art. 18-16.

application of the law. Using the concept of "political activities" without a precise specification as to their purposes in relation to the aims of the legislation creates uncertainty for a wide range of legitimate civic or professional activities and risks criminalising them[157].

299. Designations of civil society organisations as "foreign agents" risk stigmatising and delegitimising civil society actors, media, and individuals, and having a chilling effect on freedom of expression (Article 10 of the Convention). Creating a new legal status as "foreign agents" risks restricting organisations' ability to carry out their activities, to participate in public life and, ultimately, may not be justified as necessary in a democratic society under Article 11 of the Convention[158]. The creation of separate registers for organisations, even if phrased in a neutral way, intrinsically conveys suspicion regarding foreign funding.

300. Criminalising all breaches of registration obligations, without any distinction as to their severity, fails to satisfy the conditions of necessity and proportionality under Article 11 of the Convention. This is particularly the case when other less intrusive enforcement tools (civil and administrative) are available and adequate for the purposes of the transparency regime. When criminal sanctions are set without considering the gravity and seriousness of the offence, notably whether there was any actual harm or malicious intent, they risk being applied in a disproportionate manner[159].

4. Prohibition on foreign funding of broadcasting

301. Legal measures which prohibit broadcasters' acceptance of funding from "foreign powers" risk being applied in an arbitrary manner and not being in line with the positive obligations under Article 10 of the Convention to guarantee media pluralism. When these measures are applied indiscriminately to all foreign individuals, organisations without exemptions for funding that supports legitimate journalistic activities, or for the ordinary commercial and philanthropic relationships of independent media they may not be justified as necessary and proportionate under Article 10 of the Convention[160].

5. Prohibition on foreign grants

302. Legislation prohibiting the acceptance by individuals or organisations of foreign grants for the implementation of societal projects without prior authorisation from the State risks interference with the right to freedom of association (Article 11 of the Convention). Such interference may amount to a violation when the legislation does not set out clear terms and precise criteria for authorisation assessment, is not substantiated with evidence of a pressing societal need, is not coupled with measures making sufficient domestic funding accessible, is not accompanied by safeguards against over-reaching enforcement measures or may lead to disproportionate sanctions.

CHAPTER 6 – STRUCTURAL CHALLENGES AND GAPS IN ADDRESSING FIMI

303. This chapter identifies, in line with the Committee's Terms of Reference, the structural challenges and gaps in the responses of member States to FIMI and related conduct. Building on the preceding analysis, it clarifies where limitations or inconsistencies persist, without prejudging the nature or scope of any possible future action at Council of Europe level.

---

[157] European Commission for Democracy through Law (Venice Commission), Opinion on the Law on the Registration of Foreign Agents, the Amendments to the Law on Grants and Other Laws Relating to "Foreign Influence" (Georgia), CDL-AD(2025)034, 9-10 October 2025, § 104.
[158] European Court of Human Rights, *Ecodefence and Others v. Russia*, no. 9988/13, judgment of 10 October 2022; *Kobaliya and Others v. Russia*, no. 39446/16, judgment of 22 January 2025.
[159] European Commission for Democracy through Law (Venice Commission), Urgent Opinion on the Law on Transparency of Foreign Influence (Georgia), CDL-PI(2024)013, 21 May 2024.
[160] European Commission for Democracy through Law (Venice Commission), Opinion on the Law on the Registration of Foreign Agents, the Amendments to the Law on Grants and Other Laws Relating to "Foreign Influence" (Georgia), CDL-AD(2025)034, 9-10 October 2025.

A. Divergent conceptual understanding of FIMI

304. A structural challenge identified in this study concerns differences in how FIMI is understood among Council of Europe member States. Although the term is increasingly used in policy and operational contexts and has notably been developed and operationalised, its scope and implications are not interpreted in a uniform manner across the Organisation.

305. As reflected in the discussions within the Committee, divergences persist in how FIMI is characterised, in the criteria used to identify relevant conduct and, in the thresholds applied when assessing seriousness. Member States may also differ in the scope of activities considered to fall within the concept. This includes diverging views on the relationship between FIMI and broader hybrid threats or other forms of co-ordinated interference, such as sabotage or criminal acts linked to foreign State interests.

306. While several forms of co-operation between member States are already in place and have proven their value, these differences may affect the comparability of national approaches and complicate cross-border co-operation in responding to FIMI.

B. Uneven institutional arrangements and operational capacities

307. Member States differ in the extent to which institutional arrangements and operational capacities are in place to address FIMI, including to understand, detect and respond to the phenomenon. While some States have established specialised units, strategic communication structures or national co-ordination mechanisms relating to the digital information environment, others may lack equivalent structures or operate with more fragmented or less formalised arrangements.

