RESONANT

Handbook on Information Suppression and FIMI

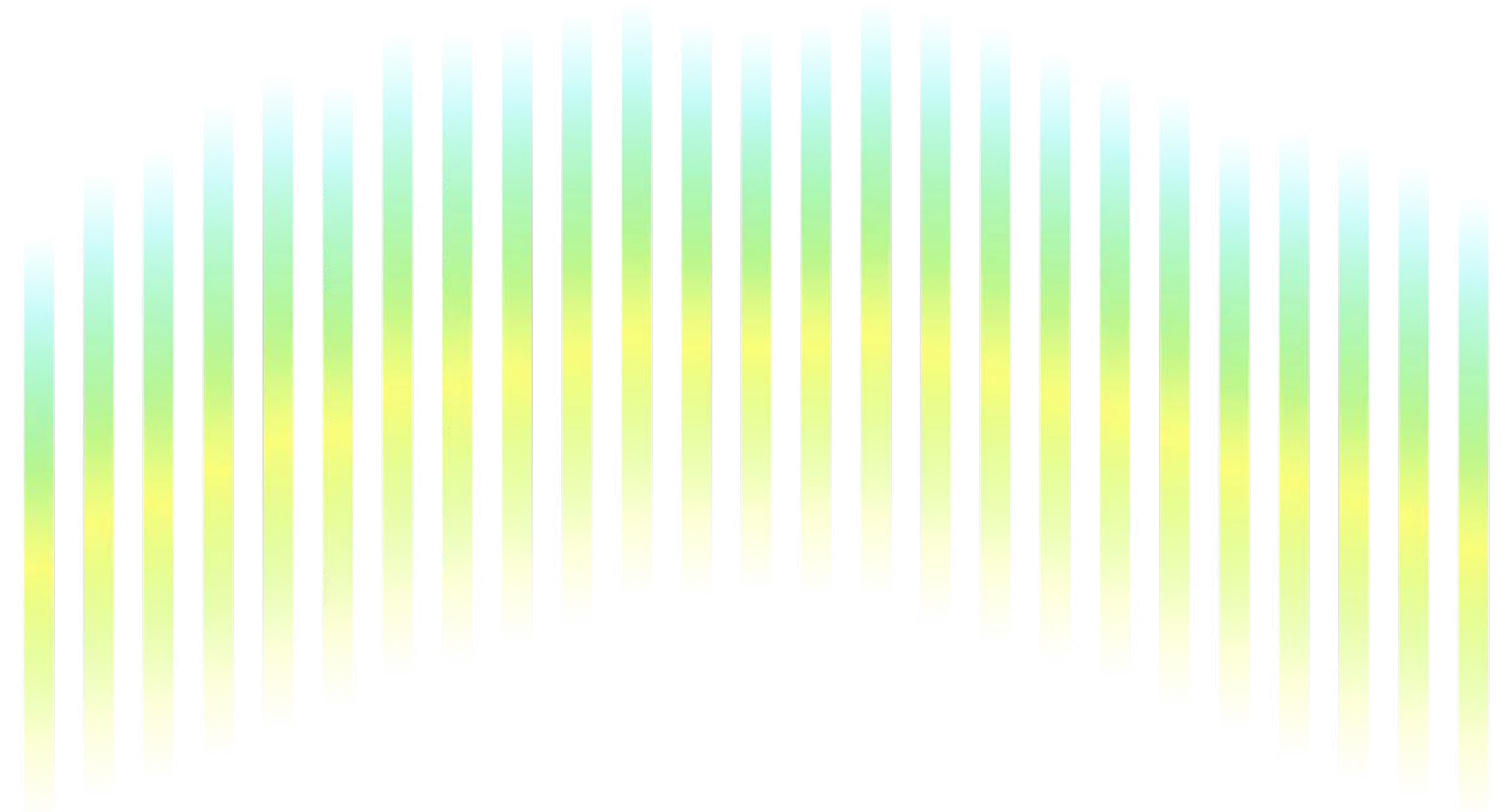
Co-funded by the European Union

MULTIDISCIPLINARY RESEARCH COOPERATION ON INFORMATION SUPPRESSION AND DIASPORA COMMUNITIES AS A TARGET OF FOREIGN INFORMATION MANIPULATION AND INTERFERENCE

© RESONANT Consortium, 2024

Any dissemination of results reflects only the author's view and the European Commission is not responsible for any use that may be made of the information it contains.

This deliverable contains original unpublished work except where clearly indicated otherwise. Acknowledgement of previously published material and of the work of others has been made through appropriate citation, quotation, or both. Reproduction is authorised provided the source is acknowledged.



RESONANT

Foreign Information Manipulation and Interference (FIMI) including information suppression concern a series of threatening behaviours in the information domain and represents a major challenge, in terms of counteraction and the policy-making in this matter. Numerous FIMI operations carried out by non-EU State and non-State actors, often recorded within and beyond EU borders, aims to domestically threaten fundamental rights and freedoms and could as well produce threatening effects outside of their borders.

The RESONANT project aims to create a better picture and understanding of State and non-State actors applying information suppression and to recommend strategies, tools and methodologies to reduce the impact and the vulnerability of the target groups, as the Diaspora Communities. In order to understand which actors outside the EU use in a coordinated manner Tactics, Techniques and Procedures (TTPS) of information suppression, RESONANT proposes to analyse information suppression incidents, thus creating an Evidence Base. Considering both the domestic and cross-border dimensions of information suppression, the project will also examine the mainly adopted TTPs, as well as the available Tools for their Detection and Analysis. For enhancing the knowledge regarding the effects of information suppression, RESONANT proposes an analysis of Behavioural changes in Diaspora Communities as result of information suppression and of the Awareness and Preparation of EU State Authorities in terms of practical legal means, providing selected Case Studies.

Furthermore, the project will propose the definition of a Methodological Toolkit and Policy Recommendations, as well as the organisation of Table-Top Exercises and Focus Group Policy Discussion, for addressing information suppression and FIMI. RESONANT will realise a Handbook of methodologies and policy recommendations, contributing to communicate and disseminate practical means to counter information suppression and FIMI.[1]

1 Grant Agreement No 101132439, p. 8.

© 2026 RESONANT | Horizon Europe Grant Agreement N. 101132439

Index of Figures 5
Index of Tables 5
List of acronyms 5
1. Introduction 6
1.1 The RESONANT project 6
1.2 Purpose of the document 7
1.3 Scope of the document and intended audience 7
1.4 Structure of the document 8
2. Conceptual Foundations 9
2.1 Glossary 9
2.2 Terms in context 12
2.3 Main legal frameworks 13
3. How FIMI Works: TTPs, Behavioural Patterns and Social Impact 16
3.1 From isolated content to coordinated environments 16
3.2 Social impact framework 19
3.3 Observable behavioural patterns 20
3.4 From individual behaviour to social dynamics 21
3.5 Impact assessment 23
4. From Signals to Evidence: The streamlined version of the Detection Methodology 25
4.1 Open/Park incidents 25
4.2 Incident Sheet 28
4.3 Step by step guidance 37
4.4 Practical example 40
5. From Analysis to Action 42
5.1 Decision thresholds 42
5.2 Escalation logic: how to change the level of response 44
5.3 When NOT to act 45
6. Counteraction in Practice 46
6.1 Principles of effective response 46
6.2 Type of response 48
6.3 Constraints and feasibility 50
6.4 Role-based guidance 52
7. Limits, Risks and Misuse 55
7.1 Methodological Limits 55
7.2 Risks of misinterpretation and misuse 56
7.3 Practical Implications for Practitioners 58
8. Final remarks 59
Annex – Glossary 60
Annex – Digital literacy in the classroom: a ready-to-use simulation to practise recognising FIMI. 65
Bibliography 78

© 2026 RESONANT | Horizon Europe Grant Agreement N. 101132439
Co-funded by the European Union

Index of Figures

Figure 1	Scheme illustrating the key questions underlying each category of term.	9
Figure 2	Brief overview of the key terms mentioned in the RESONANT Handbook.	11
Figure 3	Timeline of the main legal pillars, relevant for the Handbook.	13
Figure 4	Analysis of the impact of coordinated narratives on social dynamics.	19
Figure 5	Principles of effective response.	46
Figure 6	Main features of each category of response.	48
Figure 7	How the intersection of feasibilities allows an effective response.	52
Figure 8	Workflows for each category of actor analysed, according to RESONANT Stakeholder Board.	54
Figure 9	Scheme of the RESONANT approach.	65
Figure 10	Fake Euronews screenshot from Telegram channel “Шкварка News”	77

Index of Tables

Table 1	Glossary contextualisation table.	13
Table 2	Simplified outline of a possible disinformation campaign.	17
Table 3	Summary table of the differences between the categories of the Social Impact Framework.	19
Table 4	Summary table of selected examples of behavioural patterns observed in RESONANT.	20
Table 5	Social dynamics and related manifestation.	22
Table 6	Table summarising the three levels of impact and their characteristics.	23
Table 7	Evidence x Severity Matrix.	36
Table 8	Table summarising the main features of each response.	49
Table 9	Most appropriate type of response to a range of examples according to RESONANT Stakeholder Board.	49
Table 10	Overview of the four dimensions of gaps and constraints described.	51

List of Acronyms

Abbreviation	Definition
DSA	Digital Services Act
EMFA	European Media Freedom Act
FIMI	Foreign Information Manipulation and Interference
GRs	Guardrails
LEAs	Law Enforcement Agencies
OSINT	Open-source intelligence
TLP	Traffic Light Protocol
TTPs	Tactics, techniques and procedures

© 2026 RESONANT | Horizon Europe Grant Agreement N. 101132439

1. Introduction

Foreign Information Manipulation and Interference (FIMI) and information suppression have become increasingly significant challenges for democratic societies. Coordinated attempts to manipulate information environments, distort public debate, intimidate individuals and communities, or suppress legitimate voices cannot be left solely to institutions and governments. As information ecosystems become more interconnected and digital platforms facilitate the rapid dissemination of narratives across borders, recognising and responding to these phenomena can no longer remain the exclusive responsibility of a limited group of specialists, but it requires the involvement of researchers, journalists and civil society organisations, as well as society as a whole.

The **RESONANT Handbook on Information Suppression and FIMI** has been developed to support this broader effort. It offers practical guidance on how information manipulation operates, how to recognise its main characteristics, assess available evidence and identify appropriate response options. Throughout the document, technical concepts are presented in an accessible manner and translated into practical tools that can be applied by a wide variety of actors in everyday contexts.

The Handbook represents the final methodological output of the RESONANT project. It consolidates the knowledge generated throughout the project into a single operational resource, bringing together conceptual foundations, behavioural research, legal analysis, methodological development and policy recommendations. Its objective is to promote a shared understanding of FIMI and information suppression while encouraging consistent, proportionate and rights-respecting approaches to their identification and management.

1.1 The RESONANT project

The RESONANT project[2] was established to improve European capacity to understand, detect and respond to FIMI and information suppression. Bringing together universities, research centres, law enforcement agencies, public bodies and specialised organisations from across Europe, the project adopted a multidisciplinary approach combining social sciences, law, behavioural research, communication studies and security analysis.

Over three years, the project examined how information manipulation from foreign actors affects democratic societies and, in particular, how it targets vulnerable communities such as diaspora groups. RESONANT research investigated both the behavioural consequences of manipulation and the legal and institutional capacity to respond effectively while respecting fundamental rights.

The project combined multiple research methods and validation activities. These included literature reviews, empirical case studies, interviews with members of diaspora communities, legal and policy analysis, methodological development, simulation exercises, workshops and consultations with experts. Particular attention was devoted to validating the project's findings through focus groups and stakeholder engagement involving researchers, journalists, public authorities, civil society organisations, security practitioners and representatives of affected communities.

RESONANT also benefited from continuous dialogue with other Horizon Europe projects working on FIMI, disinformation and hybrid threats: Athena, Adac.io, De-Conspirator, ARM, Saufex, members of

2 Horizon Europe - Grant Agreement N. 101132439.

© 2026 RESONANT | Horizon Europe Grant Agreement N. 101132439
Co-funded by the European Union

the FIMI Cluster. These exchanges enabled the consortium to compare methodologies, discuss emerging challenges and ensure that the project's outputs remained aligned with broader European research efforts.

1.2 Purpose of the document

This Handbook has been developed as a practical guide for understanding key concepts underlying FIMI and how manipulation campaigns are designed and implemented, presenting a simplified methodology for recognising potential indicators of coordinated information manipulation. It also provides guidance on assessing available evidence and selecting proportionate response options according to the specific characteristics of each situation.

The Handbook is intended to support informed decision-making, not to replace professional investigation. It does not aim to provide definitive answers in every situation, nor does it encourage immediate conclusions based on isolated observations. Instead, it promotes a structured, evidence-based approach that helps readers distinguish between legitimate public debate, isolated misinformation and coordinated manipulation campaigns.

A central objective of the Handbook is to encourage responsible action. Recognising suspicious content is only the first step. It is also crucial to understand what should happen next, who should be involved, which response options are appropriate and which actions are to be avoided, since they could inadvertently amplify harmful narratives or create unnecessary risks.

1.3 Scope of the document and intended audience

This Handbook is intended for a broad audience. It has been written for people who may encounter manipulated information during their professional activities or everyday use of digital platforms or media, even if they have no previous expertise in FIMI analysis.

Researchers working in disciplines unrelated to information manipulation may discover suspicious narratives while collecting online data. Journalists may observe coordinated amplification of particular stories or narratives. Civil society organisations may witness targeted campaigns against vulnerable groups. Public officials, educators and community organisations may identify narratives affecting the communities with which they work. Citizens themselves increasingly encounter suspicious social media posts, coordinated online behaviour or misleading articles whose authenticity is difficult to assess.

For all these readers, the Handbook provides practical support for recognising FIMI and information suppression and evaluating possible courses of action. It explains how to identify characteristics of manipulated narratives and information suppression techniques, while emphasising the importance of evidence, context and proportionality before drawing conclusions.

The document is equally concerned with what happens after a potential FIMI incident has been recognised. Different users of the Handbook are entitled with different responsibilities, expertise and resources. For this purpose, the Handbook translates the European approach fostered through the EEAS FIMI Toolbox, which distinguishes among responses implemented by citizens, non-governmental organisations and governmental actors.

© 2026 RESONANT | Horizon Europe Grant Agreement N. 101132439

Ultimately, the Handbook seeks to contribute to a broader culture of resilience. Building resilience against FIMI is not solely the responsibility of governments, security agencies or specialised analysts. It depends upon informed communities, responsible institutions and aware citizens, able to recognise manipulation, understand its potential consequences and contribute, within their own roles, to protecting democratic debate.

To ensure this outcome, the Handbook offers a ready-to-use simulation to practise recognising FIMI. This simple tool, which can be found in the annex at the end of the document, can be used in schools to provide a useful exercise designed to guide pupils (and others) in developing a critical and informed perspective on FIMI and disinformation.

1.4 Structure of the document

The Handbook is organised as a progressive guide that accompanies users from the basic concepts of FIMI to practical approaches for detection, assessment and response.

Following this introduction, **Section 2** introduces the conceptual foundations of FIMI and information suppression, defining the main terminology used throughout the Handbook and explaining how these phenomena relate to democratic processes and information ecosystems.

Section 3 examines how FIMI campaigns operate in practice. It introduces common tactics, techniques and procedures (TTPs), illustrates recurring behavioural patterns observed during the RESONANT research, and explains the social impacts that manipulation campaigns may produce for individuals, communities and democratic institutions.

Section 4 presents a streamlined version of the RESONANT detection methodology. It describes how observable signals can be transformed into structured evidence through a practical analytical process suitable for non-specialist users while maintaining methodological rigour.

Building on this analysis, **Section 5** explains how analytical findings can support informed decision-making. It presents a practical framework for selecting proportionate responses according to the available evidence, the potential impact of the incident and the role of the practitioner.

Section 6 focuses on counteraction in practice. It discusses the principles that should guide effective responses, illustrates different categories of intervention, examines the practical constraints that may affect implementation, and provides role-specific guidance together with operational checklists for different categories of users.

Finally, **Section 7** discusses the limits of the methodology and highlights the importance of avoiding misuse, overreaction and unintended consequences. Throughout the Handbook, particular emphasis is placed on proportionality, protection of fundamental rights and the need to ensure that responses to FIMI strengthen democratic values.

© 2026 RESONANT | Horizon Europe
Grant Agreement N. 101132439
Co-funded by the European Union

2. Conceptual Foundations

Effective responses to FIMI and information suppression require a shared understanding of key concepts. To facilitate consultation and use of the present Handbook, this chapter provides a concise glossary of the core concepts used throughout the document. The glossary is designed as a practical reference tool to support a common understanding, particularly among users that are not specialists in open-source intelligence (OSINT), information operations analysis, or disinformation research.

The definitions presented hereinafter prioritise operational usability over theoretical completeness. Each term is accompanied by an explanation and an example illustrating its practical application. The definitions should not be interpreted as legal determinations or attribution criteria and the glossary is not intended to be exhaustive. Particular attention is given to concepts that are central to the RESONANT methodology, including information suppression, social impact, resilience and harm, while additional or more specialised terminology is provided in the annexes and supporting project documentation.

2.1 Glossary

Prior to presenting the definitions of the selected terms in this glossary, it is beneficial to provide an overview of the broad categories to which each term belongs. Indeed, the dynamics underlying FIMI incidents are complex and involve the simultaneous interaction of multiple factors and actors. Hence, the diagram below follows a sequential logic and divides the terms into categories ranging from the understanding of the broader context in which the action takes place to the ability to cope with its consequences at community level.

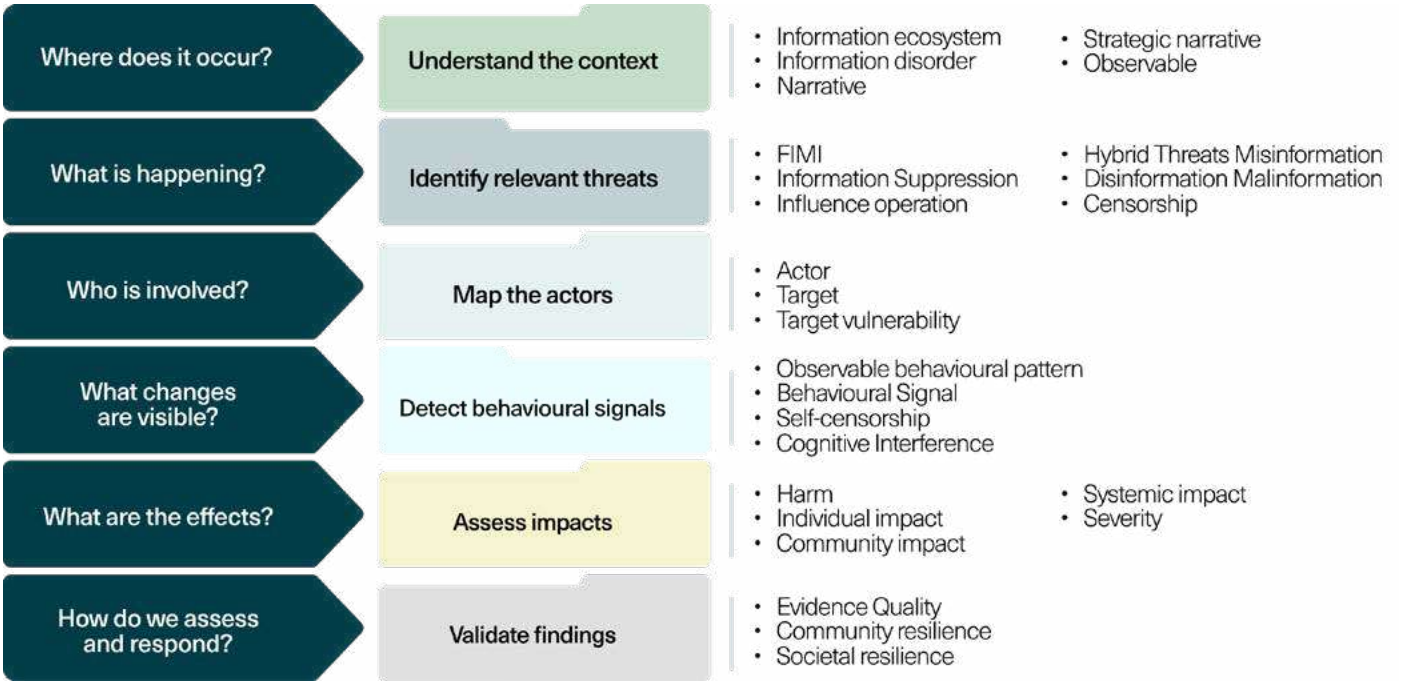


Figure 1 - Scheme illustrating the key questions underlying each category of term.

