

RESEARCH FOR INFORMATION FREEDOM

Countering information suppression

A TOOLKIT



Funded by
the European Union



Table of contents

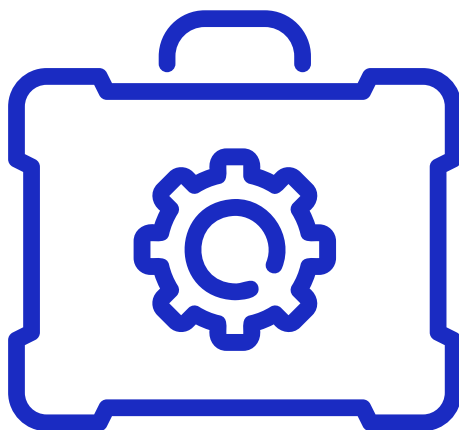
What is this toolkit?	4
How to use this toolkit	5
What is information suppression?	6
The three stages of suppression	7
A guide to TTPs Existing tools:	
TTPs and the DISARM framework	8
Response pathway	9
1) Identify	11
2) Assess	18
3) Respond	20
Additional Resources	22

What is this toolkit?

This toolkit is a practical guide for recognising and responding to a form of Foreign Information Manipulation and Interference (FIMI)¹: information suppression. It is designed for civil society organisations, journalists, diaspora organisations, researchers, human rights defenders, policy actors and others who may encounter attempts to suppress information.

Information Suppression can take many forms. It may involve direct censorship, but it can also appear as legal pressure, online harassment, intimidation, restrictions on access to data, platform manipulation, pressure on family members, or campaigns that bury independent reporting under a flood of distracting content. The purpose of this toolkit is to help users make sense of those tactics and decide what to do next.

The toolkit follows a simple pathway: identify information suppression, assess the level of risk, and choose a response that protects targeted individuals, organi-



sations, and their rights. Some situations may require the use of strategic silence while conducting protective action, such as documenting incidents, securing communications or seeking institutional support. Others may call for action, coalition-building, advocacy or escalation to policy actors.

Use this toolkit to identify

- What is happening
- Who is being targeted
- What harm may follow
- Which response is most appropriate

The aim is not to prescribe one answer for every situation, but to

- Support careful decisions that reduce harm
- Protect legitimate expression
- Strengthen responses to FIMI-related threats

¹ FIMI is defined by the EEAS as "a mostly non-illegal pattern of behaviour that threatens or has the potential to negatively impact values, procedures and political processes. Such activity is manipulative in character, conducted in an intentional and coordinated manner, by state or non-state actors, including their proxies inside and outside of their own territory"

How to use this toolkit

Civil society organisations can find this toolkit useful to recognise suppression tactics, document incidents, support people at risk, prepare safety protocols, build coalitions, or plan advocacy.

Journalists, diaspora organisations, researchers and policy actors who face similar pressures or work alongside civil society can use this toolkit to help clarify what is happening, identify who may be affected, and choose responses that protect people, information and rights.

This toolkit can be read in its entirety or used as a reference when a specific incident occurs. Each section has a different purpose. The early sections explain what information suppression is and how it works. The **identification sections** help users identify tactics in practice. The **assessment section** guides the understanding and decision-making about risk, urgency and possible resulting harm of the identified tactics.

The **response section** guides users to develop protective measures including evidence-gathering, legal options, coalition responses, and the choices between quiet and public action.



This toolkit outlines a response pathway based on a 3 step approach

1. Identify
2. Assess
3. Respond

Who is it for

- Civil society organisations
- Journalists
- Diaspora organisations
- Researchers
- Policy actors



What is information suppression?

Information suppression is broader than just censorship. The ARM project defines information suppression as **“a set of actions to silence information with the purpose of muting dissenting voices or narratives outside a country’s borders. It is transnational, highlighting the link between domestic and global tactics of information suppression, with various social groups acting as both agents and targets. Information suppression can also be the result of illiberal practices, targeting the autonomy and dignity of individuals”**.