308. These differences may reflect variations in administrative organisation, allocation of resources, levels of exposure to FIMI activities or differing threat perceptions. They may also arise from the need to reconcile detection and response functions with other legal obligations, including data protection, privacy safeguards and constitutional guarantees.

309. As a result, the speed, coherence and consistency of national responses may vary. Institutional capacity is also closely linked to broader structural conditions: media literacy and awareness-raising measures, independent and pluralistic media environments, and transparent public institutions. These conditions are likewise developed to differing degrees among member States.

C. Fragmentation of policy and regulatory approaches

310. Responses to FIMI often span multiple policy domains, including democratic governance, media regulation, cybersecurity, foreign policy and criminal law. However, co-ordination across these areas is not always structured or systematic. In some contexts, responsibilities remain dispersed across institutions, and mechanisms for whole-of-government or whole-of-society co-ordination are still evolving.

311. This fragmentation may limit the coherence and consistency of national approaches. It may also complicate the alignment between policy initiatives and regulatory or legal measures, which are closely interconnected in practice.

312. While examples of more integrated approaches exist at domestic and regional level, including within the EU framework, pan-European co-ordination remains uneven. Differences in historical experience, geopolitical exposure and institutional architecture further contribute to variations in how member States structure their responses.

D. Difficulties in assessing and strengthening resilience

313. Assessing and measuring resilience to FIMI is complex. There is no commonly agreed methodology for evaluating societal, institutional or cyber resilience in this context. Resilience depends on a combination of factors, including institutional capacity, the robustness of the information environment, public awareness, and the ability of systems to anticipate, absorb and respond to disruptive activities.

314. While various resilience-building initiatives are implemented at domestic level, approaches differ in scope and emphasis. Cyber-resilience considerations highlight that no system can be regarded as fully immune to disruption, but rather that resilience involves the capacity to adapt and recover. The absence of shared indicators or benchmarking tools limits comparability across member States.

315. A structured pan-European exchange of experience and good practices in assessing and strengthening resilience remains limited.

E. Cross-border dimensions and limits of international co-operation

316. FIMI activities frequently operate across borders, affecting multiple jurisdictions simultaneously and involving actors, infrastructures or information channels located outside the target State. This transnational character may complicate detection, attribution and response, particularly where activities unfold across different legal and regulatory frameworks.

317. While member States have adopted, to varying degrees, measures within their respective jurisdictions, co-ordination at pan-European and broader international level remains uneven. Differences in institutional capacity, legal frameworks and threat perception may limit the comparability of responses and the alignment of approaches.

318. In particular, exchanges of information and analysis between States may vary in scope and format. These exchanges may concern operational assessments, analytical findings or research co-operation, but are shaped by national legal constraints and sovereign decision-making. The absence of commonly used formats or regular co-ordination practices may affect situational awareness and the timeliness of responses in cross-border cases.

F. Challenges in detection, engagement with private actors and emerging technologies

1. Detection and co-ordinated response across jurisdictions

319. The absence of commonly agreed frameworks or escalation mechanisms, including information-sharing arrangements compatible with data protection requirements, may affect the capacity of member States to ensure timely and co-ordinated responses to cross-border FIMI threats.

2. Engagement with digital platforms and private actors

320. Digital platforms and other private actors play a significant role and bear significant responsibility in the online information environment. The effectiveness of measures addressing FIMI may therefore depend in part on co-operation between public authorities and private entities. Differences in regulatory frameworks, enforcement models and levels of institutional capacity across member States may affect how such engagement is structured and implemented in practice.

321. While certain jurisdictions have established detailed regulatory approaches to platform accountability and online safety, the scope and enforceability of such frameworks vary across the Organisation, which may create challenges in ensuring consistent responses to cross-border FIMI activities.

3. Rapid technological developments and malign use of AI

322. The rapid development and uptake of AI present additional challenges, as such systems may be used to generate, amplify or target information manipulation at scale, and may also be used for other malign purposes. These technologies raise concerns not only in relation to detection, but also as regards the malign use of AI tools in the production and dissemination of manipulative content.

323. Policies governing transparency of AI-generated content, risk assessment standards and institutional expertise continue to evolve unevenly across member States, as do the availability of specialised technical capacity, training and structured engagement with global technology providers.