© 2026 RESONANT | Horizon Europe Grant Agreement N. 101132439

In the following figures are presented eleven of the most relevant terms in the RESONANT research. They have been selected among the others – included in the annex – to illustrate the key concepts considered fundamental for the use of the Handbook.

Understand the context

[Narrative]

A structured interpretation that gives meaning and coherence to events or realities. Narratives operate as performative acts that actively constitute social reality within a performative order. In influence operations, function as epistemic weapons capable of imposing cognitive domination narratives or reshaping ontological assumptions about legitimacy, identity, and truth.

Source: D4.1 RESONANT

[Observable]

concrete elements relevant to understand how an incident unfolded – such as a tweet, a video on YouTube or an article on a website. Observables can be represented via the URL under which they were found or as files.

Source: EEAS, 2023

Identify relevant threats

[FIMI]

A pattern of behaviour that threatens or has the potential to negatively impact values, procedures and political processes. Such activity is manipulative in character, conducted in an intentional and coordinated manner. Actors of such activity can be state or non-state actors, including their proxies inside and outside of their own territory.

Source: EEAS, 2020

[Information Suppression]

The intentional action by state or non-state actors of controlling or eliminating activities or publications that disclose relevant information - data, facts, theories, or pertinent knowledge - whether to influence public opinion, restrict access to information, or maintain secrecy. These operations may take place before having the information spread (active) or after (reactive), by blocking or eliminating the information source.

Source: D1.2 RESONANT

[Misinformation]

Information that is false but believed to be true by those disseminating. It differs from disinformation in the absence of an intention to mislead or harm.

Source: Sessa, M., 2023

[Disinformation]

False information that is deliberately spread to hide the truth, to mislead, deceive or confuse people, especially in political situations.

Source: Goshylyk, N. et al., 2021

[Malinformation]

Genuine information that is shared to cause harm, often by moving information designed to stay private into the public sphere.

Source: Goshylyk, N. et al., 2021

© 2026 RESONANT | Horizon Europe Grant Agreement N. 101132439
Co-funded by the European Union

Map the actors

[Actor]

any individual, group, organisation, or institution involved in or affected by a FIMI or information suppression incident. Actors may be state or non-state entities and can fulfil different roles, such as threat actors, target actors, intermediaries, or responders.

Source: Elaboration in accordance with the RESONANT methodology

[Target]

The intended recipient or object of a FIMI operation, i.e. the entity whose perceptions, attitudes, behaviours, trust, decision-making, or functioning the threat actor aims to influence through coordinated information manipulation.

Source: Elaboration consistent with the EEAS methodology

Assess impact

[Harm]

adverse consequences that affect individuals, communities, institutions, or democratic processes as a result of a FIMI operation. It may manifest through behavioural, social, or institutional changes and serves as an operational indicator for assessing an incident's impact, severity, and response needs.

Source: Elaboration in accordance with the RESONANT methodology

Validate findings

[Community resilience]

the capacity of a community to sustain trust, cohesion, and collective action in the face of FIMI or information suppression. It relies on self-organisation, trusted relationships, institutional support, and the ability to adapt to, resist, and recover from information-related threats.

Source: Elaboration in accordance with the RESONANT methodology

Figure 2 - Brief overview of the key terms mentioned in the RESONANT Handbook.

Co-funded by the European Union

© 2026 RESONANT | Horizon Europe Grant Agreement N. 101132439

2.2 Terms in context

The present paragraph is intended to operationalise the concepts introduced in the glossary by situating them within a coherent and realistic FIMI incident. Although hypothetical, it is informed by patterns, tactics, and behavioural dynamics identified in documented cases of foreign information manipulation and information suppression. By contextualising the terminology, the example scenario facilitates a more consistent understanding of the relationships between the concepts and their practical application in the identification, analysis, and assessment of FIMI incidents.

Practical example: Illustrative FIMI scenario

Ahead of a national election in a European country, a diaspora community becomes the focus of a coordinated information campaign. A set of cloned news websites, social media accounts, and messaging channels begins circulating claims that a diaspora organisation is linked to foreign extremist groups and is influencing domestic politics. At the same time, verified information published by community associations and local institutions receives reduced visibility, is repeatedly reported to platforms, and is accompanied by targeted online harassment of community leaders. Within this environment, different types of content circulate simultaneously: some actors knowingly fabricate and amplify false claims, while others unknowingly share misleading material. Legitimate public statements and event announcements are pushed into private channels or suppressed through coordinated reporting and intimidation. The combined effect is a fragmented information space in which trust in sources, institutions, and even within the community itself is progressively weakened.

The following table provides a comprehensive overview of the terms used in the context of the Handbook, as interpreted in the example given above.

Term	Practical manifestation in the illustrative FIMI scenario
FIMI	Coordinated campaign targeting a diaspora community ahead of elections using cloned media sites, coordinated social media accounts, harassment, and suppression of legitimate content to shape perceptions and weaken trust.
Disinformation	Fabricated articles and posts falsely claiming the diaspora organisation is linked to extremist networks, deliberately created and disseminated to damage credibility and influence public opinion.
Misinformation	Users unknowingly sharing fake articles or manipulated images, believing them to be legitimate, unintentionally amplifying false narratives.
Information Suppression	Coordinated reporting of legitimate posts, algorithmic down-ranking of verified content, harassment of community leaders, and pressure leading to withdrawal into private channels.

© 2026 RESONANT | Horizon Europe Grant Agreement N. 101132439
Co-funded by the European Union

Term	Practical manifestation in the illustrative FIMI scenario
Narrative	Repeated storyline that the diaspora organisation is linked to foreign extremist groups, reinforced across fake articles, posts, and manipulated visuals to delegitimise the community.
Observable	Cloned news articles, viral social media posts, coordinated hashtags, manipulated images, and platform moderation actions (takedowns, visibility restrictions).
Actor	Foreign state-linked operators, anonymous social media accounts, diaspora organisations, journalists, civil society actors, platforms, and public authorities involved in or affected by the incident.
Target	Diaspora community and organisations directly exposed to manipulation; broader public indirectly influenced by the narratives.
Harm	Self-censorship, intimidation, reputational damage, reduced visibility of legitimate content, fragmentation of trust, and weakened civic participation.
Community resilience	Use of trusted organisations and channels, cooperation with institutions, recognition of manipulation patterns, and partial restoration of trust and participation.

Table 1 - Glossary contextualisation table.

2.3 Main legal framewors



Figure 3 - Timeline of the main legal pillars, relevant for the Handbook

The concepts and practices described in the previous sections do not operate in a legal or regulatory vacuum. FIMI and information suppression incidents may involve online platforms, media service providers, advertisers, public authorities, journalists, civil society organisations, and individual users. Depending on the nature of the incident, different legal and co-regulatory instruments may establish obligations for these actors and provide mechanisms through which affected persons and organisations can obtain information, report content or conduct, challenge decisions, and seek redress. The applicable framework and response mechanism will depend on the actors involved, the type of service, the nature of the content or conduct, the harm produced, and the Member State concerned.

Co-funded by the European Union

© 2026 RESONANT | Horizon Europe Grant Agreement N. 101132439

2.3.1 Digital Services Act (Regulation (EU) 2022/2065, Digital Services Act)

The Digital Services Act (DSA) is particularly relevant where a FIMI or information suppression incident unfolds through an online intermediary service, such as a social network, search engine, hosting service, or online marketplace. It establishes procedural obligations for service providers and gives users greater transparency and control over decisions affecting the content and services they access.

From the perspective of users, consumers, and affected organisations, relevant safeguards include:

- **Transparency of platform rules.** Users should be able to understand the terms and conditions governing content moderation, account restrictions, advertising, and the use of automated or algorithmic systems.
- **Mechanisms for reporting illegal content.** Platforms should provide accessible procedures through which users and organisations can notify content that they consider illegal. The reporting mechanism is particularly relevant where a FIMI incident involves threats, unlawful harassment, impersonation, incitement, or other forms of content prohibited by applicable law. Disinformation or manipulative content is not necessarily illegal in itself, and its legal treatment will depend on the circumstances.
- **Information concerning moderation decisions.** Where content is removed, restricted, demonetised, or made less visible, or where an account is suspended or terminated, the affected user should receive an explanation of the decision. This can help identify whether the restriction resulted from platform rules, a legal obligation, coordinated reporting, or an automated moderation process.
- **Complaint and redress mechanisms.** Users should be able to challenge certain platform decisions through an internal complaint system. Additional avenues may include out-of-court dispute settlement, complaints to the competent Digital Services Coordinator[4], and judicial proceedings.
- **Transparency of advertising and recommender systems.** Users should be able to recognise advertising, identify the actor on whose behalf it is displayed, and receive information about the main parameters used to target or recommend content. These safeguards may be relevant when investigating political advertising, micro-targeting, coordinated amplification, or the reduced visibility of reliable information.
- **Protection from manipulative interfaces and practices.** The DSA addresses interface designs that may deceive or manipulate users or impair their ability to make informed choices. It also establishes additional protections in areas such as profiling-based advertising, the protection of minors, and transactions conducted through online marketplaces.

In an information suppression investigation, the DSA can be relevant both to the content that is disseminated and to the processes through which legitimate information is removed, down-ranked, demonetised, or otherwise restricted. The platform's notification, statement of reasons, complaint record, and response to reports may themselves constitute important observables for documenting the incident.

1 https://digital-strategy.ec.europa.eu/it/policies/dsa-dscs

© 2026 RESONANT | Horizon Europe Grant Agreement N. 101132439
Co-funded by the European Union

2.3.2 European Media Freedom Act (Regulation (EU) 2024/1083, European Media Freedom Act)

The European Media Freedom Act (EMFA) addresses the functioning of the internal market for media services and seeks to strengthen media freedom, pluralism, and editorial independence. Its relevance to users and communities is mainly systemic, by seeking to maintain the conditions under which citizens can access a plurality of independent and reliable sources of information.

Relevant safeguards concern, among other matters:

- access to pluralistic and editorially independent media content;
- the protection of editorial independence;
- safeguards for journalists, journalistic sources, and confidential communications;
- transparency concerning media ownership;
- the independence and stable functioning of public-service media;
- transparency and fairness in the allocation of state advertising;
- the relationship between media service providers and very large online platforms;
- the ability of users to exercise greater control over the configuration of devices or interfaces through which media content is accessed.

The restriction of independent journalism, the intimidation or surveillance of journalists, discriminatory distribution practices, opaque changes to media visibility, and interference with editorial decisions may reduce the plurality and quality of information available to the public. The EMFA contributes to support a European media environment in which access, visibility, and editorial independence are safeguarded.

For the purposes of the RESONANT methodology, the EMFA can support the assessment of whether an incident affects only one actor or piece of content, or whether it forms part of a wider pattern that undermines media pluralism, access to trustworthy information, or the ability of targeted communities to participate in public debate. The Regulation expressly links pluralistic and independent media with informed democratic participation and resistance to disinformation and foreign information manipulation.

2.3.3 Code of Conduct on Disinformation (2025)

The Code of Conduct on Disinformation complements the legal framework, particularly the DSA, by establishing commitments for participating online platforms, advertising actors, fact-checkers, civil society organisations, and other signatories. Although it is not a law in the strict sense, the Code of Conduct represents a crucial step towards the active involvement of online providers. Its main areas include the demonetisation of disinformation, transparency of political advertising, the reduction of manipulative behaviour, user empowerment, fact-checking, and access to data for research.

From the perspective of users and communities, the Code may contribute to:

- improved access to contextual and reliable information;
- clearer identification of political or issue-based advertising;
- tools for recognising manipulated or misleading content;
- reduced use of fake accounts, bots, coordinated amplification, and other deceptive practices;
- greater visibility and use of fact-checking;
- support for media and information literacy;
- increased transparency concerning the implementation of signatories' commitments.

© 2026 RESONANT | Horizon Europe Grant Agreement N. 101132439

The Code should nevertheless be distinguished from directly enforceable individual rights. Its commitments do not necessarily give a user an autonomous right to demand that a particular item be labelled, removed, restored, or fact-checked. It can instead provide a benchmark for assessing the measures adopted by participating actors and for identifying gaps between public commitments and the response observed in a specific incident. The DSA also recognises the role of codes of conduct as possible measures for addressing systemic risks associated with disinformation and manipulative or abusive activities.

3. How FIMI Works: TTPs, Behavioural Patterns and Social Impact

This chapter aims to explain how FIMI operates by moving from coordinated information environments to observable behavioural patterns and broader social dynamics, presenting the framework for assessing how these effects develop across individual, community and civic-democratic levels.

3.1 From isolated content to coordinated environments

FIMI and information suppression cannot be understood through the assessment of individual posts, articles, videos, or claims alone. A piece of content may be false, misleading, selectively framed, or even factually accurate while still serving a manipulative function within a broader campaign. What matters is not only what is said, but how narratives are introduced, repeated, adapted, amplified, and circulated across different information spaces. FIMI campaigns' purpose is often to influence what becomes visible, credible, contested, or risky to express. Moreover, coordination does not necessarily imply that every actor is centrally controlled. Different actors may perform complementary functions, including narrative creation, reframing, amplification, cross-posting, reputational targeting, or the redirection of audiences towards less transparent channels.

A simplified campaign trajectory may involve several recurring phases:

© 2026 RESONANT | Horizon Europe Grant Agreement N. 101132439
Co-funded by the European Union

Narrative seeding 	A claim, allegation, symbolic event, or emotionally resonant frame is introduced into the information environment. *E.g.: A post claims that a new public policy will deliberately disadvantage a specific diaspora community.*
Reframing and distortion 	Existing facts, public appearances, institutional links, or political events are selectively interpreted in order to produce suspicion, antagonism, or mistrust. *E.g.: Unrelated statements and past events are selectively presented as evidence of a wider policy of discrimination.*
Amplification 	A claim, allegation, symbolic event, or emotionally resonant frame is introduced into the information environment. *E.g.: A post claims that a new public policy will deliberately disadvantage a specific diaspora community.*
Cross-platform movement 	Narratives may move between open and semi-closed spaces. A campaign may begin in language-specific channels, private groups, or alternative media before reaching more visible platforms. Conversely, highly visible platforms may be used to direct users towards opaque channels where content is less easily scrutinised. *E.g.: The narrative spreads from public platforms to private groups and alternative media, then returns to wider social media.*
Reinforcement 	Repeated exposure, coordinated framing, and the circulation of apparently independent but convergent messages can reshape the perceived credibility, relevance, or social acceptability of a narrative. *E.g.: Repeated exposure through apparently independent sources makes the narrative increasingly familiar, credible and socially accepted.*

Table 2 - Simplified outline of a possible disinformation campaign.

This logic can be described through the concept, introduced above, of Tactics, Techniques and Procedures, or TTPs. **Tactics** refer to the strategic objective pursued, such as dividing a community, delegitimising a public figure, or weakening trust in institutions. **Techniques** are the mechanisms used to achieve that objective, including distortion, hashtag hijacking, manufactured consensus, impersonation, or cross-platform amplification. **Procedures** are the concrete ways in which these techniques are implemented in a specific campaign and context.

The purpose of TTP-based interpretation is to enable analysts to organise and compare observable behaviours. Relevant questions include: Are similar narratives emerging repeatedly? Are messages synchronised or reusing the same language? Are particular accounts or channels systematically reinforcing one another? Is the narrative moving across platforms with different functions? Is the campaign directed towards a specific community, civic actor, or information space?

Co-funded by the European Union

© 2026 RESONANT | Horizon Europe Grant Agreement N. 101132439

Content analysis remains necessary to understand a narrative, its claims, its target, and the framing through which it operates. However, content-based analysis alone cannot determine whether a pattern constitutes coordinated manipulation, exactly as, in turn, behavioural signals are not sufficient in isolation. The RESONANT approach therefore combines content, coordination, contextual, and impact-related observations in order to support the identification of patterns of sustained informational pressure and better distinguish it from legitimate democratic freedom of expression.

Not every intense, polarised, or emotionally charged online discussion indicates FIMI. A controversial event, a rapidly trending hashtag, sharp rhetoric, or political disagreement may emerge through legitimate and spontaneous public debate. A pattern becomes more concerning when several indicators converge over time: synchronised activity across apparently unrelated accounts; repeated or highly similar phrasing; a stable division of roles between accounts, channels, or platforms; identifiable cross-platform trajectories; and amplification practices that create an artificial appearance of consensus or widespread concern.

These elements should be assessed collectively and in context. No single indicator is diagnostic on its own. The purpose is not to judge opinions or political positions, but to identify whether the conditions of visibility, trust, participation, or expression are being manipulated in ways that may produce pressure on a defined community or civic actor.

Practical example: coordinated smear campaign targeting Iranian-German diaspora actors

A case documented by RESONANT illustrates how a coordinated information environment may operate. A network of pseudonymous accounts on X circulated repeated accusations against Iranian-German civil society figures, portraying legitimate public, academic, and policy engagement as evidence of alignment with the Iranian regime. The campaign relied on emotionally charged language, protest-related hashtags, synchronised posting, and repeated formulations that created an appearance of broad grassroots concern.

In this example, X functioned as the public-facing layer of the operation, while links and references redirected users towards anonymous Telegram channels containing longer and less verifiable accusations. The campaign did not rely exclusively on a single demonstrably false statement. Its manipulative force derived from the combination of reputational reframing, coordinated amplification, hashtag visibility, platform redirection, and the accumulation of suspicion within a politically sensitive diaspora environment.

This example shows why FIMI identification requires the reconstruction of relationships between content, timing, platforms, and amplification practices. The next sections examine how these environments may translate into social impacts and observable behavioural adaptations within affected communities.

© 2026 RESONANT | Horizon Europe
Grant Agreement N. 101132439
Co-funded by the European Union

3.2 Social impact framework

The significance of a coordinated information environment does not lie only in its visibility, reach, or technical sophistication. It lies in its capacity to alter the conditions under which individuals and communities can safely express themselves, trust others, cooperate, and participate in public life.

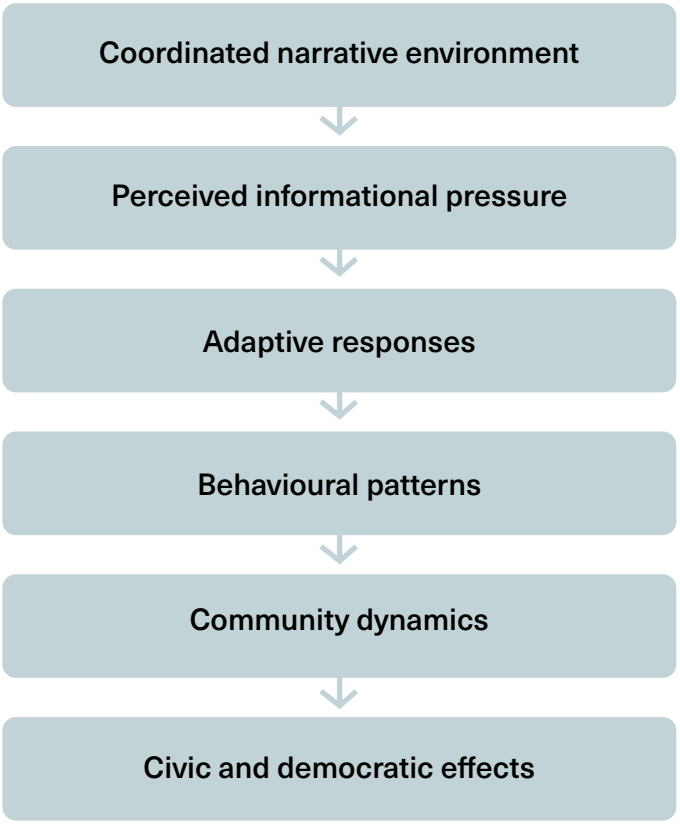


Figure 4 - Analysis of the impact of coordinated narratives on social dynamics.

FIMI can produce effects at different levels. For the purposes of the Handbook, the RESONANT Social Impact Framework distinguishes among three analytical levels:

- *Individual* – effects on specific persons and their rights, behaviour and well-being.
- *Community* – effects on groups, relationships, trust and collective participation.
- *Civic-democratic* – effects on public debate, democratic participation, social cohesion and institutional trust.

This structure builds on the macro–meso–micro inventory developed within RESONANT[3]: the micro level concerns individuals and fundamental rights; the meso level concerns diasporas, collective rights, association and assembly; and the macro level concerns states, democracy and social cohesion. Further RESONANT research, detailing the behavioural and societal effects of information suppression targeting the selected diaspora communities[4], translates these levels into a three-tiered typology of individual, community/group-based, and civic-democratic harms.