Alternatively, censorship usually refers to direct restrictions on expression or access to information within a country’s borders, such as banning a newspaper, blocking a website, removing content or preventing publication. Information suppression can include those tactics, but it also includes less visible forms of pressure, such as legal threats, administrative burdens, surveillance, harassment, smear campaigns, denial of research access,

and pressure on employers, platforms, relatives or community organisations.

It can also overlap with propaganda, which is often understood as the promotion of a preferred message, narrative or political position. In suppression campaigns, propaganda can be used to push independent information out of sight. A state or aligned actor may flood the public space with distractions, amplify loyal voices, promote misleading narratives, or create confusion so that reliable information becomes harder to find and harder to trust.

In practice, this means that information suppression is not only about what is removed. It is also about what is made too risky to produce, too difficult to circulate, or too weak to shape public debate. For more simplicity, many prefer to talk of **“transnational information suppression”**. We consider both terms as synonymous for practicality.

The 3 stages of suppression

Information suppression works across three connected stages of the information cycle: production, dissemination and salience. These dimensions help users identify where pressure is being applied and what kind of response may be needed. A single case may involve one dimension, or several at the same time.

1 Suppression of information production

→ targets the people and organisations that create information. This includes journalists, researchers, academics, civil society organisations, human rights defenders, whistle-blowers, sources and community members. Tactics may include **arrest, harassment, legal threats, surveillance, denial of visas or permits, intimidation of family members, restrictions on access to archives or data, and pressure that leads people to self-censor**. The aim is to stop information from being produced in the first place.

2 Suppression of information dissemination

→ targets the circulation of information once it exists. This can involve **closing media outlets, blocking websites, throttling internet access, shutting down platforms, restricting broadcasters,**

manipulating search results, pressuring digital companies, or limiting the ability of civil society and media actors to reach their audiences. The aim is to prevent information from travelling, especially across borders or into communities that need it.

3 Suppression of information salience

→ targets the visibility, credibility or public impact of information. Instead of removing information outright, actors may bury it under competing content, flood the space with distractions, amplify preferred narratives, discredit independent voices, or promote social norms around what should not be discussed. The information may still exist, but it becomes harder to find, harder to trust, or less likely to shape public understanding.

In practice, these dimensions often reinforce one another. A journalist may be threatened, their outlet may be blocked, and their reporting may then be drowned out by coordinated propaganda or harassment. **Looking across production, dissemination and salience helps users see the full pattern rather than treating each incident as isolated.**

TTPs and the DISARM framework

To identify and analyse information suppression, practitioners who assess and combat FIMI use shared standards: TTPs and the DISARM framework.

First, they think in terms of Tactics, Techniques, and Procedures (TTPs). This term comes from the field of cybersecurity, and it is used by analysts to identify and analyse the actions of actors conducting Foreign Information Manipulation and Interference (FIMI) operations.

Tactics are the operational goals that actors are trying to accomplish. This is used to describe stages of an information campaign. Techniques are the actions taken to accomplish tactics. Procedures are the specific combination of techniques across multiple tactics that indicate intent and may be unique for different actors². Thinking in terms of TTPs helps to describe information suppression operations in granular details: what were the resources used (for example, AI to devise a message or a visual, or coordination among users to harass a journalist online). In practice, most analysts focus on identifying and describing the tactics and techniques that they observe.

Another shared standard used to facilitate communication between those who analyse and combat FIMI is the DISARM framework, maintained by the DISARM Foundation. DISARM stands for Disinformation Analysis and Risk Management. The DISARM framework

helps structure the analysis by identifying the different techniques used in FIMI incidents. It employs a shared language, so that analysts across organisations and countries can easily exchange information. When using the DISARM framework, analysts identify which combination of techniques from the framework are used, relying on tags. These tags help ensure all analysts describe the same incidents in the same way, and are also helpful for those who use AI to analyse incidents, as tags are easily understood by large language models.