G. Financial dimensions of FIMI and related interference activities

324. Certain FIMI-related or foreign interference activities involve financial or logistical support structures that enable co-ordinated operations. Financial flows linked to FIMI activities may involve intermediary structures such as media outlets, organisations or civil society initiatives operating within the jurisdiction of member States. Limited transparency and uneven cross-border investigative co-operation regarding such funding channels may hinder efforts to detect and disrupt FIMI-related activities. In some documented cases, individuals have been recruited to carry out criminal acts such as sabotage, vandalism or cyberattacks, which may then be exploited for broader interference purposes. The financial arrangements underpinning such activities may rely on a variety of channels, including informal transfers, cash-based transactions or digital assets.

325. In this context, the challenge lies not only in addressing individual criminal offences, but in understanding how financial flows may facilitate co-ordinated interference strategies affecting the stability and functioning of democratic institutions. Approaches to monitoring and regulating emerging financial instruments, including crypto-assets, vary across member States, and implementation of existing regulatory standards remains uneven.

326. While comprehension of financial flows alone may not suffice to prevent interference activities, differences in regulatory frameworks, transparency requirements and investigative capacities may affect the ability of States to assess and respond to the financial dimension of FIMI-related conduct.

H. Corruption-related vulnerabilities in the context of FIMI

327. Corruption may, in certain cases, function as an enabler of FIMI-related or foreign interference activities. Documented examples include attempts to influence public decision-making, including foreign policy positions, through bribery or other improper inducements targeting public officials. In this context, it is important to distinguish clearly between legitimate lobbying activities conducted transparently and unlawful attempts to corrupt decision-making processes.

328. More broadly, corruption can weaken trust in democratic institutions and may increase societal vulnerability to manipulative or destabilising narratives. While corruption is not limited to FIMI-related conduct and remains a broader phenomenon affecting various sectors, its potential intersection with foreign interference raises specific concerns.

329. The Council of Europe has established comprehensive anti-corruption standards and monitoring mechanisms, notably through the Group of States against Corruption (GRECO). However, these frameworks address corruption as such and do not systematically examine risks from the perspective of foreign information manipulation and interference. The extent to which corruption-related vulnerabilities intersect with FIMI strategies may therefore vary across member States.

I. Criminal law frameworks and cross-border co-operation challenges

330. While most of the FIMI-related conduct may already fall within existing domestic criminal law frameworks in member States, legal qualifications and thresholds differ. These differences may affect the ability of authorities to investigate, prosecute and co-operate effectively in cross-border cases. Existing legally binding instruments highlighted in Chapter 3 may also support such co-operation.

331. Variations in how certain forms of foreign interference, information manipulation or related criminal conduct are defined in domestic law may affect the legal qualification of conduct across jurisdictions and complicate mutual legal assistance, extradition or other forms of judicial co-operation. The absence of a shared understanding of relevant criminal categories may therefore create practical challenges in operational contexts.

332. At the same time, as highlighted in Chapter 5, criminal law responses must remain a measure of last resort and be subject to strict safeguards to avoid disproportionate interference with freedom of expression and other fundamental rights.

J. Use and scope of existing international legal instruments

333. As noted in Chapter 3, several Council of Europe conventions establish binding sectoral frameworks relevant to specific aspects of FIMI-related conduct, including in the areas of cybercrime, international co-operation and AI. These instruments reflect agreed common legal standards among participating States.

334. However, these frameworks were not designed specifically to address FIMI as a distinct and co-ordinated phenomenon. Their application to FIMI-related conduct therefore depends on how relevant provisions are interpreted and implemented at national level. Ratification levels, implementation practices and operational use of these instruments vary across member States.

335. This may result in differences in how existing international legal tools are mobilised in response to FIMI-related activities. The relationship between these sectoral frameworks and the broader challenge posed by foreign information manipulation and interference may not always be addressed in a fully co-ordinated manner.

CHAPTER 7 – FEASIBILITY OF A COUNCIL OF EUROPE LEGAL INSTRUMENT

336. This chapter examines, in light of the structural challenges and gaps identified in the preceding chapter, the feasibility of action at Council of Europe level. In line with the Committee's mandate, it considers the potential added value of a co-ordinated approach, without prejudging the form, scope or legal nature of any future instrument. It reflects the diversity of views expressed within the Committee and identifies areas of convergence as well as issues requiring further consideration.

A. Examining the types of Council of Europe legal instruments

337. In examining the feasibility of action at Council of Europe level, it is relevant to recall the different types of legal instruments available within the Organisation.