Level	What may be affected	Examples
Individual (Micro)	Rights, behaviour and well-being	Reputation; privacy; psychological pressure; self-censorship; withdrawal
Community (Meso)	Trust, cohesion and collective agency	Fragmentation; internal monitoring; closed networks; collective stigmatisation
Civic-democratic (Macro)	Public debate and democratic participation	Reduced civic participation; distorted public debate; media pluralism; institutional distrust

Table 3 - Summary table of the differences between the categories of the Social Impact Framework.

3 RESONANT Project – Deliverable "D1.2 - Baseline report".

4 RESONANT Project – Deliverable "D3.4 - Report on Diaspora communities' case studies: the social and human rights law perspective on the effects of information suppression".

© 2026 RESONANT | Horizon Europe Grant Agreement N. 101132439

The levels should be understood as interconnected rather than isolated. An individual may withdraw from public discussion because of perceived risk; if similar responses become widespread, they may reduce interaction within a community; if this pattern persists, it may affect the community's ability to participate in public debate or engage with institutions.

Practical example: a journalist or activist repeatedly exposed to harassment may reduce their public presence (individual). Other community members may consequently avoid publicly supporting them, producing reputational distancing and weaker solidarity (community). If similar behaviour affects a broader group of journalists or civic actors, participation and pluralism may be affected (civic-democratic). Reputational distancing and weaker solidarity reflect two of the community and relational effects introduced earlier in this chapter, and rarely occurs through a single mechanism.

3.3 Observable behavioural patterns

Behavioural patterns provide the main observable link between a potential FIMI case and social impact. The work carried out by the RESONANT Consortium through the lens of the Behavioural Analysis[5] identified recurring responses among diaspora communities, including changes in how people keep themselves informed, the sources they trust, how they communicate, with whom, and how this affects their participation in public life. These patterns are considered as adaptive responses to perceived risk environments; they are not, per se, evidence of manipulation. The relevance of a behavioural pattern observed increases when it is repeated, temporally tied to an observed information environment, shared by several members of a community, or supported by other contextual or operational evidence.

Behavioural pattern	What it may indicate	What to observe
Strategic silence	Avoidance of public expression because of perceived risk	Reduced expression on specific topics; selective silencing
Selective withdrawal	Reduced participation in discussions or platforms	Disappearance from public conversations; reduced activity
Trust recalibration	Shift towards different sources or trusted networks	Changing information sources; increased reliance on specific intermediaries
Micro-network reliance	Retreat into smaller, more controllable information spaces	Increased use of closed/private channels; reduced cross-group interaction
Self-censorship	Modification of behaviour to avoid perceived consequences	Avoidance of topics, opinions, platforms or public activities

Table 4 - Summary table of selected examples of behavioural patterns observed in RESONANT.[6]

5 RESONANT Project – Deliverable "D3.2 - Report on Behavioural analysis of case studies on diaspora communities".

6 Those listed in Table 4 are the behavioural patterns, amongst those observed by RESONANT and in particular in D3.2, which the Stakeholder Board deemed to be the most relevant and most robustly justifiable. Other observed patterns were deemed to fall outside the scope of this Handbook and were excluded because they were not sufficiently characteristic of this specific problem or could not be detected using robust methodological procedures. For the sake of completeness, the patterns observed but excluded here include the following: polarisation, high engagement / virality, presence of misinformation/ disinformation, hate speech, bot or automated activity, general distrust.

© 2026 RESONANT | Horizon Europe Grant Agreement N. 101132439
Co-funded by the European Union

Additional patterns have been identified during a process of stakeholder engagement. Among those patters defensive fragmentation, anticipatory compliance, participatory fatigue and reputational distancing may be taken into account where sufficient contextual evidence is available. They should be treated cautiously, since some are difficult to distinguish from ordinary political disagreement, organisational fatigue or other external factors.

The interpretation of behavioural patterns should also consider protective factors. Strong community networks trusted local organisations, reliable institutional support, media literacy and access to alternative sources of information may reduce the effects of informational pressure. The absence of visible withdrawal does not necessarily indicate the absence of FIMI; conversely, the presence of withdrawal does not necessarily indicate its success. Behaviour must therefore be interpreted dynamically, taking account of both pressures and resilience mechanisms.

3.4 From individual behaviour to social dynamics

Individual adaptations become more significant when they are repeated, shared and mutually reinforcing, when they recur across a group, persist over time and affect relationships, communication practices or collective participation. RESONANT Research shows how strategies that initially serve as individual coping mechanisms can gradually become collective patterns.

The chain of consequences outlined above (Figure 4) moves from informational pressure to individual behavioural adaptations, then to recurring patterns capable of shaping social and community dynamics, and finally to effects of civic and democratic significance. This progression is, however, not automatic: a behavioural pattern does not necessarily result in harm at the community level. Whether it does depend on recurrence, duration, scope, intensity, stabilisation and the broader context.

The following table presents a set of dynamics observed within RESONANT research. Such dynamics can be observed in real-world contexts and can provide a bridge between individual behaviour and broader social impact.

Social dynamic	Description	Practical manifestation
Internal monitoring and self-regulation	Members become cautious about what others say or share	Avoidance of controversial subjects; informal policing of acceptable speech
Reduced civic participation	Individuals or organisations participate less in public, political or civic activities	Reduced activism, public events, media engagement or political mobilisation
Chilling effects	Fear or anticipated consequences discourage the exercise of rights	Individuals refrain from expressing opinions or associating publicly

Co-funded by the European Union

© 2026 RESONANT | Horizon Europe Grant Agreement N. 101132439

Social dynamic	What it may indicate	What to observe
Social isolation of target groups	Targeted individuals or groups become increasingly disconnected from wider networks	Reduced visibility, fewer collaborations and weaker access to institutional or civic spaces
Normalisation of avoidance	The point at which protective behaviour becomes socially embedded	Silence becomes perceived as the normal and safer way to participate
Erosion of cross-community dialogue	A stage that may precede full fragmentation	Reduced interaction between groups weaken mutual understanding and cooperation even where the groups continue to share the same physical or digital spaces
Community fragmentation	Increasing separation between subgroups and weakening of shared communication spaces	Political, generational or ideological groups increasingly communicate separately

Table 5 - Social dynamics and related manifestation.

Practical example: a diaspora community may initially show a small number of individuals avoiding public political discussions. If the pattern is short-lived and confined to a few individuals, the evidence for a broader social effect is weak. If, over several months, increasing numbers of members move political discussion into closed groups, avoid interactions with other factions and stop participating in public events, the situation may represent an emerging community-level dynamic. If this behaviour becomes normalised and community organisations lose the ability to organise collective activities or communicate with institutions, the impact has moved beyond individual adaptation.

The same progression may occur in relation to civic participation. A small number of individuals withdrawing from public debate does not necessarily affect democratic participation. A persistent pattern affecting journalists, activists, candidates, election observers or community leaders during an election period may have substantially greater significance.

This distinction is important because scale and intensity are separate dimensions. A small group may experience a very strong behavioural effect, while a larger group may experience a weaker effect. Both dimensions should therefore be assessed rather than assuming that a larger affected population automatically represents greater severity.

© 2026 RESONANT | Horizon Europe Grant Agreement N. 101132439
Co-funded by the European Union

3.5 Impact assessment

This section provides an operational framework to assess when observed behavioural patterns and social dynamics become socially significant and may require further analysis or action. For the purposes of this manual, the term "impact" is not considered synonymous of visibility, engagement or reach. High visibility may increase exposure and escalation potential, but it does not necessarily mean that an operation has produced significant social harm. Conversely, a low-visibility campaign may produce severe effects if it targets a vulnerable group, persists over time or causes substantial behavioural change. Social impact concerns the observed or reasonably foreseeable consequences of informational pressure for individuals, communities and civic-democratic participation. The assessment therefore brings together three dimensions:

1. *Confidence in the evidence* – how well the observed pattern is supported;
2. *Severity of the social impact* – how strongly and extensively behaviour, relationships or participation are affected;
3. *Dissemination and contextual factors* – elements that may increase the scope, persistence or urgency of the impact.

The following table illustrates the three levels of impact that are taken into account within the context of the RESONANT project.

Severity Level	Scope	Typical Characteristics	Illustrative Indicators
Low	Individual or localised	Limited, short-lived effects; minimal or reversible behavioural change	Isolated withdrawal; temporary silence; no spillover beyond a small group
Medium	Community / group	Sustained or repeated patterns affecting a defined group; observable constraints on participation or expression	Fragmentation within a community; persistent self-censorship; shift to closed networks; barriers to access or engagement
High	Systemic / civic	Widespread or escalating effects; significant constraints on rights, participation, or public discourse; potential or actual offline consequences	Large-scale chilling effects; cross-platform suppression; widespread disengagement; impact on civic processes or public order

Table 6 - Table summarising the three levels of impact and their characteristics.

© 2026 RESONANT | Horizon Europe Grant Agreement N. 101132439

As previously mentioned, these levels should be understood as connected but distinct. The presence of an individual-level effect does not automatically imply community-level impact, and community-level fragmentation does not necessarily produce systemic democratic effects. The transition should be assessed through observable evidence. Within each level, practitioners should consider the following dimensions:

- *Scale* – how widespread is the effect? (e.g. a single individual, a specific community group, or multiple communities across a region)
- *Intensity* – how strongly has behaviour or participation changed? (e.g. reduced posting frequency versus complete withdrawal from public life)
- *Duration* – is the effect short-term, persistent or escalating? (e.g. a few days following a single incident versus months of sustained change)
- *Reversibility* – is the effect likely to disappear if the pressure stops, or has it become normalised? (e.g. a return to previous behaviour once harassment subsides versus a lasting shift in how a community engages publicly)
- *Vulnerability* – does the effect concern individuals or groups with heightened exposure or fewer possibilities for protection? (e.g. undocumented individuals, LGBTQIA+ diaspora members, or first-generation activists with limited institutional support)
- *Spillover* – does the effect extend to other groups, institutions or offline environments? (e.g. from one diaspora association to allied civil society organisations, or from online harassment to reduced attendance at in-person events)
- *Temporal sensitivity* – does the effect coincide with elections, referenda, protests or other politically sensitive events? (e.g. a spike in harassment in the weeks preceding a national election)
- *Protective factors* – are trusted actors, community organisations, institutional capacity, media literacy or reliable information available to mitigate the impact? (e.g. an active local fact-checking network versus an information environment with no visible counter-voices)

In addition to such dimensions, there are further factors to take into account when assessing the impact of a FIMI event or information suppression.

- *Intensity and reversibility*. Ask how strongly the observed behaviour has changed and whether the effect is temporary or becoming normalised. A limited-scale pattern may still be significant where behavioural change is intense, persistent or difficult to reverse.
- *Evidence triangulation.* Assess whether the observed impact is supported by different types of evidence, including platform observations, behavioural data, community feedback, expert assessment and qualitative evidence. Avoid drawing conclusions from isolated signals or single sources.
- *Context matters.* Interpret the same behavioural signal in light of its context, including the affected population, duration, scale, surrounding events and protective factors. Similar patterns may have very different significance depending on the circumstances in which they occur.
- *Emerging risk and escalation watch.* Consider whether limited or early signals show a credible trajectory towards broader or more persistent effects. Recurrence, increasing scale, vulnerability, spillover and declining protective capacity may justify closer monitoring even where significant impact has not yet been established.
- *Democratic participation.* Consider whether the observed effects concern elections, referenda, protests or other politically sensitive periods, and whether they affect journalists, candidates, activists, minorities, civil society organisations or election observers. Timing can substantially increase the significance of otherwise limited effects.
- *Social impact is not legal harm.* A behaviour or social dynamic may have significant consequences without constituting a legal violation, particularly in cases of “lawful but harmful” content. Conversely, identifying an impact does not by itself establish a breach of rights or legal responsibility.

The analysis provided sets out a structured framework for interpreting FIMI signals without treating individual indicators as diagnostic elements. The next chapter will build on this foundation by defining how signals can be systematically collected, corroborated and assessed as evidence.

© 2026 RESONANT | Horizon Europe
Grant Agreement N. 101132439
Co-funded by the European Union

4. From Signals to Evidence: The streamlined version of the Detection Methodology

While Chapter 3 sets out the behavioural patterns and social dynamics that can signal FIMI-related pressure. Chapter 4 turns patterns into a documented, assessable case. The process has two stages.

The process has two stages. Section 4.1 covers the first decision a practitioner makes: whether an observation is worth opening as a case, or whether it should be set aside for now. Section 4.2 covers the Incident Sheet, the record used to document a case once it has been opened, gather the relevant evidence and assess its quality and record observable impact. Step by step, with a worked example, the section also offers guidance to apply the methodology.

4.1 Open/Park incidents

Before a pattern becomes a documented case, whoever is applying the methodology, e.g. a researcher, a journalist, a public authority, a civil society organisation, a security practitioner, or a representative of an affected community, must first decide whether it is appropriate to open one. This is the Open/Park gate: a brief preliminary check that precedes actual case analysis and prevents a case from being built on evidence that is not yet operationalisable or sufficient.

In order to decide, five questions can guide this preliminary check:

1. **Risk assessment.** Would opening this case, and documenting it further, expose myself, a source, or communities involved or other individuals to a risk that outweighs the value of the analysis? If so, the case cannot be opened until the risk is managed. This question asks for a judgement made upfront, before any documentation begins: is the risk of looking into this case at all manageable, or not? It is a different question from how that risk gets managed once a case is actually open.

Co-funded by the European Union

© 2026 RESONANT | Horizon Europe Grant Agreement N. 101132439

Practical example: when documenting the case is itself a risk

A journalist is told, off the record, that a specific individual within a diaspora association has been receiving threatening messages tied to their public advocacy. The information is credible, but the community is small, and any detailed written record, even an internal one, could make the source identifiable if it were ever leaked or subpoenaed. The journalist holds off on opening a full case, and instead first agrees with the source on what can safely be recorded and shared before documenting anything further.

2. **Alternative hypothesis test.** Is there a non-FIMI explanation — i.e., satire, ordinary political criticism, coincidence — that accounts for what I am observing at least as well? If so, it would be advisable to park the case.

Practical example: when documenting the case is itself a risk

A journalist is told, off the record, that a specific individual within a diaspora association has been receiving threatening messages tied to their public advocacy. The information is credible, but the community is small, and any detailed written record, even an internal one, could make the source identifiable if it were ever leaked or subpoenaed. The journalist holds off on opening a full case, and instead first agrees with the source on what can safely be recorded and shared before documenting anything further.

3. **Evidence threshold.** Do I have at least two distinct signals pointing to the same pattern, even if not yet independently verified? A single striking data point is not enough, and this includes a spike or shift with no earlier point of comparison: without something to measure it against, it is not really a second signal, only an unexplained number.

Practical example: a case built on a single source

A representative of a diaspora community receives a screenshot from a fellow member showing a Telegram group where members are being told to stop posting about an upcoming rally, alongside vague warnings about “consequences.” No other member of the group has come forward, and there’s no way to confirm who sent the original messages or whether the screenshot is complete. Before raising it further, the community representative tries to reach two other members of the same group to see whether they recognise the same pressure.

© 2026 RESONANT | Horizon Europe Grant Agreement N. 101132439
Co-funded by the European Union

Until a second source confirms the pattern, the case should be parked.

Practical example: a spike with nothing to compare it to

A security practitioner's monitoring tool flags a sudden jump in negative mentions of a diaspora cultural association on X: three times the volume from the previous week. It looks alarming, but nobody has ever tracked what a normal week of mentions looks like for this association, so there is no way to tell whether three times an almost-invisible baseline is a real signal or just noise around an otherwise quiet account.

Until there is something to compare it against, this counts as one unexplained data point, not two distinct signals and the case should not be opened.

4. **Deconfliction check.** Is this case already open and being tracked elsewhere? If so, opening a duplicate record adds no value; flag it as a contribution to the existing case instead of opening a new one.

Practical example: someone else is already on it

A public authority starts building a case around a cluster of accounts targeting a diaspora media outlet, only to learn through a partner network that a fact-checking organisation has been tracking the same accounts for two weeks and already has a more developed evidence trail.

Rather than opening a parallel case, the authority reaches out to contribute its observations to the existing one, avoiding duplicated effort and a fragmented record.

5. **Positionality check.** Do I have direct knowledge of the community involved, or someone who does, to interpret what I am seeing? Without contextual knowledge the case cannot be properly analysed; it is strongly recommended to park it until that knowledge is available.

Practical example: recognising the limits of an outside view

A researcher, with no personal connection to a particular diaspora community, notices what looks like a coordinated effort to discourage the community from engaging with a local integration programme. Without knowledge of the community's internal dynamics, the researcher cannot tell whether this reflects outside pressure or an ordinary, long-standing internal disagreement about the programme.

© 2026 RESONANT | Horizon Europe Grant Agreement N. 101132439

Before opening a case, the researcher reaches out to a trusted contact within the community to help interpret what is being observed.

Answering these five questions is a quick, largely qualitative exercise, and the record it produces should be agile: a working title for the case, one decision – Open or Park – a one-line rationale, and a timestamp. The rationale is where the analyst summarises the decision following the 5 questions. For example, "Open – second independent source confirms the pattern, no ordinary explanation fits as well" or "Park – single source only, no way yet to rule out an ordinary explanation."

A parked case is kept in the record and can be reopened as soon as a second source appears, a point of comparison is established, or the alternative explanation stops holding up. The gate exists to protect the credibility of every case that does move forward: a case built on a weak basis risks mistaking an ordinary event for something more serious.

4.2 Incident Sheet

Once the preliminary check is performed and the case is open, it is possible to start the analysis through the use of the Incident Sheet: the working record used to document what was observed, who it affected, how strong the evidence is, how severe the impact is, and what safeguards were applied while handling it. Its standardised structure enables comparison across cases and subsequent independent review.

Each section covers a different aspect. The narrative summary and target fields allows to collect information about what happened and to whom, in plain terms. The evidence quality and impact severity fields guide the analysis on the sources and the effects reach, and support the choice of the action pathways. Additional fields represent a further layer of context sensitivity, ethical safeguards and responsible information handling. The severity modifiers situate the case within its wider context: recurrence, scale, reversibility and other relevant factors that can support a solid analysis. Furthermore, responsible data handling is governed by a Traffic Light Protocol (TLP), establishing the degree of dissemination of the case analysis. Finally, the Guardrails checklist documents which safeguards, from data minimisation to the protection of vulnerable groups, were actually applied while handling the case.

Field: Incident ID and title

How to fill:
Unique code + short title
(e.g., RSN-2025-012 — Platform X takedown spike)[7]

Field: Country and local context

How to fill:
Country, region, language(s) implicated.

Field: Time window of the incident

How to fill:
Start dd/mm/yyyy – End dd/mm/yyyy

7 The code could be structured, as in this example, using an acronym or a series of letters that refer to the project or context in which the case is being analysed. 'RSN' in this instance is an abbreviation of 'RESONANT'. It may be useful to include the year and a case identification number (case no. 12 of 2025) as well as a few keywords to identify the case immediately. In any event, it is important to assign a unique code to each case. Within the same organisation or in the work of the same analyst, it is advisable to use a consistent and uniform approach to ensure clear case naming conventions.

© 2026 RESONANT | Horizon Europe
Grant Agreement N. 101132439
Co-funded by the European Union

Field: One-line narrative summary

How to fill:
Use this field to provide a concise, factual synopsis of the incident as observed at the time of assessment. Summarise what was observed, the tactic or technique apparently involved, where it occurred (platform/channel), who/what appears to be targeted (if evident), and why it is relevant in terms of potential FIMI impact.

Example

"Content asserting that narrative circulated on [platform/channel] via [tactic/technique, e.g. coordinated inauthentic accounts], and during the same window, [observable effect] was recorded, affecting [target]."

Field: Affected targets[8]

How to fill:
Identify:
1. **Primary target(s):** the person, organisation, community, or public group directly targeted by the narrative, activity, or pressure.
2. **Secondary target(s):** if applicable, people or groups indirectly affected, for example because they are associated with the primary target, depend on the same i§nformation environment, or may be discouraged from participating.

Select all applicable categories:
- **Individual(s):** one or more identifiable persons, such as an activist, journalist, researcher, public official, or community member.
- **Specific organisation(s):** a named NGO, media outlet, political organisation, community association, institution, or other collective body.
- **Community or group segment:** a defined community, diaspora group, minority group, linguistic group, or other identifiable social group.
- **Civic actor or sector:** journalists, civil society organisations, election observers, researchers, activists, local authorities, or other actors performing a public or democratic role.
- **General public:** a broad and non-specific public audience affected by the narrative or its consequences.
- **Unclear / not yet identifiable:** use where the available information does not allow the analyst to identify a target reliably.

Field: Observed behavioural and social effects

How to fill:
Use this field to record observable changes in behaviour, participation, trust, or community relations that may indicate the social effects of the incident. No single observable proves that FIMI is present, establishes causation, or justifies attribution. Observables should be interpreted together, over time, and in relation to the relevant narrative, context, and evidence.