The DISARM framework initially focused on FIMI, but is continuously being updated to better support the analysis of information suppression incidents. **Version 2.0 of the framework includes offline techniques of information suppression, and is accompanied by two playbooks which describe how to use the framework.** The framework and accompanying playbooks are linked to in the resource section of this toolkit.

Analysing information suppression incidents using the lens of TTPs, and relying on the DISARM framework can help analysts in understanding these incidents and reporting them, the first steps to assess how serious information suppression incidents are, and to develop adequate responses.

² This definition is adapted from the one provided by the EEAS consecutive FIMI reports.





Response pathway

Responding to information suppression is challenging: by definition, the information that has been suppressed is not (easily) visible or detectable. This means that analysts, researchers, journalists and policymakers often only became aware of information suppression if they are themselves targeted, or based on the testimony of those who have been targeted. This is why specific cases of information suppression are difficult to spot, and are frequently identified as part of a system rather than as specific incidents.

This toolkit provides a simple pathway to determine how to respond to information suppression, based on three steps of **“Identify, Assess, and Respond”**:

1 Identify

Check that the incident constitutes information suppression.

2 Assess

Analyse what kind of assets or actors have participated in the incident, which actions were undertaken, who was targeted, and what are the possible effects of the incident to assess how serious the incident is, and how vulnerable one is to such incidents.

3 Respond

Based on the assessment, determine which response strategy should be adopted. Adequate responses vary depending on who is the target of information suppression, how serious the incident is for the target and broader society, and who is in a position to respond.

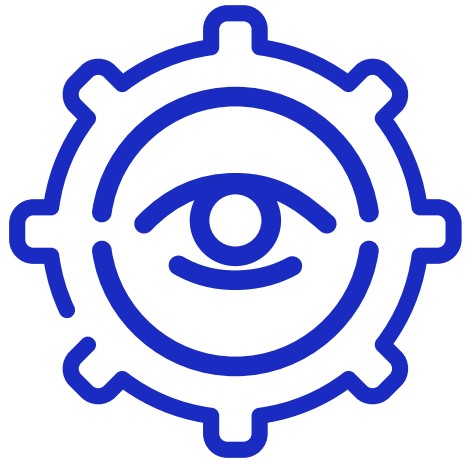
Each of these steps in the response pathway is detailed in the following pages to best help in assessing information suppression incidents and choosing an adequate response to combat information suppression and support those who are targeted. Note that this pathway is aligned with other toolkits that target FIMI more broadly.

1 Identify

This section focuses on how to identify when an incident constitutes a case of information suppression. To do so, it is useful to focus on the main characteristics of information suppression. First, **information suppression designates actions that target information or knowledge** and, by extension those who produce, disseminate, or make it more salient.

Second, it is transnational, meaning that a **foreign dimension is involved, at least indirectly**. This can be because those conducting acts of suppression are linked to a foreign state, or because those who are targeted are targeted because of their link to a foreign state either as citizens from that state, or because they produce or share information or knowledge connected to that state.

Information suppression can take the form of direct action, for example personal



attacks or cyber attacks against an organisation's website. It is also important to emphasise that information suppression can also result from established or internalised personal or societal norms, or self-censorship.

The following set of guiding questions and examples can be used to assist in recognising information suppression: from suppression of the production of information, and the suppression of its dissemination, to the management of its salience.

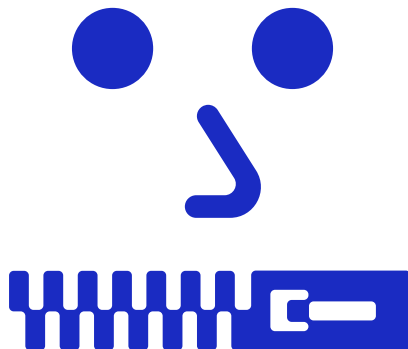
Examples of production suppression

1 In August 2021, a senior BBC journalist in Moscow was expelled from Russia when the country refused to extend her accreditation³. Russian authorities presented the decision as a response to refusals or delays by the British authorities to issue visas to Russian journalists. This incident is not isolated, and other foreign journalists have been expelled in the same way⁴.