338. Council of Europe conventions may take the form of detailed conventions or framework conventions. Detailed conventions typically contain more specific obligations, while framework conventions establish broader commitments, leaving greater discretion to States in domestic implementation. Both types are legally binding upon the States that ratify them and normally require implementation in domestic law. They may be supplemented by additional protocols of a similar nature.

339. Conventions and framework conventions generally provide for follow-up mechanisms (committees of the parties) responsible for overseeing implementation. Where appropriate, they may also be accompanied by structured co-operation mechanisms, including networks of designated national contact points. Depending on the subject matter, these networks may operate on a continuous basis, including, where necessary, on a 24/7 basis, facilitating direct exchanges between competent authorities.

340. Council of Europe conventions are open to accession by non-member States, which may also be invited to participate in their negotiation. This feature may enhance the geographic reach and operational coherence of co-operation frameworks.

341. Recommendations adopted by the Committee of Ministers are not legally binding but create a political commitment for all member States from the moment of their adoption. They are generally more flexible instruments and may provide guidance, standards or principles, including on criminalisation. However, as they do not create binding obligations, they do not in themselves establish formal co-operation mechanisms between States comparable to those provided under conventions.

342. The choice between these instruments therefore has implications in terms of legal effect, flexibility, monitoring arrangements, operational co-operation and the scope of participation.

B. Articulating the nature of the threat and appropriate measures

343. The Committee's discussions highlighted areas of emerging convergence. The analysis in Chapter 6 highlighted differences in how FIMI is understood among member States. Action at Council of Europe level could consist of articulating a shared understanding of the nature of the FIMI threat and appropriate responses, while further clarifying key concepts, including FIMI and adjacent notions.

344. This clarification would provide common reference points reflecting existing Council of Europe standards. It would aim to enhance legal certainty, support comparability of national approaches and strengthen cross-border co-operation. Further work could also explore possible approaches towards some degree of alignment of legal definitions, considering the diversity of domestic legal frameworks.

345. Any approach of this kind would need to consider the diversity of national legal traditions and institutional structures, as well as the need to preserve flexibility in domestic implementation. Any such work should remain complementary to initiatives undertaken in other international fora.

C. Strengthening institutional capacity and co-ordination

346. A further area for consideration concerns institutional capacity to address FIMI-related conduct. The analysis in Chapter 6 highlighted variations in the organisation and co-ordination of competent authorities across member States.

347. Possible approaches at Council of Europe level could include the articulation of guiding principles on institutional preparedness, the exchange of good practices, or the development of structured co-operation frameworks between designated national authorities. The scope and legal effect of these measures would depend on the type of instrument chosen.

348. Any initiative in this area would need to preserve flexibility in order to accommodate differing constitutional systems, administrative structures and legal traditions. Cross-border co-operation between relevant national services could also be strengthened, building on existing legal frameworks and institutional arrangements.

D. Promoting a holistic and comprehensive policy approach

349. The structural challenges identified in Chapter 6 suggest that responses to FIMI may remain fragmented across policy domains. Measures relating to resilience, digital governance, criminal law, foreign policy and international co-operation are often developed within separate or diverging institutional and legal frameworks.

350. A more holistic, multi-stakeholder approach at Council of Europe level could aim to strengthen coherence between these different strands of action. This may involve clarifying how preventive, regulatory, enforcement and co-operative measures interact, and ensuring that responses are mutually reinforcing rather than isolated.

351. Particular attention could be given to electoral contexts and other periods of heightened democratic vulnerability. Clarifying roles and responsibilities of relevant public authorities, platforms and oversight bodies in such situations may contribute to greater predictability and co-ordination, without prejudging the form of legal or regulatory responses, while respecting the work of journalists and other relevant actors.

352. Depending on the form envisaged, this approach could take the form of guiding principles, common reference frameworks or structured exchanges designed to promote policy alignment, while preserving flexibility for national implementation.

E. Strengthening resilience to FIMI

353. Resilience was identified in Chapter 6 as a central dimension of responses to FIMI, encompassing institutional preparedness, media pluralism, education and public awareness. Differences in approaches and methodologies across member States may affect comparability and the cumulative impact of resilience-building efforts.

354. Action at Council of Europe level could contribute to greater coherence by facilitating the exchange of experience and the identification of common reference points for resilience strategies. Depending on the form envisaged, this might include the development of shared methodological tools for assessing resilience, the articulation of guiding principles, or the promotion of structured co-operation among experts and competent authorities.

355. Education and awareness-raising measures remain key components of resilience. A common framework could support further reflection on standards and best practices in this area, while allowing flexibility for national implementation.