For each selected observable, indicate whether it is:
- **Observed directly:** supported by primary evidence, such as documented statements, participation data, interviews, or traceable public actions;
- **Reported:** described by a reliable affected person, organisation, or source, but not independently verified;
- **Inferred:** a reasonable analytical interpretation based on several cues, which should be recorded cautiously.

8 See Annex – Glossary.

Caveat: never record an individual's proper name in this field. Use a role-based or generic descriptor instead (e.g. "a diaspora community leader," "a local journalist.") A written record naming a real person creates exposure that cannot be undone if it is ever disclosed or accessed without authorisation.

© 2026 RESONANT | Horizon Europe Grant Agreement N. 101132439

		Observed directly	Reported	Inferred
A. Individual or small-group behavioural adaptations	**Strategic silence:** avoidance of public expression on specific topics because speaking is perceived as risky.			
	Selective withdrawal: reduction or cessation of participation in a discussion, platform, organisation, or public activity.			
	Trust recalibration: a shift in the sources, people, communities, or channels considered reliable or safe.			
	Reputational distancing: public or visible avoidance of association with a targeted person, group, or organisation.			
	Reduced civic participation: decline in engagement in public, political, professional, or civic processes, including meetings, events, consultations, advocacy, or elections.			
B. Community and relational effects	**Fragmentation:** breakdown of a shared information or communication space into more isolated groups with limited exchange or trust.			
	Internal monitoring or self-policing: increased self-regulation, mutual scrutiny, or concern about what can safely be said within a community.			
	Erosion of solidarity: reduced willingness to publicly support, defend, or associate with targeted individuals or groups.			
	Chilling effects: a broader climate in which people limit expression or participation because they perceive risk, intimidation, or possible repercussions.			

© 2026 RESONANT | Horizon Europe Grant Agreement N. 101132439
Co-funded by the European Union

		Observed directly	Reported	Inferred
	Barriers to representation or public voice: reduced visibility or participation of a community, organisation, or civic actor in public debate, media, research, or institutional engagement.			
	Delegitimisation of civic actors: sustained framing of journalists, activists, observers, or NGOs as suspicious, foreign-influenced, or destabilising. Very relevant for democratic resilience and election observation contexts			

Important:
- Use strategic silence when an individual or small group avoids speaking on a specific issue.
- Use chilling effects when the pressure appears to affect the wider environment and discourages expression or participation beyond the directly targeted person.
- Use selective withdrawal for disengagement from a specific space or activity.
- Use reduced civic participation where the effect extends to wider public, political, or civic engagement.
- Use fragmentation where there is evidence of separation between groups or information spaces.
- Use erosion of solidarity where people remain present but are less willing to visibly support one another.

Methodological note: The complexity of reality blurs the boundaries between analytical categories and their manifestations. Since interpretation is inherently subjective, the standpoint adopted should be that of the specific community concerned. Therefore, the incident reporter should either have direct knowledge of the community or, if not, consult a member. This judgement rests on interpretation, not direct measurement, so wherever possible, corroborate it with other types of evidence, such as platform data, behavioural indicators, or independent community feedback.

Field: Evidence quality level[9]

How to fill:
Low: the assessment relies on a single source or observation and has not yet been independently corroborated.
Medium: the assessment is supported by two sources, or by one highly reliable source together with additional consistent indicators or case-specific evidence.
High: two or more independent and reliable sources confirm a consistent pattern within the same observation period.

How do I decide?

9 Evidence quality rates how solid the sourcing behind a case is, independently of how serious the case appears to be. A single source counts as low. Two independent sources, or one strong source backed by supporting details, count as medium. High evidence quality needs two or more independent sources showing a consistent pattern within the same observation window. This rating answers one question only — can the observation be trusted? — and is combined separately with impact severity to decide what happens next.

© 2026 RESONANT | Horizon Europe Grant Agreement N. 101132439

Evidence Quality Level

Level	Meaning	Select this level when...
Low — initial signal	The observation is plausible but not yet sufficiently confirmed.	You have one source, one screenshot, one report, or one limited observation. The information may be useful for monitoring, but alternative explanations remain possible.
Medium — corroborated signal	The observation is supported, but some uncertainty remains.	You have two sources that are not fully independent, or one strong and traceable source supported by additional observations such as timestamps, archived links, screenshots, platform traces, or consistent narrative cues.
High — strongly corroborated pattern	The observation is supported by several independent and consistent sources.	Two or more independent sources, or clearly distinct forms of evidence, confirm the same pattern within the relevant time window. The evidence is traceable and no major contradiction remains unresolved.

Field: Impact severity

How to fill:
Low
Medium
High

How do I decide?

Impact Severity

Level	Meaning	Select this level when...
Low — limited impact	Effects are localised, short-lived, and likely to be reversible.	The incident affects one person or a small group; there is limited disruption; any withdrawal, silence, or reputational effect appears temporary; there is no clear spillover beyond the immediate setting.
Medium — sustained community impact	Effects are repeated or persistent and affect a defined community, organisation, or group.	There are observable barriers to expression, access, trust, association, or participation; a community segment is affected over time; people shift towards closed channels, reduce engagement, or show sustained signs of pressure.
High — widespread civic or rights-related impact	Effects are widespread, escalating, difficult to reverse, or linked to serious rights, safety, or democratic consequences.	The incident affects multiple groups or a broad public sphere; it creates large-scale chilling effects; it significantly constrains participation or public debate; it is linked to credible safety concerns, offline harm, or serious disruption around civic processes.

© 2026 RESONANT | Horizon Europe Grant Agreement N. 101132439
Co-funded by the European Union

Important:
A high-visibility incident is not automatically high severity.
A case can be low evidence but high severity where there is a credible indication of significant potential harm.
A case can be high evidence but low severity where the impact remains localised and reversible.
Do not assign "High" only because the target belongs to a diaspora, minority, or vulnerable group. Consider whether the circumstances create a demonstrably greater risk of harm.

Field: Severity modifiers[10]

How to fill:
For each of the following modifiers, please mark: **Not observed / Possible / Present / Not applicable**

		Not observed	Possible	Present	Not applicable
Recurrence	Has the same pattern appeared repeatedly over time?				
Scale	How many people, groups, organisations, or platforms are affected?				
Reversibility	Are the effects likely to disappear quickly, partly persist, or remain after content is removed or corrected?				
Duration	Are the effects temporary, repeated, or sustained over a longer period?				
Stabilisation	Are withdrawal, silence, mistrust, or restrictive practices becoming normal within the affected group?				
Target vulnerability	Does the target face context-specific exposure that may increase harm?				
Spillover effects	Does the impact extend beyond the initial target?				
Offline implications	Are there signs of real-world consequences?				
Proximity to democratic events	Mark this field when the incident occurs close to elections or electoral campaigns; demonstrations, referenda, protests, or major political events; other high-visibility civic processes.				

Important:
- One isolated or uncertain modifier should usually be recorded but should not automatically change the base impact severity level.
- Consider increasing the rating of impact severity level by one level where **two or more modifiers are clearly present** and point in the same direction.
- Do not move directly from Low to High without documenting a clear rationale.

10 Severity modifiers are contextual factors that adjust how seriously a case is treated, without changing how solid the underlying evidence is. They include how widely the effect has spread (scale), how long it has lasted or whether it is still escalating (duration), whether it is likely to fade once the pressure stops or has become entrenched (reversibility), whether it has spread beyond the original target to other groups or offline settings (spillover), and whether those affected have fewer resources or protections available to them (vulnerability).

© 2026 RESONANT | Horizon Europe Grant Agreement N. 101132439

Field: Tiering Evidence quality × Impact severity

How to fill:
Matrix for action pathways

Severity \ Evidence	Low	Medium	High
Low	**Monitor** Keep the case under routine observation; set a date to check again.	**Monitor** Seek corroboration of the pattern with a second source and set a date to check again.	**Mitigate** The evidence is solid even if the impact still looks limited; prepare mitigation steps now, to be ready if severity rises.
Medium	**Monitor** Brief the team internally on what has been observed, and set a date to check again.	**Mitigate** Notify the relevant internal and external stakeholders. Prepare mitigation measures.	**High-priority** Escalate for senior review and coordinate the response with partner organisations.
High	**Mitigate** The apparent impact is serious but the evidence is still thin; corroborate it while preparing mitigation measures.	**High-priority** Escalate for senior review and synchronise the response across partner organisations.	**High-priority** Escalate for senior review and coordinate an immediate response with partner organisations.

Table 7 - Evidence x Severity Matrix.

Monitor (green) – The case should be kept monitored. It should be checked and updated periodically, with internal briefing if something changes. No outside communication, no mitigation action.

Mitigate (yellow) – The case moves beyond watching. A practitioner gathers more sources, prepares proportionate steps such as community outreach or a cautious internal alert and keeps a written account of the reasoning. This action pathway encourages to consider lighter, resilience-focused responses.

High-priority (red) – The case needs the involvement of a senior expert. Evidence and reasoning could be shared with colleagues or partner organisations and any relevant public or institutional actor.

Field: Guardrails

How to fill:
Tick all the GRs that you applied:

☐ **GR-01 — Data minimisation.** Where I processed data, I limited collection and use to what was necessary for this assessment and used aggregated or metadata-only information wherever feasible.

© 2026 RESONANT | Horizon Europe Grant Agreement N. 101132439
Co-funded by the European Union

- ☐ **GR-02 — Lawful basis and informed consent.** Where identifiable persons, participants, or personal information were involved, I documented the applicable lawful basis and obtained informed consent where required.
- ☐ **GR-03 — Pseudonymisation and identifiers.** Where personal or potentially identifying information was retained, I pseudonymised records and excluded direct identifiers unless their use was strictly necessary and authorised.
- ☐ **GR-04 — Secure storage and access control.** Where data or case materials were collected or retained, I stored them in an approved secure environment and restricted access to authorised users only.
- ☐ **GR-05 — Provenance and reproducibility.** For the evidence used in this assessment, I recorded source provenance, collection details, and analytical steps sufficient to enable review and reproducibility.
- ☐ **GR-06 — Baselines and observation windows.** Where the assessment relied on comparison over time or on quantitative indicators, I declared the relevant baseline, observation window, and any material limitations.
- ☐ **GR-07 — Independent corroboration.** Before treating a signal as substantiated, I sought corroboration from independent sources or documented why independent corroboration was not available.
- ☐ **GR-08 — Attribution caution and confidence.** Where attribution was considered, I distinguished observable evidence from inference, stated the level of confidence, and did not present attribution as established without sufficient validated evidence.
- ☐ **GR-09 — Retention and deletion.** Where data or case materials were retained, I applied the relevant retention period and deletion or disposal procedure.
- ☐ **GR-10 — Classification and sharing rules.** Before sharing incident-related information, I applied the relevant Traffic Light Protocol (TLP) classification, handling, and sharing rules.
- ☐ **GR-11 — Controlled environments and synthetic data.** Where exercises, testing, or training activities were conducted, I used controlled environments and synthetic datasets wherever feasible.
- ☐ **GR-12 — Vulnerable-group safeguards.** Where the incident involved vulnerable individuals or groups, I applied enhanced safeguards to minimise exposure, re-identification, and the risk of further harm.

Field: Traffic Light Protocol (TLP)

How to fill:
Use this field to decide who may receive or further share the incident record and its annexes.
The TLP label is not a measure of incident severity or evidence quality.

Red / Amber+Strict / Amber / Green / Clear.
(This label applies to the incident record and its annexes at the time of assessment. It may be revised if the sensitivity of the information changes).

© 2026 RESONANT | Horizon Europe Grant Agreement N. 101132439

Traffic Light Protocol (TLP)[11]

TLP Label	Who may receive or share the information?	Select this level when...	Example
TLP:RED	Only the specifically named recipients. No further sharing.	Any wider disclosure could create a substantial privacy, reputational, safety, or operational risk.	The record contains identifiable information about a threatened activist, a confidential source, or a person at risk of retaliation.
TLP:AMBER+STRICT	Only members of the recipient's own organisation. It must not be shared with external partners, clients, or stakeholders.	The case requires internal assessment, legal review, or management action, but external circulation could expose individuals, evidence, or institutional activity.	An internal incident assessment contains non-public evidence, possible identifying details, or unresolved allegations.
TLP:AMBER	Members of the recipient's organisation and external actors who need the information in order to act or protect themselves.	Selected partners, stakeholders, or service providers need the information for mitigation, safeguarding, or coordinated response, but wider circulation would create unnecessary risk.	A pseudonymised early-warning note is shared with relevant project partners, support organisations, or competent authorities.
TLP:GREEN	A defined trusted community, including peers and partner organisations within that community. It must not be shared through public channels.	The information is useful for awareness, learning, or coordination and no longer creates a significant individual or operational risk if shared within a trusted community.	An anonymised case summary or pattern analysis circulated among researchers, NGOs, journalists, or trained practitioners.
TLP:CLEAR	Anyone. Public sharing is permitted.	The information is public, verified, sufficiently redacted where necessary, and presents minimal foreseeable risk of harm or misuse.	A public case study, published methodological example, or public guidance note with no sensitive annexes.

Field: Caveats

How to fill:
Reasons for caution; alternative explanations.

Field: Analyst / Reviewer

How to fill:
Initials or names, dates.

Field: Annexes

How to fill:
Screenshots, links, documents.

11 Traffic Light Protocol (TLP) is a four-label scheme that specifies how far recipients may redistribute information. TLP: RED – only the people present in the exchange; no further sharing. TLP: AMBER – shareable only within your own organisation and to clients/stakeholders on a need-to-know basis; AMBER+STRICT = only inside your organisation. TLP: GREEN – shareable within the community (e.g., partner network), not on public channels. TLP: CLEAR – freely shareable/publishable (subject to copyright).

© 2026 RESONANT | Horizon Europe Grant Agreement N. 101132439
Co-funded by the European Union

4.3 Step by step guidance to the Incident Sheet

In order to facilitate the use of the Incident Sheet, this section provides step-by-step guidance, together with explanatory examples.

Step 1 – Identify and delimit the incident

Begin with the Incident ID and title, country and local context, and time window. Give the case a unique identifier and a short title that allows it to be recognised later. Record the geographical, linguistic and political context, where relevant, and define the period covered by the observation.

The one-line narrative summary should then describe only what is currently known. State what was observed, where it appeared, who appears to be affected, and why the case may be relevant. Avoid conclusions about the identity or intentions of the actor at this stage.

Questions that may guide the reflections are: *What first drew my attention to this case? What can I observe directly, and what am I currently assuming? It is also crucial to assess the context: What was happening when the content or activity appeared? Is the activity connected to an election, protest, diplomatic event, crisis or other sensitive situation?*

For example, saying: *"A coordinated campaign on X smearing members of the Iranian community in Germany, appeared across the platform during the same week" is preferable to a more conclusive statement such as "A foreign actor launched a coordinated campaign to silence the community."* The second formulation contains an attribution and causal conclusion that the evidence may not yet support.

Step 2 – Identify who is affected

The Affected targets field asks who is directly and indirectly affected. Start with the primary target, the one person or group the most affected, then consider whether the effects extend to associated individuals, organisations or wider groups called secondary target. *Is there a specific person, community, institution or information space that appears to be affected?*

The Incident Sheet distinguishes between individuals, organisations, communities or group segments, civic actors and the general public. This distinction is important: the same content can have very different implications depending on who is targeted.

For example, a defamatory narrative concerning a private individual may remain an individual-level incident. The same narrative directed repeatedly at journalists, activists or a diaspora organisation may produce wider effects such as reputational distancing, self-censorship or reduced civic participation.

Do not assume that membership of a vulnerable group automatically makes an incident high severity. Vulnerability is a modifier that must be considered together with the actual circumstances of the case.

© 2026 RESONANT | Horizon Europe Grant Agreement N. 101132439

Step 3 – Record behavioural and social effects

The Observed behavioural and social effects section is central to the RESONANT approach. Chapter 3 explains that behavioural changes are among the most useful observable indicators of social impact, but that no individual indicator is diagnostic of FIMI. Among the patterns presented (e.g. strategic silence, selective withdrawal, trust recalibration, etc...), select those supported by the available information and mark each as directly observed, reported, and inferred. This distinction is important because an interviewee reporting that people are afraid to speak is different from observing a documented reduction in participation or from an analyst inferring a chilling effect from several indirect signals requires further caution.

The relevant question is: "What changed, and what evidence do we have that the change actually occurred?", and not yet: "Who caused the change?". This distinction helps prevent premature attribution.

Step 4 – Rate the quality of the evidence

The Evidence quality field assesses how well the observation is supported.

- *Low*: one source or observation, without independent corroboration.
- *Medium*: two sources, or one highly reliable source supported by additional consistent evidence.
- *High*: two or more independent and reliable sources confirming a consistent pattern within the same observation period.

Repeated reposts of the same original source do not constitute independent corroboration. Many accounts repeating the same claim does not automatically increase evidence quality if they derive from one source. It is crucial to ask: *Do independent sources confirm the same observation? Which evidence is direct, and which is based on secondary reporting or interpretation?*

Where sources disagree, record the disagreement in Caveats and avoid assigning a high rating without further verification. When uncertainty remains, it is preferable to select the lower level and schedule a reassessment. This reflects the evidence-corroboration logic developed in RESONANT.

Step 5 – Assess impact severity

The Impact severity field asks how significant the observed or reasonably foreseeable effects are. A first assessment can be made using the three levels scale:

- *Low*: localised, limited and short-lived effects;
- *Medium*: repeated or sustained effects within a defined community;
- *High*: wider effects on participation, rights or the information environment, including credible risks of offline harm.

The initial rating should then be tested against the severity modifiers. Ask whether the pattern:

- recurs over time;
- affects multiple people, groups, organisations or platforms;
- is reversible or likely to persist;
- lasts for a significant period;
- becomes normalised within the affected group;
- concerns a particularly vulnerable target;
- produces spillover effects;
- has offline implications;
- occurs close to an election, referendum, protest or other significant civic event.

© 2026 RESONANT | Horizon Europe Grant Agreement N. 101132439
Co-funded by the European Union

These modifiers should be considered together. One uncertain modifier should normally be recorded without changing the impact severity rating. Two or more clearly present modifiers pointing in the same direction may justify increasing the severity by one level. A direct jump from Low to High requires a clear rationale.

Importantly, *visibility is not severity*. A widely viewed post may have limited social impact, while a relatively small campaign may have severe consequences if it causes sustained withdrawal from civic participation within a vulnerable community.

Step 6 – Apply the action pathway

The Incident Sheet combines evidence quality and impact severity to indicate the appropriate next step.

This specific approach is discussed in detail in section 5.1 "Decision thresholds".

Step 7 – Record safeguards, handling and uncertainty

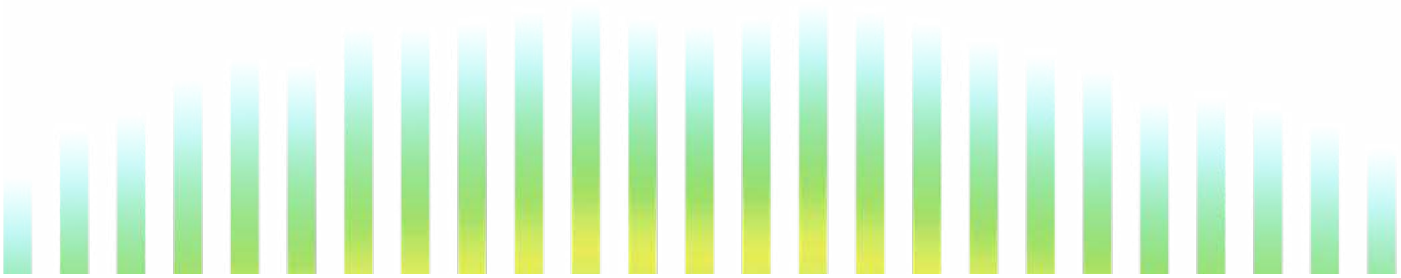
The Guardrails section records whether data minimisation, lawful processing, pseudonymisation, secure storage, provenance, independent corroboration, attribution caution and vulnerable-group safeguards have been applied.

These safeguards are crucial: investigating FIMI can itself expose people to additional risks.

The Traffic Light Protocol (TLP) field concerns the handling and sharing of the incident record. It is not an indicator of severity or evidence quality. It provides instruction on how openly the information contained in the case analysis may be shared.

Finally, use Caveats to record alternative explanations, missing information, conflicting sources and assumptions. The Analyst/Reviewer field creates accountability for the assessment, while Annexes should contain the material necessary to reproduce or review the analysis, such as screenshots, links and documents.