→ The target of the incident is a journalist, who is directly involved in producing information on Russia for foreign audiences. Foreign authorities are involved, as the decisionmakers behind the refusal of accreditation. Combined, these two elements point towards information suppression.

→ Expelling the journalist will directly affect her (and her organisation's) ability to produce new information: production of information is sup-pressed.

2 In 2021 investigations by Amnesty International and a consortium of journalists revealed that Rwandan political opponents, human rights defenders, as well as Belgian journalists had been targeted by the surveillance software



Pegasus⁵, which silently infects mobile phones and exploits hidden security flaws, without any action (like clicking on a link) from their user.

→ It is suspected that the Rwandan government is behind these efforts, according to Belgian security services and to forensic evidence identified by Amnesty International.

→ Surveillance does not directly limit the ability of the target to produce information. Rather, it enables other forms of suppression through surveillance, for example identifying those whose visas should not be issued, or facilitating the formulation of personal threats: two forms of suppression of information production. Once the targets are made aware of the surveillance, it can also have a chilling effect: they might be less willing to investigate controversial or sensitive topics to protect themselves.

³ www.transcontinentaltimes.com/expulsion-of-senior-bbc-journalist-from-russia-direct-assault-on-media-freedom/

⁴ www.reuters.com/world/europe/russia-declines-renew-visa-spanish-reporter-el-mundo-2024-03-21/

⁵ www.lemonde.fr/pixels/article/2021/09/17/des-journalistes-belges-espionnes-via-le-logiciel-pegasus_6095080_4408996.html and www.lemonde.fr/international/article/2024/05/29/au-rwanda-opposants-et-proches-du-regime-cibles-par-le-logiciel-espion-pegasus-pendant-des-annees_6236172_3210.html

Examples of dissemination suppression

1 Shortly after the publication of Catherine Belton's book 'Putin's People', in 2020, the author and her publisher faced a wave of lawsuits for defamation filed by four Russian oligarchs and by the state-owned company Rosneft within the UK court system (and later Australia), each citing different passages of the book, leading to multiple yet overlapping legal actions forcing the author and publisher to engage in a costly defence. This type of legal action is described as Strategic Litigation Against Political Participation (SLAPP), where the process is so complex and costly that it deters the dissemination of unwanted information⁶.

→ The targets are an investigative journalist and her publisher as information producers and disseminators.

→ The foreign connection is present with the engagement of four Russian oligarchs and a Russian state-owned company; the extent to which the Russian state itself is involved is unclear.

→ The legal actions follow the publication of an investigative book, and render its dissemination and promotion more difficult (and possibly impossible, if the lawsuits were to be lost).

2 European academic with expertise on Ethiopia⁷. One of them was targeted by a widespread smear campaign following their analysis of the war in Tigray. This included accusations by Ethiopian intelligence services of being paid by an opposition group, as well as death threats. The campaign led to the cancellation of public events where the academic was supposed to participate.

→ Though it is difficult to conclude that all aspects of the smear campaign are centrally coordinated, direct accusations were made by the Ethiopian intelligence services, and included the Ethiopian media, indicating a connection to foreign interests.

→ The campaign started after the targeted person published opinions regarding the Tigray conflict in the media, followed by death threats that in particular led to the cancellation of public events, affecting dissemination.

→ This type of event can also affect the production of future knowledge/information (can lead to self-censorship).

⁶ More details can be found in Jānis Juzefovičs, Vineta Kleinberga, Una Aleksandra Bērziņa Čerenkova, Andrey Makarychev, Yuliia Kurnyshova, Mariëlle Wijermars, and Gunhild Hoogensén Gjörv (2026) p13 www.arm-project.eu/publication/russian-information-suppression-as-fimi/

⁷ www.aftenposten.no/verden/i/weK825/norsk-professor-trues-paa-livet-av-etiopiere-det-paagaar-en-aktiv-koordinert-hatkampanje-mot-meg