356. This may also include reflection on practical skills enabling individuals to recognise manipulative techniques, including the use of emerging technologies, and on support mechanisms for independent fact-checking and civic oversight initiatives.

F. Enhancing international co-operation

357. The transnational nature of FIMI-related activities has an impact on the adequacy of existing mechanisms for international co-operation. Differences in legal frameworks, institutional capacities and operational practices may affect the speed and consistency of cross-border responses.

358. Several forms of co-operation may be envisaged, depending on the level of formality and legal basis considered appropriate. At a more flexible level, enhanced exchange of information, analytical assessments and good practices could take place through existing platforms or through arrangements established by decision of the Committee of Ministers.

359. Consideration could also be given to the exchange of best practices and possible guidance concerning the public attribution of FIMI operations, while recognising that decisions on attribution remain within the competence of member States. This reflection might address evidentiary thresholds, safeguards against wrongful or politically motivated attribution, and co-ordination of public communication, while respecting national legal frameworks and due process guarantees

360. More formalised structures, including standing co-ordination mechanisms or networks of designated contact points, may provide a clearer legal basis for facilitating operational exchanges between competent authorities, including on a continuous basis. In certain fields, these mechanisms have been established through conventions providing for committees of the parties and, where appropriate, operational networks facilitating direct exchanges between competent authorities, including on a continuous basis.

361. The implications of each option would differ in terms of legal effect, durability, monitoring arrangements and the possible participation of non-member States. Clarifying which forms of co-operation require a binding legal framework and which may be established through more flexible instruments may therefore be relevant to the assessment of feasibility.

362. A future Council of Europe legal instrument on FIMI which provides for or allows member States to introduce powers and procedures that interfere or are likely to interfere with human rights and fundamental freedoms should also provide that member States must ensure that the implementation of such powers and procedures is subject to conditions and safeguards provided for under their domestic law. Such conditions and safeguards should provide for adequate protection of human rights and fundamental freedoms in compliance with the European Convention on Human Rights.

G. Improving detection capacities and engagement with private actors

363. The detection of FIMI-related activities, particularly where they unfold across jurisdictions and digital platforms, raises practical co-ordination challenges. Variations in national legal frameworks and institutional arrangements may affect the timeliness and consistency of responses.

364. Depending on the level of formality envisaged, action at Council of Europe level could contribute to greater clarity regarding escalation procedures, information-sharing practices and engagement with relevant private actors. These arrangements could take different forms, ranging from non-binding guidance to more structured co-operation frameworks.

365. Depending on the instrument envisaged, consideration could also be given to articulating baseline expectations regarding platform due diligence in addressing co-ordinated inauthentic behaviour and systemic risks linked to FIMI, while ensuring full respect for freedom of expression and proportionality requirements.

366. Member States may have varying levels of leverage when engaging with large online service providers, owing to differences in institutional capacity and market size. In this context, enhanced co-operation and exchange of experiences at Council of Europe level could support more effective and co-ordinated engagement with these actors.

H. Responding to emerging technologies and the use of AI

367. The use of AI and potentially other emerging digital technologies in the context of FIMI operations presents additional challenges. Differences persist in regulatory approaches, transparency requirements and institutional expertise across member States.

368. Existing Council of Europe standards, including those relating to cybercrime and AI, and potentially other emerging digital technologies, provide a relevant legal and normative framework. Further reflection could consider how these standards may apply to the malicious use of AI in the context of FIMI-related conduct, considering the need to ensure compatibility with human rights, democracy and the rule of law.

I. Addressing the financial dimension of FIMI

369. The financial dimension of certain FIMI-related or foreign interference activities raises questions regarding the adequacy and coherence of existing regulatory and investigative frameworks. Funding structures may involve a range of mechanisms, including informal transfers, opaque financing arrangements or digital assets, and may intersect with criminal, financial and transparency regulations. Financial flows linked to FIMI activities may in certain instances involve intermediaries based within member States' jurisdictions. This underscores the importance of transparency and investigative co-operation in addressing such channels.

370. Council of Europe instruments relating to anti-money laundering, confiscation of proceeds of crime and financing of terrorism provide relevant legal standards and co-operation mechanisms. Consideration could be given to how these existing frameworks may apply to financial flows linked to FIMI-related conduct, taking into account differences in implementation and enforcement across member States.

371. Depending on the approach envisaged, action at Council of Europe level could range from promoting greater awareness and co-ordination in the use of existing tools to clarifying how financial investigations and asset-tracing measures may interact with broader responses to foreign interference. An adaptation of relevant existing standards to the specific requirements in relation to the disruption of FIMI could provide added value.