The completed Incident Sheet, correctly filled out, becomes a concise analytical record that can support monitoring, further investigation or handover to another actor. It does not establish attribution or legal responsibility by itself. Observed behavioural and social consequences do not automatically constitute legal harms and attribution requires separate assessment. The following section presents an example of a real-life case, on the base of which the relative Incident Sheet has been filled out.



Co-funded by the European Union

© 2026 RESONANT | Horizon Europe Grant Agreement N. 101132439

4.4 Practical example

The following is an example useful to illustrate how the methodology can be applied to incidents with different characteristics. It has been selected from the case corpus developed with RESONANT[12].

Case example 1 – The "Chancellor's Act" narrative

The example concerns the long-running conspiracy theory that German Chancellors must sign a secret "Chancellor's Act" in Washington before taking office. According to the narrative, the alleged document binds Germany to the United States and demonstrates that the country lacks genuine sovereignty. The narrative resurfaced prominently in Russian-language media and online channels in late 2024 and early 2025. RESONANT Research identifies Russian and pro-Kremlin media, anonymous blogs and other platforms as important dissemination infrastructures.[13]

The case is particularly useful for the Handbook because it demonstrates that high visibility and repetition do not automatically translate into high social impact. The principal effect identified was the longer-term reinforcement of distrust and cynicism towards democratic institutions.

Incident Sheet field	Completed assessment
Incident ID and title	RSN-EX-01 — "Chancellor's Act" conspiracy narrative
Country and local context	Germany; also circulated internationally. Primary languages: Russian and German. The narrative was particularly relevant to audiences sceptical of NATO, the United States and German sovereignty.
Time window	Long-running narrative; renewed amplification documented particularly in **December 2024–January 2025.**
One-line narrative summary	Russian-language anti-western narrative repeatedly amplified across online platforms.
Affected targets	**Primary**: segments of the German and international public, particularly conspiracy-oriented, nationalist and Eurosceptic audiences. **Secondary**: German democratic institutions and perceptions of German sovereignty.
Observed behavioural and social effects	**Observed directly:** repeated circulation and engagement with the narrative. **Reported/inferred:** reinforcement of distrust towards German and Western institutions and normalisation of the conspiracy narrative. No clear evidence of broad behavioural withdrawal or institutional change.

12 RESONANT Project – Deliverable "D2.2 – Compendium of TTPs and countermeasures".
13 RESONANT Project – Deliverable "D2.2 – Compendium of TTPs and countermeasures".

© 2026 RESONANT | Horizon Europe Grant Agreement N. 101132439
Co-funded by the European Union

Incident Sheet field	Completed assessment
A. Individual/small-group adaptations	**Trust recalibration:** possible increased reliance on alternative/conspiratorial information sources. **Strategic silence/withdrawal**: not established.
B. Community/relational effects	Reinforcement of closed ideological information environments and distrust towards mainstream institutions. Broader fragmentation **is possible but not sufficiently demonstrated** by the available evidence.
Evidence quality	**High**. Existence, recurrence and dissemination of the narrative (multiple independent sources and platforms document the pattern).
Impact severity	**Medium**. The narrative is persistent and recurrent and contributes to institutional distrust, but documented offline or systemic consequences are limited.
Severity modifiers	**Scale**: Present; **Duration**: Present; **Stabilisation**: Possible; **Spillover**: Possible; **Offline implications**: Not established; **Proximity to democratic events**: Possible/context-dependent - the amplification window (December 2024–January 2025) coincided with the collapse of the governing coalition and the run-up to Germany's snap federal election (23 February 2025), but the narrative itself is a long-running anti-Western theme not explicitly framed around the election.
Tiering / action pathway	**Mitigate**: the persistence of the narrative justifies continued monitoring and proactive contextualisation, while the absence of clear high-severity consequences argues against disproportionate intervention.
Guardrails	GR-01 — Data minimisation; GR-05 — Provenance and reproducibility; GR-07 — independent corroboration; GR-08 — Attribution caution and confidence; GR-09 — Retention and deletion; GR-10 — Classification and sharing rules.
TLP	**Green / Clear,** the record contains only public information and no sensitive operational material.
Caveats	Repetition is not equivalent to independent corroboration. Engagement metrics demonstrate exposure, not belief or behavioural impact. Attribution to Russian actors is supported by Resonant D2.2's analysis of the information ecosystem, but individual dissemination does not establish direct control.
Analyst / Reviewer	*Name/code of the researcher/user that fills out the template.*
Annexes	*Screenshots, URLs and copies of relevant articles/posts; historical sources cited by the narrative; independent fact-checking material.*

© 2026 RESONANT | Horizon Europe Grant Agreement N. 101132439

The case illustrates how, even when the narrative is clearly observable and highly persistent, the social impact assessment should nevertheless remain cautious. The available evidence supports a finding of repeated exposure and reinforcement of pre-existing distrust but does not demonstrate that the campaign caused a specific change in political behaviour. The analysis justifies monitoring and preventive communication without automatically triggering a high-priority response.

5. From Analysis to Action

This Chapter explains further the logic behind the choice of the action pathway resulting from the analysis in the Incident Sheet. Each pathway choice is supported by the combined analysis of the strength of the evidence with the severity of the impact. The pathway indicated when a case should be kept under monitoring, when it requires a response, and when it should be brought to the attention of someone with more authority or experience.

5.1 Decision thresholds

The decision threshold provided in the Incident Sheet facilitates the reflection on the relation between the incident's effects and the response to implement.

Two questions should guide this reflection:

Evidence quality. *How solid is the evidence: a single source, or several independent ones pointing the same way?* A single source, on its own, counts as low. Two independent sources, or one strong source backed by supporting details, count as medium. High evidence quality needs two or more independent sources showing a consistent pattern within the same time window.

Impact severity. *How severe is the impact: a handful of people affected briefly, or a whole community affected over time?* As presented in Chapter 3, a low-severity case is small and short-lived: it touches one person or a very local setting and fades on its own. A medium-severity case is sustained or repeated within a defined community, such as a diaspora group fragmenting, persistent self-censorship, or a shift into closed networks. A high-severity case reaches further: wide effects on participation or rights, suppression that crosses platforms, or a credible risk of offline harm.

© 2026 RESONANT | Horizon Europe Grant Agreement N. 101132439
Co-funded by the European Union

Severity \ Evidence	Low	Medium	High
Low	**Monitor** Keep the case under routine observation; set a date to check again.	**Monitor** Seek corroboration of the pattern with a second source and set a date to check again.	**Mitigate** The evidence is solid even if the impact still looks limited; prepare mitigation steps now, to be ready if severity rises.
Medium	**Monitor** Brief the team internally on what has been observed, and set a date to check again.	**Mitigate** Notify the relevant internal and external stakeholders. Prepare mitigation measures.	**High-priority** Escalate for senior review and coordinate the response with partner organisations.
High	**Mitigate** The apparent impact is serious but the evidence is still thin; corroborate it while preparing mitigation measures.	**High-priority** Escalate for senior review and synchronise the response across partner organisations.	**High-priority** Escalate for senior review and coordinate an immediate response with partner organisations.

Table 7 - Evidence x Severity Matrix.

Signal (green).

The case should be kept monitored. It should be checked and updated periodically, with internal briefing if something changes. No outside communication, no mitigation action.

Mitigate (yellow).

The case moves beyond watching. A practitioner gathers more sources, prepares proportionate steps such as community outreach or a cautious internal alert and keeps a written account of the reasoning. This action pathway encourages to consider lighter, resilience-focused responses.

High-priority (red).

The case needs the involvement of a senior expert. Evidence and reasoning could be shared with colleagues or partner organisations and any relevant public or institutional actor.

Practical example: reading two accounts of the same pattern.

An analyst notices that members of a diaspora association have stopped posting about a contested policy. On its own, this is one source and a low-severity pattern: Monitor. A week later, interviews with two independent community contacts describe the same withdrawal, plus new reports of members leaving a shared messaging group. The evidence is now medium, the pattern has spread within the community, and the group has a documented vulnerability profile. Severity moves to medium, and the case shifts to Mitigate: closer documentation, a cautious internal alert, and consideration of a support-oriented response to the community itself.

© 2026 RESONANT | Horizon Europe Grant Agreement N. 101132439

5.2 Escalation logic: how to change the level of response

Moving a case to a higher tier of the action pathways is not regulated by pre-determined criteria. Three elements shape the decision: the strength of the case itself, the role of the analyst, and the risk that acting, or not acting, carries for the people involved.

Escalation follows the evidence. A case moves up when new information changes the underlying evidence quality or severity rating. It does not move up because time has passed or because a situation feels urgent, and a single dramatic signal is not enough.

Escalation depends on role. What a researcher can responsibly do is not what an institutional partner or a public authority can do. A researcher documenting a pattern may reasonably move a case to Mitigate on their own judgement. A High-priority case calls for a second reviewer and, where relevant, coordination with the partners or authorities best placed to act (see Section 6.4 for role-specific guidance).

A research centre or NGO. Escalation stays largely within the organisation's own structure. A High-priority case goes to a senior analyst or the team lead for a second reviewer. Anything that reaches beyond the organisation, is issued only once more than one person has reviewed the evidence and agreed on the wording. The purpose is not to create unnecessary procedural burden, but to ensure that appropriate checks are in place to identify and correct potential errors before information is made public.

A school or educational institution. School staff cannot be expected to have specialist expertise in conducting a FIMI assessment. What matters is that the institution has a clear referral pathway to the person already responsible for such matters, such as the head teacher or safeguarding lead. Once a case is classified as high priority, it should be referred to the relevant local education authority or designated ministry contact point, rather than addressed through an independent public response by the school.

An individual citizen. Journalists, activists and other citizens acting independently may not have access to colleagues, second reviewers or institutional support. For them, a high-priority classification does not trigger internal escalation; it signals the need to pause and seek assistance from an appropriate specialist body, such as a press-freedom organisation, a digital-rights group or a designated institutional contact point. Proceeding alone may create significant risks, therefore is strongly discouraged.

Escalation is reversible. A case may be de-escalated whenever new information changes the initial assessment. If an additional source does not corroborate the original evidence, a community contact clarifies that an observed pattern results from factors other than external pressure, or the initial signal proves to be isolated, the case should be reassigned to a lower tier and the Incident Sheet updated to document the reasons. Treating de-escalation as a normal and expected part of the assessment process ensures that classifications remain proportionate to the available evidence and are revised when no longer justified.

© 2026 RESONANT | Horizon Europe Grant Agreement N. 101132439
Co-funded by the European Union

The principle of proportionality underpins the entire process. A response that exceeds what is justified by the available evidence and the assessed severity may itself cause harm: it may discourage legitimate activity, unnecessarily expose individuals who were not otherwise at significant risk, or undermine confidence in the assessment. Ensuring that each response remains proportionate to the assigned priority tier protects both the people and communities the Handbook is intended to support and the integrity of the assessment process.

5.3 When NOT to act

It is important to stress that acting is not automatically the safer choice. A response initiated prematurely or on the basis of uncorroborated evidence may be as harmful as inaction. Practitioners should therefore consider at least three circumstances in which pausing, seeking further verification or refraining from intervention may be the more appropriate course.

Weak or single-source evidence. A single striking post, one account of a pattern, or an isolated data point does not justify moving beyond Monitor. Acting on such evidence risks producing a false positive, for example, by treating unrelated or legitimate activity as coordinated interference, disrupting a legitimate network, or wrongly implicating an actor. The appropriate response to a weak signal is continued observation while seeking additional, independent corroboration.

Misattribution risk. Naming a responsible actor before the evidence supports it can do lasting damage, both to the person or group wrongly named and to the credibility of the analysis itself. Where attribution is uncertain, a response should address the observed behaviour and its effects, and leave the question of responsibility open, exactly as Section 7.1 sets out.

Amplification and overreaction. Publicising a case, even for the purpose of raising awareness, may unintentionally amplify the narrative or pressure being addressed. Public statements, media engagement and widely circulated internal alerts should therefore be preceded by a careful assessment of their likely benefits and the associated risk of amplification.

Restraint does not mean inaction. In many of these situations, the most useful response is support: reaching the affected community through trusted channels, offering accurate information, or connecting individuals with organisations able to offer assistance. These resilience-building measures can often begin earlier than a public or disruptive response because they generally create fewer risks to rights, safety and trust, even while the evidence is still being gathered. They contribute directly to community resilience, as defined in Section 2, by helping to restore trust, participation and a sense of security within the affected community.

Practical example: choosing not to publish.

A journalist collects a single account describing a smear campaign against a diaspora activist. Publishing immediately would raise awareness, but the source has not been corroborated, the activist has not been consulted, and premature exposure could deepen the harm instead of limiting it. The more proportionate path is to seek a second source, reach out to the activist directly, and consider a resilience-oriented response, such as connecting the activist with a support network, while the case stays in the Mitigate tier.

Co-funded by the European Union

© 2026 RESONANT | Horizon Europe Grant Agreement N. 101132439

6. Counteraction in Practice

Identifying a FIMI campaign is just the first step. An effective response requires selecting actions that are proportionate to the evidence available, appropriate to the context, and compatible with democratic principles and fundamental rights. Poorly designed, delayed or disproportionate responses may unintentionally reinforce manipulation, increase public distrust or expose targeted communities to additional risks.

This chapter translates the action pathways resulting from the analysis into practical guidance. Drawing on the methodological work, behavioural evidence, legal analysis and operational recommendations produced across the project's deliverables[14], it presents a set of principles and practical options that can support decision-makers, practitioners, journalists, researchers and civil society organisations when responding to FIMI and information suppression.

Rather than prescribing a single response model, the chapter illustrates different forms of counteraction, their advantages and limitations, and the contexts in which each is most appropriate.

6.1 Principles of effective response

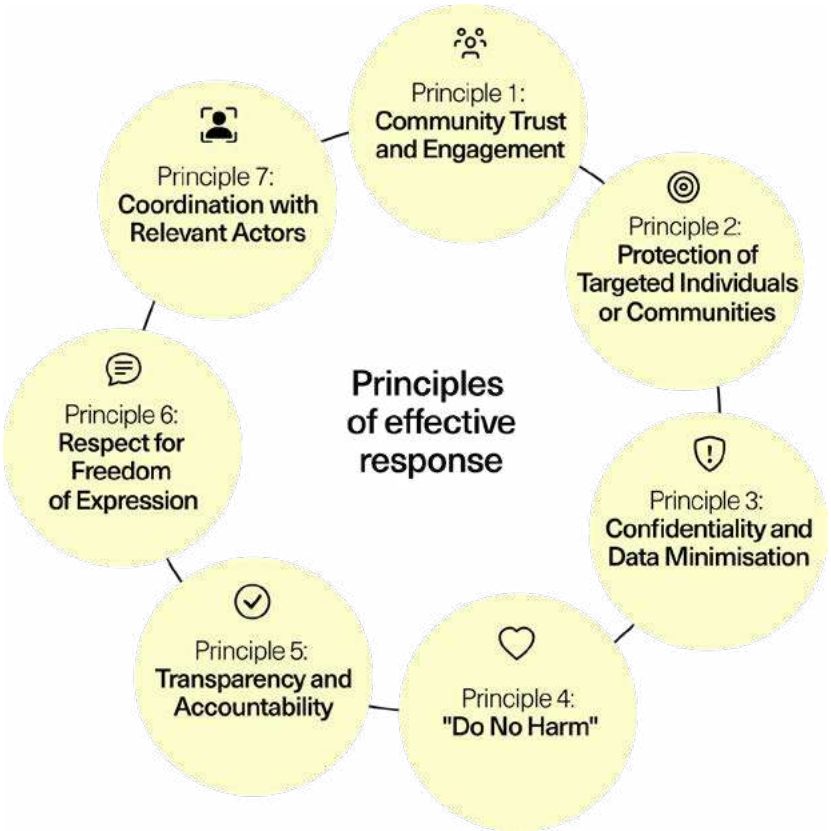


Figure 5 - Principles of effective response.

14 RESONANT Project – Deliverable "D2.2 – Compendium of TTPs and countermeasures".

© 2026 RESONANT | Horizon Europe Grant Agreement N. 101132439
Co-funded by the European Union

Proportionality, evidentiary grounding and context-sensitivity are the core elements against which an effective counteraction should be calibrated. Throughout the RESONANT project, the behavioural, legal and methodological analyses have consistently shown that inappropriate interventions may unintentionally act as multipliers of the target's vulnerability. Therefore, it is important to identify the most appropriate response for each case.

The following principles for an effective response aim to provide a common framework that can support the design of appropriate interventions:

1. *Community[15] trust and engagement*

   Responses are more effective when they are developed together with the communities they seek to protect. Building trust with affected groups improves situational awareness, facilitates the identification of emerging threats and increases the likelihood that countermeasures will be accepted and supported. Community engagement also helps practitioners understand the cultural, linguistic and social contexts within which manipulation campaigns operate.

2. *Protection of targeted individuals or communities*

   Strictly linked to the principle mentioned above, it is noted that counteraction should prioritise the safety, dignity and well-being of individuals and communities affected by FIMI. Every intervention should seek to reduce exposure to further intimidation, harassment or discrimination. Particular attention should be given to vulnerable groups whose participation in public life may already be constrained by previous experiences of surveillance, marginalisation or political pressure.

3. *Confidentiality and Data Minimisation*

   Counteraction activities frequently involve sensitive information concerning individuals, organisations or ongoing investigations. Information should therefore be collected, processed and shared only to the extent necessary for the specific operational objective. Respecting confidentiality protects individuals, preserves trust and ensures compliance with applicable legal and ethical obligations.

4. *"Do No Harm" Principle*

   Responses should reduce the overall impact of FIMI without creating additional harms. Poorly designed interventions may inadvertently amplify manipulated narratives, increase public attention towards malicious content or expose targeted individuals to further intimidation. Every operational decision should therefore include an assessment of possible unintended consequences before implementation.

5. *Transparency and Accountability*

   Operational decisions should be transparent, proportionate and capable of being explained afterwards. Clear documentation strengthens institutional credibility, facilitates cooperation between organisations and enables independent review where appropriate. Transparency also requires clarity regarding institutional responsibilities and confidence that interventions are supported by sufficiently robust evidence. This principle also prescribes that each organisation should act within its legal competences and clearly understand its responsibilities throughout the response process and that operational measures should be based on reliable and corroborated evidence.

6. *Respect for Freedom of Expression*

   Countering FIMI should never compromise the democratic values it seeks to protect. Measures intended to address manipulation should respect freedom of expression, media freedom and access to information, while recognising that restrictions may only be justified under clearly defined legal conditions. Particular caution is required where the distinction between legitimate political expression, controversial opinions and coordinated manipulation remains uncertain.

7. *Coordination with Relevant Actors*

   FIMI campaigns frequently involve multiple platforms, jurisdictions and societal actors. Effective responses therefore require coordination between organisations possessing complementary expertise and responsibilities. Information sharing, common analytical standards and regular communication improve both the quality of assessment and the effectiveness of countermeasures.

15 RESONANT Project – Deliverable "D2.2 – Compendium of TTPs and countermeasures".

© 2026 RESONANT | Horizon Europe Grant Agreement N. 101132439

6.2 Type of response

No single response will be able to address every manifestation of FIMI. Information manipulation and suppression campaigns can differ significantly in objectives, techniques, targets and expected impacts, requiring responses that can be adapted to different operational contexts. Selecting the most appropriate response requires considering both the characteristics of the campaign and the capabilities of the actors involved.

This section presents four broad categories of response: community-based, media-based, institutional and hybrid. These categories are not mutually exclusive alternatives: complementary approaches can often be combined to produce more effective and sustainable outcomes, providing practitioners with a framework for selecting response strategies that are both operationally feasible and proportionate to the identified risks.

Figure 6 presents the main features of each category of response.

Community-based responses	**Media-based responses**	**Institutional responses**
Objective: Increase resilience	*Objective:* Restore information integrity	*Objective:* Protect rights and enforce applicable rules
Examples: • awareness sessions; • trusted information networks; • community ambassadors; • digital literacy initiatives; • psychosocial support.	*Examples:* *fact-checking* • investigative journalism • explanatory reporting • coordinated debunking • contextualisation.	*Examples:* • investigations • administrative procedures • judicial remedies • DSA mechanisms • GDPR enforcement
Suitable when: • communities experience intimidation; • trust is declining; • manipulation exploits identity divisions.	*Suitable when:* • investigative reporting • fact-checking and verification • public exposure of manipulation techniques • media-literacy and awareness content	*Suitable when:* • evidence indicates significant/sustained harm • legal or institutional mandates are applicable • individuals or democratic processes are affected • coordination or escalation is required
Pay attention to: • avoid amplification and stigmatisation • protect confidentiality and vulnerable individuals • intermediaries involved	*Pay attention to:* • verify evidence • avoid repeating harmful claims • protect sources/targets • consider amplification	*Pay attention to:* • ensure legal mandate • match response to evidence/severity • coordinate authorities • protect rights
Possible actors: • civil society organisations • community leaders and trusted intermediaries • researchers and educators	*Possible actors:* • journalists • fact-checkers • researchers/analysts • civil society	*Possible actors:* • law enforcement • regulators • data protection authorities • courts • electoral bodies

Figure 6 - Main features of each category of response.