J. Assessing corruption-related vulnerabilities in the context of FIMI

372. Corruption-related vulnerabilities may intersect with FIMI-related or foreign interference activities, particularly where attempts are made to influence public decision-making through improper inducements. While corruption is a broader phenomenon affecting various sectors, its potential interaction with foreign interference raises specific concerns in certain contexts.

373. The Council of Europe has established comprehensive anti-corruption standards and monitoring mechanisms, including through GRECO and the relevant criminal and civil law conventions. Consideration could be given to how these existing frameworks address, or could be interpreted in relation to, corruption risks linked to FIMI-related conduct.

374. Depending on the approach envisaged, action at Council of Europe level could involve clarifying the relationship between anti-corruption standards and foreign interference vulnerabilities or facilitating greater coherence between existing monitoring mechanisms and emerging challenges.

K. Considering criminal law options in relation to FIMI-related conduct

375. As examined in Chapter 5, criminal law responses to FIMI-related conduct raise complex human rights considerations and must remain a measure of last resort. The issue at this stage is however not whether criminalisation is appropriate *in abstracto*, but whether and how action at Council of Europe level could address challenges identified in Chapter 6.

376. Different legal instruments would entail different implications. A recommendation could provide guidance on safeguards, principles of legality and proportionality, and the treatment of aggravating circumstances linked to foreign interference and may also encourage the consideration of criminalisation in domestic law[161].

377. A convention could in addition foresee binding obligations concerning the criminalisation of specific forms of FIMI-related conduct, subject to sufficiently clear definitions of the relevant offences. A framework convention could achieve the same while leaving a larger margin of appreciation with regards to implementation by the Parties.

378. Any future Council of Europe legal instrument on FIMI providing for criminal law measures should ensure that the implementation of such measures is subject to appropriate conditions and safeguards under domestic law. Such conditions and safeguards should ensure adequate protection of human rights and fundamental freedoms in compliance with the European Convention on Human Rights.

379. Each option would have consequences in terms of legal effect, degree of harmonisation, monitoring arrangements and impact on domestic criminal law systems. The existence of clearly defined and commonly understood criminal provisions in this area may support deterrence and facilitate cross-border co-operation with regard to conduct that are already criminalised in domestic law.

L. Making use of existing Council of Europe legal instruments

380. As noted in Chapter 3, several Council of Europe conventions establish binding sectoral frameworks relevant to certain aspects of FIMI-related conduct, including in the areas of cybercrime, international co-operation and AI. These instruments provide important legal standards and mechanisms that may be mobilised in specific contexts.

381. However, these frameworks were not designed to address FIMI as a co-ordinated and cross-cutting phenomenon. Their applicability therefore depends on how individual provisions are interpreted and implemented at national level. Variations in ratification status, entry into force and operational practice may limit their combined effectiveness in responding to complex FIMI-related activities.

CHAPTER 8 – CONCLUSIONS

382. In accordance with its Terms of Reference, the Committee was tasked with examining the feasibility of developing a Council of Europe legal instrument addressing foreign information manipulation and interference (FIMI), including disinformation, and exploring possible approaches to prevention, awareness-raising and education measures, and in particular whether certain forms of FIMI-related conduct could warrant criminalisation.

383. The Committee considered that FIMI constitutes a serious threat to democratic and national security, human rights and the rule of law, both in Europe and globally. Such activities may further undermine democratic debate and the functioning of free and pluralistic media. The discussions within the Committee have also reflected a growing shared understanding of the nature of the threat posed by FIMI.

384. Due to the transnational character and cross-border effects of FIMI, there is added value in member States adopting a co-ordinated approach to countering FIMI and working together to prevent, build resilience against, and disrupt FIMI operations, as well as to ensure accountability. Such co-operation could be based on a set of shared principles and must remain rooted in respect for democracy, human rights and the rule of law.

385. The Committee has also identified areas for further strengthening co-operation, particularly in fields such as digital governance and addressing the challenges related to online service providers in the context of countering and disrupting FIMI. For example, online platforms, often based outside the jurisdiction of member States, may play a role in enabling foreign actors to disseminate manipulated information aimed at undermining the integrity, independence and effectiveness of democratic processes and institutions.

---

[161] See, for example: CM/Rec(2024)4 on combating hate crime; CM/Rec(2022)16 on combating hate speech; and CM/Rec(2019)1 on preventing and combating sexism.