© 2026 RESONANT | Horizon Europe Grant Agreement N. 101132439
Co-funded by the European Union

The following table provides an overview of the stakeholders involved, the objectives and the most suitable circumstances in which each type of response could be applied, including hybrid responses, which may incorporate elements of the other three, depending on the specific case to which they are applied.

Response	Main actors	Typical objective	Best suited for
Community	NGOs, diaspora	resilience	intimidation
Media	journalists	information correction	false narratives
Institutional	authorities	enforcement	illegal conduct
Hybrid	multiple actors	systemic response	coordinated campaigns

Table 8 - Table summarising the main features of each response.

The following table summarises the responses provided by the experts of the RESONANT Stakeholder Board when asked to assign the most appropriate type of response to a range of possible effects of FIMI/ information suppression events[16].

	Monitor only	Community-based	Media-based	Institutional	Hybrid
Weak evidence and high risk of amplifying a low-reach narrative	✓				
Targeted harassment, intimidation or reputational attacks against a person or group					✓
A misleading or manipulative narrative is gaining public visibility			✓		
A vulnerable community is showing signs of withdrawal, fear or self-censorship		✓			
Cross-platform coordination appears to affect public discourse or civic participation					✓
There are potential safety, public order, electoral integrity or legal concerns				✓	
The affected group requests support but does not want public exposure		✓			

Table 9 - Most appropriate type of response to a range of examples according to RESONANT Stakeholder Board.

16 The survey was administered to the more than 50 members of the RESONANT Stakeholder Board between 30 June and 9 July 2026. Specifically, the question was No. 5: 'Q5 – Which response type would normally be most appropriate in the following situations?'. The list of situations proposed corresponds to that shown in the table.

© 2026 RESONANT | Horizon Europe Grant Agreement N. 101132439

6.3 Constraints and feasibility

However, a countermeasure that works in theory, in practice may encounter significant obstacles that limit their implementation or reduce their effectiveness. In this context, legal frameworks may provide suitable remedies while remaining difficult to activate in practice because of procedural complexity, fragmented institutional responsibilities or limited resources. Similarly, organisational constraints may prevent timely responses even when sufficient evidence has already been collected.

For these reasons, every response should be evaluated considering its practical feasibility, not just for the theoretical suitability. This section discusses the principal structural, operational, cross-border, and institutional factors that may influence implementation. Understanding these constraints enables practitioners to select realistic courses of action and to anticipate the limitations that may emerge during implementation.

In any case, when assessing the feasibility of a response, the social and cultural dimension must also be taken into account. A response may, in fact, be perfectly viable from a legal, technical and institutional point of view, but it may prove ineffective if there is a lack of trust, if there is a fear of being monitored, if there are language barriers, or if there are no community organisations or credible intermediaries capable of facilitating the collaboration with the affected group.

The following elements emerged clearly during the RESONANT research as critical factors capable of either enabling a response or undermining its effectiveness.

6.3.1 Structural constraints

Structural gaps arise where existing legal or governance frameworks are not designed to address the characteristics of FIMI campaigns. These gaps limit the range of available legal responses and often require policy, educational or community-based measures instead of judicial intervention.

6.3.2 Operational constraints

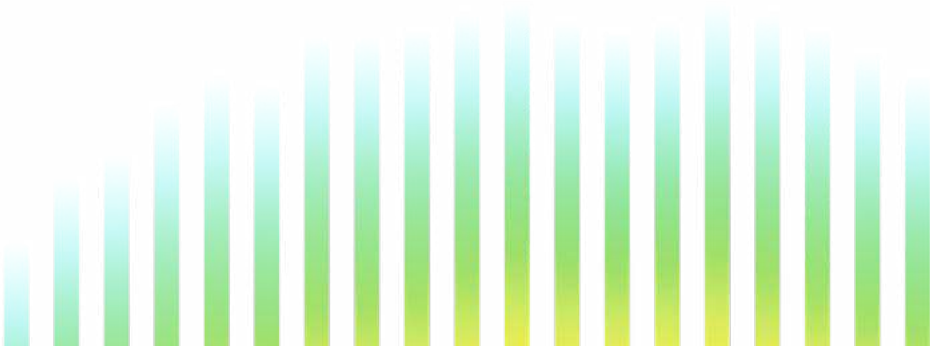
Operational gaps concern the practical application of otherwise existing legal or institutional tools. Even appropriate legal instruments may remain unused or produce delayed outcomes. Practitioners frequently need to complement legal responses with documentation, victim support and community engagement.

6.3.3 Cross-border constraints

Many FIMI campaigns operate simultaneously across multiple jurisdictions, platforms and legal systems. Effective responses often depend on international cooperation. Delays in information exchange or unclear jurisdictional responsibilities may significantly reduce the effectiveness of mitigation measures.

6.3.4 Institutional constraints

Institutional gaps concern the organisational capacity required to implement responses consistently. Different organisations may react inconsistently to similar incidents, creating uncertainty for victims and reducing confidence in institutional responses.



© 2026 RESONANT | Horizon Europe
Grant Agreement N. 101132439
Co-funded by the European Union

The following table provides an overview of the four dimensions of gaps and constraints described. In particular, it shows how these differ in terms of their impact and which stakeholders are involved, either actively or passively.

Constraint category	Main limitations	Impact on countermeasures	Actors implementing the response	Actors primarily affected
Structural	Individual-focused legal frameworks, limited regulation of lawful but harmful content, lack of collective protection	Legal remedies may be unavailable or only partially applicable	EU institutions, legislators, regulators	Diaspora communities, journalists, civil society
Operational	Complex procedures, low legal awareness, evidentiary burdens, delayed responses	Existing remedies remain difficult to activate or ineffective in practice	Courts, law enforcement, DPAs, platforms, NGOs	Victims, community organisations, human rights defenders
Cross-border	Jurisdictional fragmentation, attribution difficulties, limited international cooperation	Responses become slower and less coordinated across countries and platforms	National authorities, EU agencies, international partners	Cross-border communities, investigators, public authorities
Institutional	Limited expertise, fragmented governance, insufficient resources and coordination	Uneven implementation and reduced institutional effectiveness	Public authorities, regulators, security agencies, judicial bodies	Practitioners, reporting communities, civil society organisations
Social and cultural	Low trust in institutions, fear of surveillance or retaliation, language barriers, cultural differences, limited legal literacy, weak community organisation, absence of trusted intermediaries	Even well-designed legal, institutional or technical responses may fail if they are not trusted, understood or accessible to the communities concerned. These factors influence reporting, cooperation with authorities, participation in awareness initiatives and the uptake of available remedies.	Public authorities, civil society organisations, diaspora associations, community leaders, journalists, researchers, victim-support organisations	Diaspora communities, vulnerable individuals, victims of FIMI, local communities and all actors relying on community cooperation

Table 10 - Overview of the four dimensions of gaps and constraints described.

© 2026 RESONANT | Horizon Europe Grant Agreement N. 101132439

The diagram below graphically illustrates what is described in this section.

- Structural constraints define whether an appropriate legal or policy response exists.
- Operational constraints determine whether available tools can be used effectively.
- Cross-border constraints affect coordination across jurisdictions and platforms.
- Institutional constraints determine whether organisations possess sufficient capacity, expertise and resources.

Taken together, these four dimensions, when adapted to the socio-cultural context in which the response is intended to be implemented, determine the feasibility of each response option proposed.

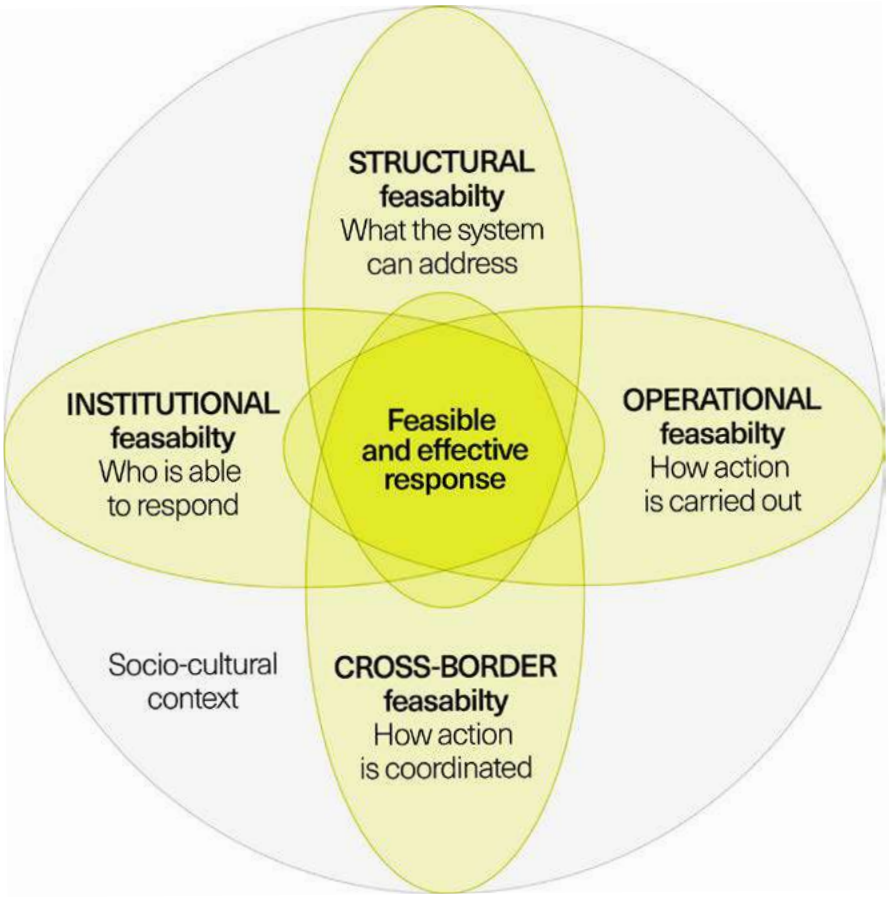


Figure 7 - How the intersection of feasibilities allows an effective response.

6.4 Role-based guidance

Although the principles and response models presented in the previous sections are generally applicable, their practical implementation necessarily depends on the role, responsibilities and capabilities of the actors involved. Public authorities, researchers, journalists, civil society organisations and diaspora communities contribute to countering FIMI in different ways and operate under different legal and organisational mandate and constraints. Practical guidance must therefore recognise these differences while maintaining a coherent overall methodology.

© 2026 RESONANT | Horizon Europe
Grant Agreement N. 101132439
Co-funded by
the European Union

This final section, as illustrated in Figure 8, translates the general framework developed throughout the Handbook into role-specific recommended workflows intended to support day-to-day operational decisions. This is intended to provide practical guidance that can assist different categories of practitioners in adapting the RESONANT methodology to their own professional environments. The workflows presented, validated by the RESONANT Stakeholder Board[17] aims to illustrate the sequence of actions that might be taken by each actor should they encounter, what could be a FIMI event or an act of information suppression.

CITIZENS

1. Pause before sharing or reacting
2. Check the source and date
3. Look for corroboration from reliable sources
4. Save basic evidence if the content may be harmful
5. Avoid engaging directly with suspected hostile actors
6. Report harmful content to the platform
7. Inform a trusted organisation, journalist, moderator or community actor
8. Support the targeted person privately and safely
9. Avoid reposting harmful content, even to criticise it
10. Block or mute abusive accounts
11. Seek help if there are threats, doxxing or safety concerns
12. Protect personal data and avoid sharing screenshots with identifying information

NGOs

1. Assess immediate safety or wellbeing concerns
2. Collect reports from affected individuals with consent
3. Document incidents without overexposing individuals
4. Identify whether the issue is isolated or repeated
5. Consult trusted community members or intermediaries
6. Provide support to the targeted person or group
7. Create safe spaces for discussion
8. Prepare community guidance or awareness material
9. Use trusted messengers rather than public confrontation
10. Avoid naming suspected perpetrators without strong evidence
11. Coordinate with journalists, researchers or fact-checkers
12. Refer to legal, psychological or institutional support where needed
13. Report threats, doxxing or safety concerns to competent actors
14. Monitor chilling effects, withdrawal or reduced participation

17 Stakeholder Board members involved in the survey were asked: "Q10 - According to the methodology, different types of users of the RESONANT Handbook follow different workflows. Do you think the steps described for each category are appropriate? Is the order of the process correct?".

© 2026 RESONANT | Horizon Europe Grant Agreement N. 101132439

JOURNALISTS

1. Assess whether the content has sufficient public relevance
2. Verify the factual claim
3. Verify the source, context and origin of the content
4. Avoid amplifying low-reach content unnecessarily
5. Distinguish between debunking a claim and investigating a campaign
6. Assess whether the case involves harassment, intimidation or target exposure
7. Contact the affected person or organisation where appropriate
8. Consult community or language experts
9. Redact personal data, harmful content or identifying details
10. Contextualise the narrative rather than repeating it
11. Avoid speculative attribution
12. Coordinate with editorial or legal review
13. Include guidance on reliable sources or support resources
14. Monitor backlash after publication

RESEARCHERS

1. Define the analytical question and scope
2. Identify the target community, issue or information environment
3. Collect basic evidence: links, screenshots, timestamps, platforms
4. Distinguish between content, narrative, behavioural patterns and social impact
5. Assess recurrence, scale, duration and stabilisation
6. Seek contextual, linguistic or community expertise
7. Check whether evidence is sufficient or still speculative
8. Apply the evidence/severity logic
9. Assess risk of harm, exposure or amplification
10. Avoid attribution unless supported by a separate validated framework
11. Produce a non-attributive analytical note
12. Recommend monitoring, mitigation or escalation
13. Define a reassessment timeline
14. Apply data minimisation and privacy safeguards

Figure 8 - Workflows for each category of actor analysed, according to RESONANT Stakeholder Board.

The constraints discussed in this chapter demonstrate that responding to FIMI is not a mere matter of selecting the appropriate countermeasure. Effective responses require a careful assessment of the legal, operational, institutional and social context in which they will be implemented, alongside a clear understanding of the potential consequences of intervention. Practitioners, researcher and every actor that may encounter a FIMI event or an information suppression action should therefore adopt a proportionate, evidence-based and context-sensitive approach. It is crucial to balance the need to mitigate harmful activities against the risks of overreaction, misattribution, unnecessary amplification of hostile narratives or unintended impacts on the rights and safety of affected individuals and communities. Considering these factors from the outset helps ensure that countermeasures remain credible, lawful and effective.

© 2026 RESONANT | Horizon Europe Grant Agreement N. 101132439
Co-funded by the European Union

7. Limits, Risks and Misuse

The methodology presented in this Handbook supports analytical assessment and situational awareness. It identifies indicators and patterns of concern, but it cannot independently establish intent, responsibility, or legal accountability, and it does not constitute an attribution framework (see Section 1.2). This section sets out the boundaries of the framework. Section 7.1 covers the methodological limits inherent in an effects-based, behaviourally grounded approach: what the methodology can demonstrate, what it can observe, and the conditions under which its outputs hold. Section 7.2 covers the risks that arise in operational use: misreading organic social behaviour as interference, acting on insufficient evidence, and exposing the people the methodology is meant to protect. These boundaries are conditions of correct use, and every assessment produced with this Handbook should be read against them.

7.1 Methodological Limits

The methodology's outputs are built to support analytical assessment and situational awareness. Attribution, legal qualification, and liability determination fall to competent authorities working under their own evidentiary standards.

Limits of attribution. The methodology measures behaviour, not identity. It defines interference through recurring clusters of TTPs and treats the question of who is behind them as a separate matter. The behavioural patterns in Chapter 3 and the indicators in Chapter 4 show that a community or an information environment is under strain. They do not show who is responsible, whether the pressure is centrally directed, or whether it is intentional. Within the assessment process, attribution can only ever enter as a hypothesis. A dedicated safeguard keeps this restraint in place at every stage, requiring the observed behaviour to be kept separate from any claim about who caused it. The methodology itself does not issue attribution.

Data and platform limitations. The methodology is based on observations, but some relevant behaviour cannot be observed. Much of that behaviour happens in closed or semi-closed spaces. Fieldwork carried out in RESONANT found that fear of infiltration or online exposure pushes discussion into invitation-only channels. Access to platform data compounds the difficulty: experts consulted described researcher access as underdeveloped, the data available as less detailed than before, and the procedures for obtaining it as slower and more complex. Several of the patterns considered in this Handbook take the form of silence and withdrawal, but disengagement generates little data to observe, and an absence of signal can still conceal real harm. Verification also takes longer than harm does to unfold, often days or weeks against hours, and the sustained observation this Handbook recommends depends on a continuity of platform access that current conditions do not reliably provide. The methodology's own validation adds a further limit: it has been tested through a small number of simulated cases and a single real-world round, covering six cases in total, which leaves some geographies and communities underrepresented.

Context dependency. The observed behaviours in this Handbook cannot be interpreted without context. The behavioural research behind RESONANT drew on fifty-eight interviews across six diaspora communities and found that the same visible behaviour can carry opposite meanings depending on

Co-funded by the European Union

© 2026 RESONANT | Horizon Europe Grant Agreement N. 101132439

the context where it occurs. Silence often works as a form of protection. and can coexist with quieter, more situational forms of civic engagement. An analyst unfamiliar with the relevant baseline can easily read protective silence as indifference, or ordinary variation as a meaningful narrowing of public space. The behavioural signals in Chapter 3 can be properly identified only when the analyst has a working knowledge of the community's context, language and channels of communication, and only when that observation continues over time. Finally, context also limits how precisely severity can be assessed. The methodology provides steps and criteria, but evaluating impact, reversibility and vulnerability still require a degree of judgement.

Warning. No single behavioural signal or social dynamic in this Handbook is enough on its own. A striking indicator cannot establish that interference has occurred, identify who is responsible, or justify a response by itself. A finding becomes meaningful once several signals converge, corroborate each other across independent sources, hold up over time, and are read within the context of the community observed.

7.2 Risks of misinterpretation and misuse

This section examines the judgements analysts must make when interpreting and assessing the available data, as well as the potential consequences of errors in that process.

Distinguishing coordination from organic conflict and polarisation. The main interpretive risk is mistaking authentic social behaviour for interference. Genuine grievance, ordinary political disagreement, fatigue within an organisation, and legitimate civic mobilisation can all produce signals that look like informational pressure. Fieldwork for RESONANT found communities fragmenting and retreating for reasons that include pre-existing ideological and generational divides alongside outside pressure. Interference designed well is built to look organic, so an authentic appearance offers no guarantee of an authentic cause. Either error carries a cost: treating organic conflict as coordinated interference pathologises legitimate dissent and burdens the people observed; missing real interference leaves harm unaddressed.

The Handbook is built with this risk in mind. Patterns too ambiguous to distinguish organic from coordinated behaviour were left out of Chapter 3, and none of the signals that remain carry weight on their own. The detection process requires corroboration across at least two independent sources, ideally drawn from different surfaces, within an aligned time window.

Mini-case | Illustrative

An analyst monitoring a diaspora network observes shrinking coalitions, cancelled joint initiatives, and a retreat into smaller, trusted circles, a pattern documented in RESONANT fieldwork across several of the communities studied. Read on its own, this pattern fits two very different stories: a coordinated campaign of intimidation, or ordinary organisational fatigue and internal disagreement. Only knowledge of the network's history, sustained observation, and corroboration on a second measurement surface can tell the two apart. Acting on the pattern alone risks mistaking a legitimate falling-out for interference.

© 2026 RESONANT | Horizon Europe Grant Agreement N. 101132439
Co-funded by the European Union

Acting on single or weak signals. The Handbook's decision process is designed to prevent action on insufficient evidence. The evidence-and-impact assessment described in Chapter 5 then sets the level of response according to both the strength of the evidence and the severity of the impact. This discipline is most likely to slip under pressure: a single striking signal, an alarmed stakeholder, or the urgency of an unfolding situation can push practitioners toward a response before corroboration arrives. Acting on weak evidence produces false alarms, drains scarce analytical capacity, damages the credibility of future assessments, and can harm the people concerned.

Overexposing or harming targets. In most cases, the people whose behaviour this methodology observes are themselves targets of informational pressure. Fieldwork for RESONANT records the conditions they live under, including coordinated smear campaigns, doxing, cyberattacks, and threats reaching relatives who remained at home, and forms of surveillance directed at family members abroad. Anyone applying the Handbook carries a specific duty of care. Publishing, naming or otherwise circulating a suppression dynamic can re-expose the people affected. Because publication itself carries this risk, anonymisation, restricted circulation and careful classification apply by default to any output describing a community, network or individual, including cases that do not seem particularly vulnerable.



Mini-case | Illustrative

A monitoring team identifies a smear campaign against a named diaspora activist and prepares to publish its findings to raise awareness. The methodology treats this kind of harm as only partially reversible at best, and doxing followed by sustained harassment as not reversible at all. Publishing the activist's name and the details of the campaign would extend its reach, confirm to whoever is behind it that the pressure landed, and turn a recoverable harm into a lasting one. The safer course is to document the dynamic under a restricted classification, withhold or anonymise the individual's identity, and engage the people affected directly before any external communication.

Every stage of the analysis should be governed by a common set of safeguards: collecting only the data necessary for the stated purpose; avoiding direct identifiers wherever possible; storing material securely and restricting access; documenting the evidence and reasoning underlying each finding; and applying clearly defined retention periods. To support responsible information handling, the Incident Sheet includes a Traffic Light Protocol (TLP) classification, a colour-coded system that defines how widely the information contained in the case analysis may be shared.

The TLP also supports the mitigation of the potential dual-use risk. If misused, it could enable hostile actors to assess the effectiveness of different intimidation tactics or to monitor and profile the very communities it was intended to protect. Records showing who became silent, withdrew from participation or changed their behaviour could, in the wrong hands, reveal vulnerabilities and potential points of pressure. To mitigate this risk, analytical outputs should be shared only in accordance with the assigned TLP classification, applying the most restrictive level compatible with the legitimate purpose of the disclosure. Institutions adopting this Handbook should therefore protect its outputs through clear governance arrangements, secure storage and proportionate access controls, ensuring that a tool developed to safeguard the information space does not place the people and communities it is intended to protect at further risk.

Co-funded by the European Union

© 2026 RESONANT | Horizon Europe Grant Agreement N. 101132439

7.3 Practical Implications for Practitioners

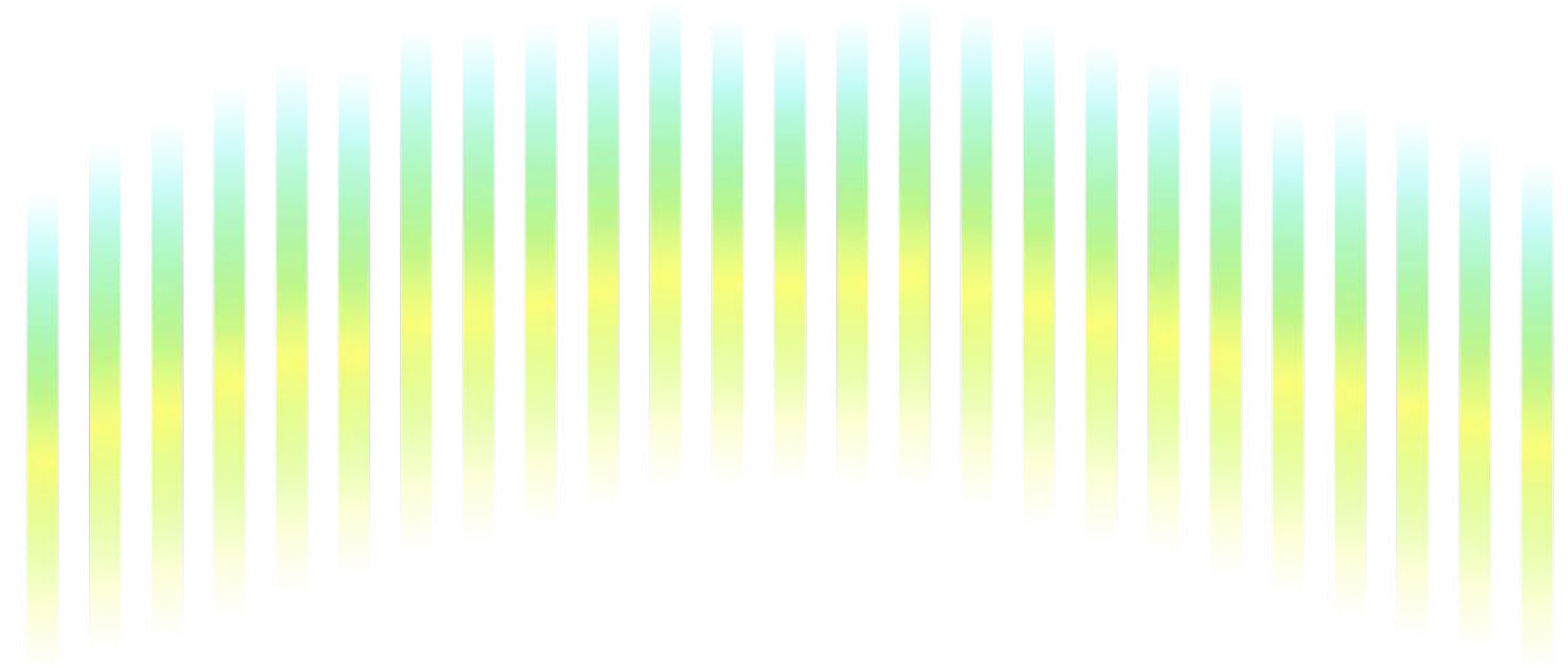
The limits and risks above mentioned can be translated into a small number of habits that anyone applying this Handbook should carry into daily practice.

On attribution. An assessment conducted using this methodology should report observed behaviours and documented effects; it should not be presented as a determination of responsibility. Where a practitioner considers attribution necessary, this should trigger further corroboration and, where appropriate, referral to the competent authorities identified in Section 7.1.

On weak or isolated signals. Before a case moves beyond monitoring towards escalation or an outward-facing response, the practitioner should be able to identify the independent evidence corroborating the initial signal, the period over which the pattern was observed, and the baseline against which any change was assessed. If any of these elements cannot be established, the case should remain under monitoring, regardless of its apparent urgency.

On the exposure of the people observed. Any output that identifies, or could enable the identification of, a community, network or individual should be treated as sensitive from the outset. Indicators such as silence, withdrawal or reduced engagement should likewise be interpreted cautiously and in context: their significance depends on the community concerned and its linguistic, social and historical circumstances, and no isolated instance should be regarded as conclusive. The appropriate TLP classification and access controls should be applied when the output is created.

These practices translate the methodological limitations and risks described above into safeguards for routine analytical work. Applying them consistently helps ensure that assessments conducted using this Handbook remain within its ethical, evidentiary and operational boundaries.



© 2026 RESONANT | Horizon Europe Grant Agreement N. 101132439
Co-funded by the European Union

8. Final remarks

The RESONANT Handbook brings together three years of research, methodological development and stakeholder engagement. Its purpose is to provide a practical framework for understanding, assessing and responding to FIMI and information suppression outside the context of academic research and therefore contribute to the enhancement of societal resilience. These phenomena are extremely complex and in constant evolution: their significance emerges from the interaction between information tactics, behavioural responses, social dynamics, vulnerabilities and the wider democratic context. The Handbook aims to provide a structured path, from first signal to evidence, from evidence to impact assessment, and from assessment to proportionate and rights-respecting action. It also stresses the importance of recognising uncertainty, avoiding premature conclusions and considering the possible consequences of interventions themselves.

The value of this approach ultimately depends on how it is used in everyday information environments. Awareness of FIMI, information suppression, fabricated or misleading content and coordinated manipulation is not the responsibility of specialists alone. Researchers, journalists, public authorities, civil society organisations and ordinary users all encounter information that can shape perceptions, relationships and participation in public life. Being able to pause, question a source, recognise unusual patterns, seek additional evidence and understand the possible effects of sharing or amplifying content is an important part of democratic resilience and of the "job" of being an active citizen. The health of our information environment affects how we communicate, how communities interact and how democratic societies function. External actors can exploit existing vulnerabilities, including divisions within communities, mistrust and social marginalisation, but resilient societies can reduce these opportunities through awareness, cooperation and informed participation.

The first line of defence is a collective one: society and citizens have a role to play in protecting the European information environment and strengthening democratic values.

Co-funded by the European Union

© 2026 RESONANT | Horizon Europe Grant Agreement N. 101132439

Annex – Glossary

Understand the context

Information ecosystem

The ecosystem in which information is produced, circulated, interpreted, and contested. It can be understood as an informational ecology shaped by technological infrastructures, cognitive practices, and performative interpretation processes. Its stability depends on epistemic integrity; its degradation produces informational alienation, self-referential bubbles, and epistemic vulnerability. (RESONANT D4.1).

Information disorder

The ecosystem formed by misinformation, disinformation, and malinformation and their societal consequences. Information disorder represents a degraded informational ecology characterised by epistemic entropy, cognitive overload, and erosion of shared interpretive frameworks. (RESONANT D4.1).

Narrative

A structured interpretation that gives meaning and coherence to events or realities. Narratives operate as performative acts that actively constitute social reality within a performative order. In influence operations, narratives function as epistemic weapons capable of imposing cognitive domination or reshaping ontological assumptions about legitimacy, identity, and truth. (RESONANT D4.1).

Strategic narrative

Long-term narrative frameworks designed to shape perceptions of legitimacy, identity, or geopolitical order. Strategic narratives function as instruments of cognitive domination, embedding durable interpretive structures that stabilise performative political orders and sustain politics of enmity or protection dramaturgies. (RESONANT D4.1).

Observable

Concrete elements relevant to understand how an incident unfolded – such as a tweet, a video on YouTube or an article on a website. Observables can be represented via the URL under which they were found or as files (EEAS, 2023).

Identify relevant narratives

Foreign Information Manipulation and Interference (FIMI)

A pattern of behaviour that threatens or has the potential to negatively impact values, procedures and political processes. Such activity is manipulative in character, conducted in an intentional and coordinated manner. Actors of such activity can be state or non-state actors, including their proxies inside and outside of their own territory. (EEAS, 2020).

© 2026 RESONANT | Horizon Europe Grant Agreement N. 101132439
Co-funded by the European Union

Information suppression

The intentional action (nature of action) by state or non-state actors of controlling or eliminating activities or publications that disclose relevant information - data, facts, theories, or pertinent knowledge - (content of the actions), whether to influence public opinion, restrict access to information, or maintain secrecy (purpose of the action). These operations may take place before having the information spread (active) or after (reactive), by blocking or eliminating the information source (RESONANT D1.2).

Influence operation

A coordinated effort to affect perception or behaviour through informational means rather than physical force. Influence operations constitute practices of cognitive warfare operating within hybrid conflict, deploying epistemic weapons, affective governance, and symbolic destabilisation strategies. (RESONANT D4.1).

Hybrid threats

Coordinated activities combining political, informational, economic, cyber, and social instruments to destabilise societies without conventional warfare. Hybrid threats correspond to forms of hybrid conflict in which informational and cognitive operations act alongside institutional and technological pressures. Power is exercised through curved strategic space — indirect influence, distributed deterrence, and manipulation of informational ecology rather than direct confrontation. (RESONANT D4.1).

Misinformation

Information that is false but believed to be true by those disseminating. It differs from disinformation in the absence of an intention to mislead or harm. (Sessa, M. 2023).

Disinformation

False information that is deliberately spread to hide the truth, to mislead, deceive or confuse people, especially in political situations (N. Goshylyk et al., 2021).

Malinformation

Genuine information that is shared to cause harm, often by moving information designed to stay private into the public sphere (N. Goshylyk et al., 2021).

Censorship

Suppression or prohibition of any content (parts of books, films, news, speech, public communication, or other information) on the basis that such material is considered obscene, politically unacceptable, “inconvenient”, harmful, sensitive, or a threat to security for the governments, private institutions, and other controlling bodies. (N. Goshylyk et al., 2021).

© 2026 RESONANT | Horizon Europe Grant Agreement N. 101132439

Map the actors

Actor

Any individual, group, organisation, or institution involved in or affected by a FIMI or information suppression incident. Actors may be state or non-state entities and can fulfil different roles, such as threat actors, target actors, intermediaries, or responders. (Elaboration in accordance with the RESONANT methodology).

Target

The intended recipient or object of a FIMI operation, i.e. the entity whose perceptions, attitudes, behaviours, trust, decision-making, or functioning the threat actor aims to influence through coordinated information manipulation. A target may be primary or secondary: the primary target is the person, organisation, community, or public group directly targeted by the narrative, activity, or pressure, while a secondary target is indirectly affected, for example through its association with the primary target or through the same information environment. (Elaboration consistent with the EEAS methodology).

Target vulnerability

The degree to which an individual, group, organisation, or community is susceptible to harm from an information-disorder or FIMI-related incident, considering the characteristics and contextual conditions that may increase their exposure to, or amplify the potential impact of, such harm. It includes factors such as limited protection, heightened exposure, and the target's significance for information integrity, civic participation, social cohesion, or democratic resilience. (Elaboration in accordance with the RESONANT methodology).

Detect behavioural signals

Observable behavioural pattern

A recurring and empirically identifiable behaviour, observed over time or across individuals, that reflects a response to perceived environmental or informational conditions. Its significance increases when it is repeated, shared across a community, temporally linked to an information environment, or supported by contextual evidence. Such patterns should be interpreted cautiously, considering alternative explanations, contextual factors, and resilience mechanisms, and should not alone be taken as evidence of manipulation. (Elaboration in accordance with the RESONANT methodology).

Behavioural signal

A measurable change in individual or collective behaviour that may indicate a response to an altered informational or social environment. Its significance depends on deviation from a baseline, persistence over time, and corroboration with other evidence. Because similar behaviours may have alternative explanations, signals must be interpreted within their specific social and contextual environment and cannot, in isolation, establish FIMI or its impact. (Elaboration in accordance with the RESONANT methodology).

Self-censorship

Voluntary suppression or non-disclosure of information by individuals or media actors as a result of the political pressure, threats, coercion, or other forms of external influence, whether perceived or actual (RESONANT D1.1).

© 2026 RESONANT | Horizon Europe Grant Agreement N. 101132439
Co-funded by the European Union

Cognitive interference

Manipulative framing, deception, or narrative tactics are used to distort understanding, undermine trust, or induce confusion - where the primary effect is informational distortion rather than access/visibility constraints. (RESONANT D4.1).

Assess impacts

Harm

Adverse consequences that affect individuals, communities, institutions, or democratic processes as a result of a FIMI operation. It may manifest through behavioural, social, or institutional changes and serves as an operational indicator for assessing an incident's impact, severity, and response needs. (Elaboration in accordance with the RESONANT methodology).

Individual impact

The effects of an information-disorder phenomenon in on a person's psychological well-being, cognition, behaviour, rights, and information practices. It encompasses emotional and cognitive responses, such as fear, uncertainty, fatigue, or disorientation, as well as behavioural changes in information seeking, communication, self-expression, or participation. It also includes changes in how individuals interpret, evaluate, and trust information. (Elaboration in accordance with the RESONANT methodology).

Community impact

The effects of an information disorder phenomenon on the relationships, cohesion, trust, solidarity, and collective behaviour of a diaspora or other social group. It encompasses changes in intra-community dynamics, including polarisation, fragmentation, reputational distancing, internal monitoring, reduced solidarity, conflict, or mobilisation, as well as changes in shared information and meaning-making practices. (Elaboration in accordance with the RESONANT methodology).

Systemic impact

The broader effects of an information disorder phenomenon on the civic, democratic, social, and informational environment in which individuals and communities operate. It includes potential effects on public debate, democratic participation, institutional trust, social cohesion, pluralism, and civic integration. Systemic impacts may emerge when individual and community-level effects become sufficiently widespread, persistent, or interconnected to influence the functioning and resilience of the wider democratic system. (Elaboration in accordance with the RESONANT methodology).

Severity

The assessed magnitude and extent of the potential adverse impact associated with an information incident or information-disorder phenomenon. It reflects the degree to which an incident may affect individuals, communities, institutions, democratic processes, or the broader information environment, considering factors such as scale, intensity, duration, reach, affected populations, and potential consequences. (Elaboration in accordance with the RESONANT methodology).

© 2026 RESONANT | Horizon Europe Grant Agreement N. 101132439

Validate findings

Evidence quality

The degree to which information is reliable, relevant, verifiable, consistent, and sufficiently corroborated to support a confident analytical assessment of a potential incident. It reflects the strength and credibility of the evidentiary basis. Higher-quality evidence increases confidence in identifying and characterising an incident and supports proportionate action, while lower-quality evidence requires cautious interpretation and further monitoring. (Elaboration in accordance with the RESONANT methodology).

Community

A socially connected and internally diverse group of individuals who share relevant characteristics, experiences, identities, or affiliations, while potentially differing in political, generational, linguistic, religious, socioeconomic, or other dimensions. A community is therefore not assumed to be homogeneous or characterised by internal consensus but rather understood as a plural and potentially unequal social structure in which actors may have different levels of visibility, representation, legitimacy, and access to decision-making or participation. (Elaboration in accordance with the RESONANT methodology).

Community resilience

The capacity of a community to sustain trust, cohesion, and collective action in the face of FIMI or information suppression. It relies on self-organisation, trusted relationships, institutional support, and the ability to adapt to, resist, and recover from information-related threats. (Elaboration in accordance with the RESONANT methodology).

Societal resilience

The capacity of communities and institutions to anticipate, withstand, and recover from manipulation attempts. Societal resilience depends on epistemic resilience, informational ecology health, and the preservation of epistemic integrity through pluralism, critical dialogue, and adaptive institutional feedback. (RESONANT D4.1).

© 2026 RESONANT | Horizon Europe
Grant Agreement N. 101132439
Co-funded by the European Union

Annex – Digital literacy in the classroom: a ready-to-use simulation to practise recognising FIMI.

ANNEX A – CLASSROOM WORKSHOP GUIDE

Understanding Information Manipulation through Social Impact

FIMI (Foreign Information Manipulation and Interference) refers to activities that seek to influence people, communities, or public debate through the deceptive or manipulative use of information, often by foreign state or non-state actors. These activities can take many forms and often occur in complex information environments where facts may be incomplete and intentions difficult to determine.

This workshop does not aim to identify who created a message, establish responsibility, or determine whether information is true or false. Such assessments often require specialised expertise, access to evidence, and investigative capabilities. The activity, instead, invites participants to explore who may be affected, including journalists, diaspora communities, civil society organisations, public institutions, minority groups, and the wider public, depending on the context; which vulnerabilities may be exploited; what social impact could emerge; and how individuals, communities, organisations, and institutions can respond.

The RESONANT approach is summarised as follows:



Figure 9 - Scheme of the RESONANT approach.

The rationale is that resilience, trust and democratic participation can provide an overarching protective layer against the penetration and impact of FIMI.

Target Group: Students aged 15+, youth groups, community participants

Duration: 75–90 minutes

Group Size: 12–30 participants

Learning Outcomes

By the end of the workshop participants will be able to:

- Recognise signs of possible information manipulation
- Identify which communities may be affected
- Assess potential social impacts
- Distinguish between low and high-risk situations
- Discuss appropriate responses
- Propose actions that strengthen community resilience

Co-funded by the European Union

© 2026 RESONANT | Horizon Europe Grant Agreement N. 101132439

Operational indications

This workshop guide provides all the materials needed to facilitate the exercise. It includes a step-by-step sequence of activities, detailed worksheets for participants to complete during the sessions, and structured guidelines to conduct/support effective and focused group discussions.

The Guide Also Contains A Final Plenary Debrief Structure Designed To Consolidate Learning outcomes and close the exercise.

At the end of the document, you will find a shared scenario card based on a real FIMI case. The objective of this activity is to introduce participants to the scenario Card as a practical tool for applying the concepts and analytical steps presented in the manual. The Scenario Card presents a realistic FIMI case scenario, allowing participants to explore how information manipulation may unfold in a concrete and recognisable context. Using the worksheets, participants will work through each of the steps presented in the manual, identifying the relevant elements of the case, recognising the indicators and mechanisms of FIMI, and discussing how these can inform an appropriate response. In this way, the activity connects the conceptual framework presented in the manual with its practical application, demonstrating how a FIMI scenario can be identified, analysed and addressed in practice.

FOR THE TEACHER

Before the activity starts:

→ Arrange students into groups of 4–6.
→ Print for each group:

- ☐ Scenario Card
- ☐ Worksheet 1 – What Do We Know?
- ☐ Worksheet 2 – Community Impact Map
- ☐ Worksheet 3 – Impact Assessment
- ☐ Worksheet 4 – Response Planning
- ☐ Worksheet 5 – Building Resilience

© 2026 RESONANT | Horizon Europe
Grant Agreement N. 101132439

Co-funded by the European Union

ACTIVITY 1

What Is Happening?

Time: 10 minutes

Teacher Instructions

Give each group the Scenario Card.

Ask students to read it together:

"Your task is not to determine who is responsible or whether the information is true or false. Your task is to understand the impact and effects it may have on people and communities."