386. The Committee has acknowledged that member States do not conceptualise FIMI in a uniform manner, particularly with regard to the notion of “foreign interference”. For some member States, the interference element of FIMI is understood primarily as operating within the informational sphere. Other member States consider the interference element of the term FIMI to include a broader hybrid threat strategy. Both understandings of the term interpret the aims of FIMI to be undermining trust and engagement in democratic processes and institutions, creating an atmosphere of insecurity and vulnerability, exploiting political and social divisions within a population, and sometimes involving criminal activities.

387. The lack of an agreed concept of FIMI reflects the different experiences and levels of exposure of member States to FIMI operations. These differences have led to the adoption of different responses to the threat. The Committee considers that further efforts aimed at bringing together the various concepts of FIMI and the corresponding responses are warranted.

388. The Committee has also agreed on the importance of the various categories of responses to FIMI identified in this study, including resilience-building measures, governance and regulatory responses, detection and analytical capacities, accountability and enforcement mechanisms, network disruption as well as national and international co-operation frameworks. The Committee emphasised that these responses are complementary and that addressing FIMI effectively requires a holistic, whole-of-government and whole-of-society approach. In particular, measures aimed at strengthening resilience, digital governance and international co-operation were highlighted as key elements in addressing FIMI.

389. The Committee was requested under its Terms of Reference to examine the feasibility of criminalising certain conduct related to FIMI. The Committee noted that some relevant conduct may already be criminalised under domestic law, for example sabotage, corruption or certain forms of cybercrime. The Committee agreed that criminalisation should remain a measure of last resort.

390. Some of the members of the Committee were opposed to additional criminal law provisions in a Council of Europe instrument related to FIMI, stressing the potential negative effects on the rights guaranteed under Article 10 of the European Convention on Human Rights and the risk of legal uncertainty due to duplication effect with existing legally binding instruments.

391. Other members of the Committee were in favour of including criminalisation provisions in a Council of Europe instrument addressing FIMI-related conduct, noting that some relevant offences were already criminalised at domestic level. From a procedural law perspective, they considered that international co-operation in criminal matters, including mutual legal assistance and extradition, could be facilitated if certain criminal offences were recognised under specific conditions as FIMI-related crime. Examples of relevant offences at domestic level include sabotage, corruption, cybercrime, money laundering, illicit financing of electoral campaigns, and organised crime.

392. The Committee underlined the risks inherent in criminalisation. It recommended leaving the question of whether and how to criminalise certain conduct related to FIMI to a possible subsequent committee that may be tasked with the elaboration of a legal instrument of the Council of Europe on FIMI. Should the Committee of Ministers decide to pursue criminalisation of FIMI-related conduct, this issue would require further in-depth examination.

393. The Committee, in accordance with its Terms of Reference, also examined issues relating to the media in the context of FIMI. While underlining the key importance of free and independent media and journalism providing a counter point to FIMI and disinformation, the Committee noted that most of these issues are already addressed by Council of Europe standards. Any future legal instrument should therefore focus on specific FIMI related responses and build upon the Organisation's existing acquis.

394. Given the multifaceted nature of FIMI, effectively countering it requires a comprehensive approach combining preventive, regulatory, analytical and co-operative measures across multiple policy domains.

395. The Committee finally noted that several international frameworks relevant to some aspects of FIMI already exist. A possible new initiative at Council of Europe level should therefore be complementary to these frameworks. The Committee considered that a Council of Europe legal instrument on FIMI could provide added value, notably through its human rights-based and rule-of-law approach, the Organisation’s pan-European membership and the potential global vocation of a future instrument.

396. In examining the feasibility of elaborating a Council of Europe legal instrument addressing FIMI, the Committee has identified a number of challenges and gaps which could be addressed by the Council of Europe in a legal instrument.

397. Members of the Committee expressed different views regarding the possible form of such legal instrument.

398. Some members preferred a non-legally binding instrument in the form of a recommendation by the Committee of Ministers to the member States. Such an instrument, though not legally binding, creates a political commitment for all member States. It can be adopted and take effect immediately, without the need for ratification procedure. Addressed only to member States, a recommendation cannot serve as a basis for involving non-member States in the counter-FIMI activities under the Council of Europe. That said, it can be a more flexible instrument than a convention.

399. Other members preferred a legally binding instrument in the form of a convention or a framework convention. Both types of treaties are legally binding on their Parties upon ratification or accession. A framework convention establishes a framework of principles, procedures and institutional co-operation to guide the implementation of commitments by the Parties. Framework conventions usually contain principles, and are less detailed in the legal requirements for its Parties than conventions. Such instruments may be open to negotiation accession by non-member States, which could strengthen the effectiveness and global outreach.