Students complete Worksheet 1. The aim of this step is to break down the FIMI case into its main components, identifying the elements that are available for analysis and highlighting any gaps or uncertainties in the information provided. The reflective question encourages participants to recognise the subjective assumptions that may shape their interpretation of the scenario and to reflect on how these can influence their assessment, particularly where information is incomplete or uncertain.

WORKSHEET 1

What Do We Know?

Question	Notes
What is happening?	
What messages are circulating?	
Who is talking about the issue?	
What evidence is available?	
What information is missing?	
What remains uncertain?	

Reflection Question

What implicit assumptions are we making?

Co-funded by the European Union

© 2026 RESONANT | Horizon Europe Grant Agreement N. 101132439

ACTIVITY 2

Who Is Affected?

Time: 15 minutes

Teacher Instructions

Ask groups to identify all people and communities that could be affected.

The aim of this step is to identify the people and communities that may be affected by the situation, considering both direct and indirect effects. Participants are encouraged to look beyond the most obvious target and consider how the effects of FIMI may extend to other groups and relationships within the wider community. The questions below help participants explore the different forms that these effects may take, including emotional responses, changes in trust, and potential tensions between groups or institutions.

Students complete Worksheet 2.

WORKSHEET 2

Community Impact Map

Directly Affected

Group	How are they directly affected?

Indirectly Affected

Group	How are they indirectly affected?

© 2026 RESONANT | Horizon Europe
Grant Agreement N. 101132439

Co-funded by the European Union

Discussion Questions

1. Which groups may feel worried, angry or excluded?

2. Which groups may become more distrustful?

3. Which relationships between groups, communities, institutions or authorities, media and the public could be strained, weakened or damaged because of the situation?

- ☐ Community ↔ Institutions
- ☐ Community ↔ Community
- ☐ Community ↔ Citizens
- ☐ Citizens ↔ Authorities
- ☐ Media ↔ Public
- ☐ Other _____

Co-funded by the European Union

© 2026 RESONANT | Horizon Europe Grant Agreement N. 101132439

ACTIVITY 3

How Serious Is the Situation?

Time: 15 minutes

Teacher Instructions

Explain: Remember, the aim is not only to state whether the content is true. We are evaluating its possible impact. Its intensity varies also depending on different contextual, economic, social, political and racial factors. For this reason, assessing contextual conditions is essential, as they may provide indicators of the severity and spread of FIMI-related impacts. Students complete Worksheet 3.

WORKSHEET 3

Evidence quality level and Impact Severity Assessment

Step 1: Initial Rating - Evidence quality

In this first step, assess the quality of the information sources available in the Scenario Card. Consider how many sources are available, how independent they are, and whether they provide consistent information. Based on these factors, determine the overall quality of the available information.

Circle one of the following:

LOW / MEDIUM / HIGH

- **Low**. A single source
- **Medium**. Two sources or one very strong source plus supportive case cues.
- **High**. Two or more independent sources show a consistent pattern in the same time window.

Step 2: Impact Severity Factors

In this step, assess the potential severity of the situation by considering the scope and observable impact described in the Scenario Card. Consider how many people or groups may be affected, how widespread or persistent the effects may be, and the extent to which they may affect individuals, communities or the wider social environment.

Circle one of the following:

LOW / MEDIUM / HIGH

Use the following descriptions to assign a base severity level based on the incident's **scope** and **observable impact:**

Low: The situation has a localised and short-lived impact, affecting a limited number of people or a specific community or setting.

Medium: The situation has a sustained impact on a community segment (e.g. a diaspora cluster) or creates clear barriers to access or participation.

High: The situation has a wide impact on civic participation, rights or public order, involves a credible risk of physical harm, or produces large-scale chilling effects, including through cross-platform suppression.

© 2026 RESONANT | Horizon Europe Grant Agreement N. 101132439
Co-funded by the European Union

Step 3: Adjust for Severity modifiers

In this step, consider whether specific factors may amplify, extend or prolong the potential impact identified in the previous step. These severity modifiers help you assess whether the initial severity rating fully captures the scope and potential consequences of the situation. Tick every factor that applies to the scenario.

Tick every factor that applies.

Factor	Yes
Repeated over time	☐
Affects many people	☐
Lasting consequences	☐
Effects may continue	☐
Harmful behaviours may become normal	☐
Vulnerable groups targeted	☐
Impact spreads beyond original audience	☐
Possible offline consequences	☐
Close to elections or sensitive events	☐

Total Score

___ / 9

- Count the number of modifiers that apply.
- Use the following adjustment rule:

Number of modifiers	Adjustment
0–1	No change
2–3	Increase severity by one level (Low → Medium; Medium → High)
4 or more	Increase severity by one level and discuss whether the case represents a particularly significant or sustained impact
Any modifier indicating credible offline harm or serious risk to vulnerable groups	Consider increasing severity by one level regardless of the total score

Modifiers do not automatically determine severity on their own. They help participants consider whether the impact may be broader, more persistent, or more harmful than initially assessed. The final severity rating should combine the initial severity level with the contextual effect of the modifiers.

Co-funded by the European Union

© 2026 RESONANT | Horizon Europe Grant Agreement N. 101132439

Step 4: Evidence quality × Impact severity

In this step, combine the final assessment of evidence quality with the impact severity level to identify the appropriate course of action. The matrix indicates whether the case should be monitored, mitigated, or treated as a high-priority case requiring further review and coordination.

Severity \ Evidence	Low	Medium	High
Low	**Monitor** Keep the case under routine observation; set a date to check again.	**Monitor** Seek corroboration of the pattern with a second source and set a date to check again.	**Mitigate** The evidence is solid even if the impact still looks limited; prepare mitigation steps now, to be ready if severity rises.
Medium	**Monitor** Brief the team internally on what has been observed, and set a date to check again.	**Mitigate** Notify the relevant internal and external stakeholders. Prepare mitigation measures.	**High-priority** Escalate for senior review and coordinate the response with partner organisations.
High	**Mitigate** The apparent impact is serious but the evidence is still thin; corroborate it while preparing mitigation measures.	**High-priority** Escalate for senior review and synchronise the response across partner organisations.	**High-priority** Escalate for senior review and coordinate an immediate response with partner organisations.

Green (Monitor / Low priority)

You don't take immediate action. You log the case, keep it under observation, and may do light verification (e.g., check additional sources later). It stays within routine analysis workflows, usually handled by individuals to assess whether the information is true or false.

Yellow (Mitigate / Medium priority)

Look into the case more closely. Gather additional sources or evidence, note possible risks, and inform the relevant experts. Be ready to act if the situation develops or worsens by signalling the case to professional fact-checkers (e.g. La Buloteca; DISARM Foundation contact form, Trusted flaggers under the Digital Services Act, EFCSN).

Red (High-priority / Critical)

Flag the case immediately to relevant research centres (e.g. INACH, EDMO Hubs, FIMI-ISAC, AccessNow, Mapping Media Freedom) or supervising academic leads. Prioritise it for rapid review, share all available evidence, and contribute to coordinated action to respond to potential harm or disruption.

Discussion about the rationale



What made your group choose this severity level?

© 2026 RESONANT | Horizon Europe Grant Agreement N. 101132439
Co-funded by the European Union

ACTIVITY 4

What Should Be Done?

The aim of this activity is to translate the assessment developed in the previous steps into a proportionate response. Participants should consider which actions are appropriate given the potential impact of the situation, the quality of the available information and the level of attention indicated by the matrix. The focus is not on choosing the most visible or immediate response, but on considering what action is justified, by whom, and at what stage.

Time: 15 minutes

Teacher Instructions

Ask groups:

"Not every situation requires immediate intervention. It is important to understand how and who should act before."

Students discuss possible responses.

WORKSHEET 4

Response Options

Tick all responses that seem appropriate.

Response	Appropriate?
Monitor only	☐
Provide accurate information	☐
Community awareness campaign	☐
Contact trusted community leaders	☐
Public communication	☐
Refer to specialised organisations	☐
No immediate action	☐

Discussion Questions

1. What risks could arise if no response is taken?

Co-funded by the European Union

© 2026 RESONANT | Horizon Europe Grant Agreement N. 101132439

2. What risks could arise from responding too quickly or disproportionately?

3. How can responses address the potential impact without increasing tensions or causing unintended harm?

ACTIVITY 5

Building Resilience

The aim of this activity is to move from responding to the immediate situation to considering how individuals, communities, organisations and institutions can strengthen their resilience over time. Participants are encouraged to identify practical measures that could reduce vulnerability, improve preparedness and help communities respond more effectively if a similar situation occurs again.

Time: 15 minutes

Teacher Instructions

Ask students:

"Imagine this situation happens again next year. What could help the community deal with it better?"

Students complete Worksheet 5.

WORKSHEET 5

Community Resilience Plan

Use the worksheet to identify practical measures that could strengthen resilience at different levels. Consider what can be done by individuals, communities, organisations and public institutions, recognising that resilience depends on actions and capacities across these different levels.

Individual Level

What can individuals do to reduce the risk of being influenced by FIMI in their daily lives?

© 2026 RESONANT | Horizon Europe Grant Agreement N. 101132439
Co-funded by the European Union

What practical steps can you take to protect yourself from misleading or manipulative information (e.g. how you check information, who you trust, how you react online)?

Community Level

What can community groups do?

Organisation Level

What can schools, NGOs or associations do?

Institutional Level

What can public authorities do?



Co-funded by the European Union

© 2026 RESONANT | Horizon Europe Grant Agreement N. 101132439

FINAL DEBRIEF

Time: 10–15 minutes

Teacher-Led Discussion

Bring the class back together. Ask each group to discuss their key takeaways. Their discussion can be structured around answering a set of final questions: What information seemed reliable and what uncertain? Which groups did you identify as directly and indirectly affected? How severe did you perceive the impact? Which responses felt proportionate and pertinent? What long term measures could reduce future vulnerability?

Have each group report their conclusions. After each group's report, discuss recurring patterns, similarities and differences. Highlight that:

- Different groups may reach different conclusions while using the same framework. This is normal, as this is not a straightforward exercise when working with people and lived experiences.
- In real-world situations, complete information is rarely available. Focusing on impact rather than attribution helps identify appropriate actions to support affected people.
- It is important to understand how vulnerabilities might exacerbate the impact of FIMI and contribute to spillover effects.
- Successful responses focus not only on the incident itself but also on strengthening community resilience over time.

© 2026 RESONANT | Horizon Europe
Grant Agreement N. 101132439
Co-funded by the European Union

SCENARIO CARD

The "Chimney Incident" Story About a Ukrainian Refugee in Poland

- In late 2024, a disturbing story began circulating widely on social media, messaging apps, and alternative news websites.
- The story claimed that a Ukrainian refugee in Poland attempted to enter a Polish family's home through the chimney. According to the posts, the man became stuck in a ventilation shaft and later died. Some versions of the story also claimed that the incident had been reported by a well-known international news channel.
- The narrative spread quickly and was shared across different platforms, often accompanied by emotional comments, memes, and screenshots that appeared to show news coverage.
- As the story spread, it triggered strong reactions. Some users expressed fear and anger, suggesting that refugees might pose a danger to local communities. Others questioned whether the story was real, pointing out that no clear or official confirmation of the event could be found.
- Fact-checking organisations and journalists later examined the claim and reported that they could not verify that such an incident had taken place, and that no reliable reporting supported the version circulating online. They also noted that some images and screenshots shared with the story appeared to be manipulated or taken out of context.
- Despite this, the story continued to circulate in some online spaces, often being shared without additional verification.

Information Currently Available

- A story about a Ukrainian refugee allegedly dying in a chimney incident in Poland is circulating online.
- Some posts claim that a major international news outlet reported the incident.
- The story appears in multiple formats (text posts, screenshots, memes).
- Emotional reactions include fear, anger, and concern about safety.
- Fact-checkers and journalists report that the incident cannot be confirmed and no reliable sources verify it.
- Some shared materials appear inconsistent or potentially manipulated.
- The story is spreading across different platforms and communities.

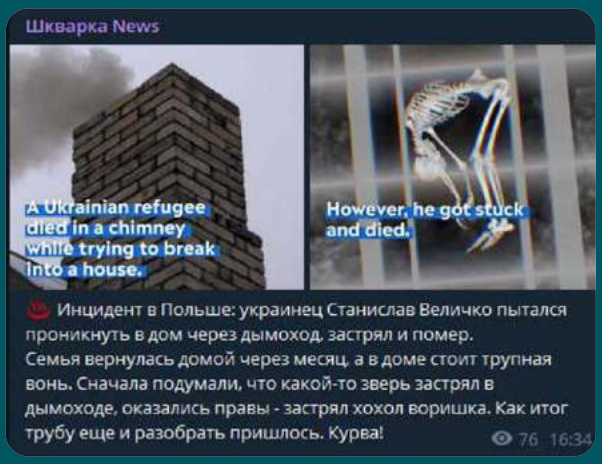


Figure 10 - Fake Euronews screenshot from Telegram channel "**Шкварка** News"

Evidence Overview:

- **Evidence supporting the incident as real:** No verified or credible evidence has been confirmed by reliable news organisations or official sources.
- **Evidence supporting the claim that it is false or unverified:**
  - Fact-checking organisations report no confirmed incident matching the description.
  - No official police, emergency, or municipal reports support the story.
  - Shared "news screenshots" appear inconsistent or potentially fabricated.
  - No established international media outlet has confirmed reporting the incident.
- **Evidence status overall:** The story remains unverified and disputed, with strong indications of fabrication or manipulation, but no confirmed real-world case corresponding to the viral narrative.

Co-funded by the European Union

© 2026 RESONANT | Horizon Europe Grant Agreement N. 101132439

Bibliography

Dvorakova, Z., & Polents, I. (2021). Entrepreneurship education and digital literacy as element of innovative learning. In Digital transformation and new challenges (pp. 253-263). Springer, Cham. https://www.researchgate.net/profile/Zuzana-Dvorakova/publication/354169895.

EEAS, "1st EEAS report on foreign information manipulation and interference threats: Towards a framework for networked defence" (2023). https://euvsdisinfo.eu/uploads/2023/02/EEAS-ThreatReport-February2023-02.pdf.

EEAS, "Tackling Disinformation, Foreign Information Manipulation & Interference, Strategic communications" (2020). https://www.eeas.europa.eu/node/410751_ku.

Frau-Meigs, D., et al. (2025). Fighting disinformation through media literacy: From current practices to policy making in Europe. InMedia. The French Journal of Media Studies, (10). https://journals.openedition.org/inmedia/3232.

Goshylyk, N., et al. (2021). Glossary of Media Literacy Terms. Ivano-Frankivsk: Vasyl Stefanyk Precarpathian National University. https://kaf.pnu.edu.ua/wp-content/uploads/sites/89/2021/03/Glossary-of-Media-Literacy-Terms.pdf.

Margaros, K., et al. (2026). Detecting FIMI: A methodological framework for testing OSINT tools in TTPs detection. Open Research Europe, 6(157), 157. https://zenodo.org/records/21627200.

Pérez-Escoda, A., et al. (2026). Enhancing teachers' digital competence for combating disinformation and fake news through the use of social media in classroom. Journal of New Approaches in Educational Research, 15(1), 4. https://link.springer.com/content/pdf/10.1007/s44322-026-00051-6.pdf.

Robandi, B., et al. (2025). Enhancing digital literacy and teacher-preneurship through a critical pedagogy-based training platform. Journal of Engineering Science and Technology, 20(2), 558-576. https://jestec.taylors.edu.my/Vol%2020%20Issue%202%20April%202025/20_2_12.pdf.

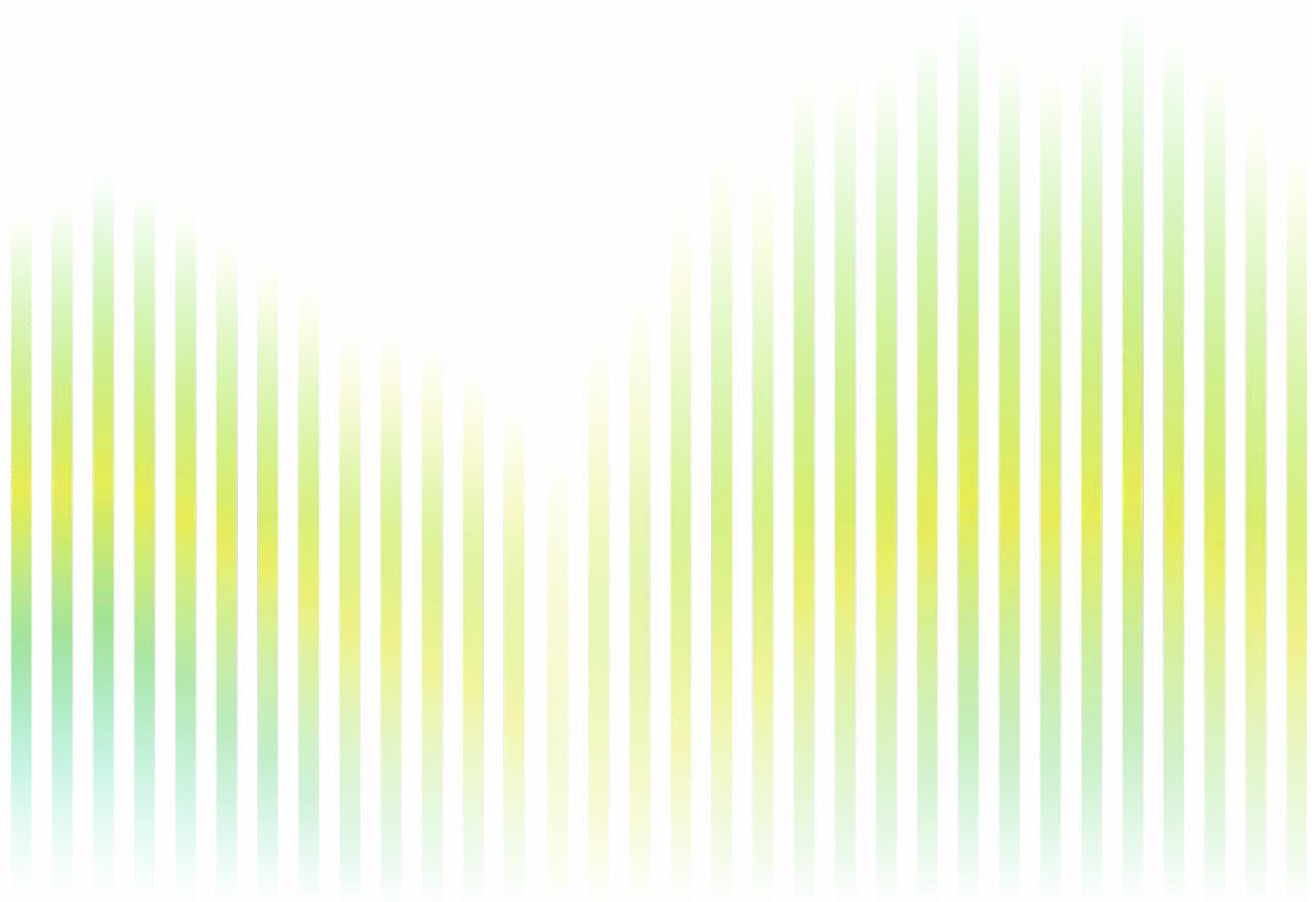
Sessa, M. (2023). Glossary. EU Disinfo Lab https://www.disinfo.eu/wp-content/uploads/2023/03/EUDL_Disinformation_Glossary.pdf.

Sharma, Y., Suri, A., Sijariya, R., & Jindal, L. (2025). Role of education 4.0 in innovative curriculum practices and digital literacy–A bibliometric approach. E-learning and Digital Media, 22(1), 1-32. https://journals.sagepub.com/doi/pdf/10.1177/20427530231221073.

RESONANT Deliverables

- RESONANT Project – Deliverable D1.2 – Baseline report
- RESONANT Project – Deliverable D2.2 – Compendium of TTPs and countermeasures
- RESONANT Project – Deliverable D3.2 – Report on Behavioural analysis of case studies on diaspora communities
- RESONANT Project – Deliverable D3.3 – Report awareness and preparation in host countries to stem FIMIs against diaspora communities
- RESONANT Project – Deliverable D3.4 – Report on Diaspora communities' case studies: the social and human rights law perspective on the effects of information suppression

© 2026 RESONANT | Horizon Europe Grant Agreement N. 101132439
Co-funded by the European Union



Co-funded by the European Union

© 2026 RESONANT | Horizon Europe Grant Agreement N. 101132439



Co-funded by
the European Union

MULTIDISCIPLINARY RESEARCH COOPERATION ON INFORMATION SUPPRESSION AND DIASPORA COMMUNITIES AS A TARGET OF FOREIGN INFORMATION MANIPULATION AND INTERFERENCE