400. The Committee also noted that the options discussed in this study should not necessarily be seen as mutually exclusive. Depending on the decision taken by the Committee of Ministers, different forms of action at Council of Europe level could be pursued, either separately or in combination.

401. Hence the Committee cannot pronounce itself on the choice of legal instrument but merely notes that this choice will have implications for the range and characteristics of the measures that can be implemented under the type of legal instrument chosen.

402. The Committee recalled that any future Council of Europe legal instrument on FIMI providing for measures, whether criminal or otherwise, that interfere or are likely to interfere with human rights and fundamental freedoms should subject the implementation of such measures to appropriate conditions and safeguards under domestic law. Such conditions and safeguards should ensure effective protection of these rights and freedoms in compliance with the European Convention on Human Rights.

403. Building on the considerations set out in chapter on the feasibility of a Council of Europe legal instrument, and depending on the choice of legal instrument, the Committee suggests that the following elements could be considered for inclusion in a Council of Europe legal instrument on FIMI:

(a) Articulating the nature of the threat and appropriate measures

404. Further developing a shared understanding of the nature of the threat and appropriate responses concerning FIMI and related notions, with a view to enhancing legal certainty, consistency of approaches, and effective cross-border co-operation, while respecting the diversity of national legal traditions.

(b) Strengthening societal and media resilience

405. Promoting media and information literacy and public awareness of manipulation techniques in the context of countering FIMI. This also includes targeted support for independent and pluralistic journalism, building on existing Council of Europe standards. It may also involve structured co-operation among experts and competent authorities for the exchange of good practices

(c) Addressing systemic risks in the digital information environment

406. Encouraging transparency, risk assessment, and proportionate due diligence measures in relation to co-ordinated inauthentic behaviour, political advertising, and algorithmic amplification with a view to safeguarding information integrity, in a manner consistent with freedom of expression, proportionality requirements, and existing regulatory frameworks. This may also include further reflection on the role of emerging digital technologies, including artificial intelligence, and on practical approaches to co-operation with digital platforms.

407. Particular challenges may arise for some member States in engaging effectively with large digital platforms, given differences in institutional capacity and market size. Enhanced co-operation and exchange of experience at Council of Europe level may therefore contribute to more balanced and effective engagement with such actors.

(d) Protecting electoral integrity

408. Ensuring appropriate safeguards to protect electoral processes from foreign interference, including cybersecurity measures, transparency requirements, and proportionate co-operation mechanisms involving relevant public authorities and digital platforms, in full respect of Article 3 of Protocol No. 1 to the European Convention on Human Rights (right to free elections) and related human rights guarantees.

(e) Enhancing institutional preparedness and structured operational co-operation

409. Encouraging the designation or establishment of competent national structures responsible for detecting and analysing FIMI-related activities, and facilitating structured, timely and operational cross-border co-operation, including through designated contact points and agreed modalities for information-sharing, particularly in situations of heightened democratic vulnerability, such as electoral processes.

(f) Developing guidance for the attribution of FIMI operations

410. Consideration could also be given to the exchange of best practices and possible guidance concerning the public attribution of FIMI operations. Such guidelines might address evidentiary thresholds, safeguards against wrongful or politically motivated attribution, and co-ordination of public communication. It should respect national legal frameworks and due process guarantees, recognise that decisions on attribution remain within the competence of member States, and ensure compatibility with the European Convention on Human Rights as applied and interpreted by the European Court of Human Rights.

(g) Considering criminal law options as a measure of last resort

411. Where appropriate and depending on the form of any instrument under discussion, considering the establishment of baseline standards or guidance concerning the criminalisation of intentional and co-ordinated interference conducted on behalf of, or under the direction or control of, foreign States or foreign actors, including where such conduct is carried out with the intention of benefiting them.

412. Any such measures should remain a measure of last resort and be subject to appropriate safeguards to ensure full respect for human rights and fundamental freedoms, in line with the European Convention on Human Rights.

413. In conclusion, the feasibility study reflects the work of the Committee at the current stage and within the time available. The Committee agreed on the feasibility of a Council of Europe legal instrument addressing FIMI, with a particular focus on supporting resilience building, sharing of best practice and facilitating international co-operation and an emphasis on a shared set of principles grounded in human rights, democracy and the rule of law. However, the study should not be considered exhaustive or definitive as to the scope of issues that may need to be addressed. Further work would be required for a possible Council of Europe legal instrument, particularly in light of the rapidly evolving nature of FIMI-related challenges, which continue to pose a threat to democracy.