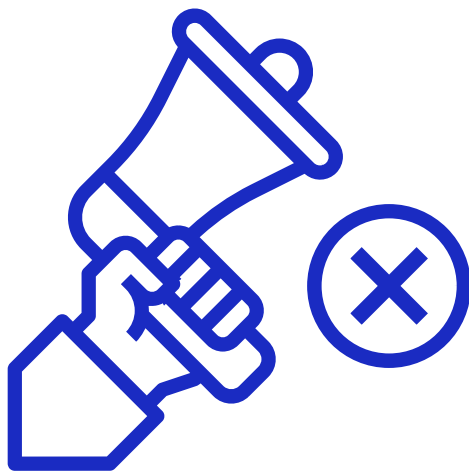
Examples of salience management

1 Identifying cases of information suppression through salience management can be difficult, as this is rarely highly visible without in-depth investigations. In February 2024, the Citizen Lab identified a series of 123 websites posing as local news outlets in a series of European, Asian, and Latin American countries but operated from within China and propagating pro-Chinese narratives⁸, in addition to targeted personal attacks.

→ In this instance the target is not one individual person, but the potential audiences in the countries these websites claim to be based in. They claim to be news websites, disseminating information and current events.

→ A foreign operator, China, is present, as this is where the fake news websites are operated from.

→ How salience management affects information is more diffuse: while this network of websites does not necessarily



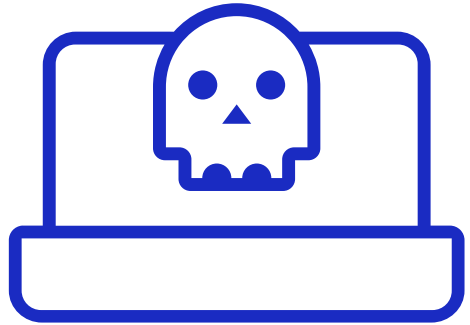
suppress specific, targeted news items, nor make them impossible to access, it floods the internet with pro-China content, making legitimate information more difficult to find (less salient), while spreading disinformation.

2 Another example is the case of the AI-generated propaganda promoting Ethiopia's access to the sea which flooded social media in September 2025⁹. On the one hand, the campaign promoted a core, unifying issue in Ethiopia (its loss of access to the sea). On the other hand, it was so conspicuous that it overwhelmed dissenting voices and diluted critical narratives that warned against an escalating tension and a possible war with neighbouring Eritrea.

→ The target is the online audience: Ethiopians, including those abroad, but also neighbouring audiences (particularly Eritrea, who gained independence from Ethiopia in 1993, causing Ethiopia's loss of sea access) and more international audiences (posts are in multiple languages including English).

→ This can appear as a purely domestic campaign, but it includes a geopolitical discourse (changing national borders), which can be seen as targeting discourses beyond Ethiopia.

→ This campaign promotes a specific narrative to broader audiences, but it also out-competes dissenting voices. It thus constitutes an effort at managing the salience of specific types of information beyond borders.



Summary

An incident may constitute information suppression when it targets information, knowledge or those involved in producing and sharing it, and has a connection to foreign interests.

- Ask whether information, knowledge or an information actor is being targeted.
- And look for a direct or indirect connection to foreign interests.
- Identify where the impact occurs – production, dissemination or salience.
- Remember that suppression may be direct, or may operate through pressure, norms and self-censorship.

⁸ citizenlab.ca/research/paperwall-chinese-websites-posing-as-local-news-outlets-with-pro-beijing-content/

⁹ Matti Pohjonen, Amanuel Kebede & Lovise Aalen (2026) Information Suppression in Ethiopia pp36-37 www.arm-project.eu/publication/information-suppression-in-ethiopia/

Is this information suppression?

Use the questions below to assess whether an incident or activity may be information suppression.



1



Is information or knowledge targeted?

Is the incident or activity affecting a piece of information or knowledge, or an organisation or individual involved in information or knowledge work?

Yes

No

2



Is there a connection to foreign interests?

Is the incident or activity connected to a foreign country or to foreign interests?

Yes

No



**This is not
information
suppression**

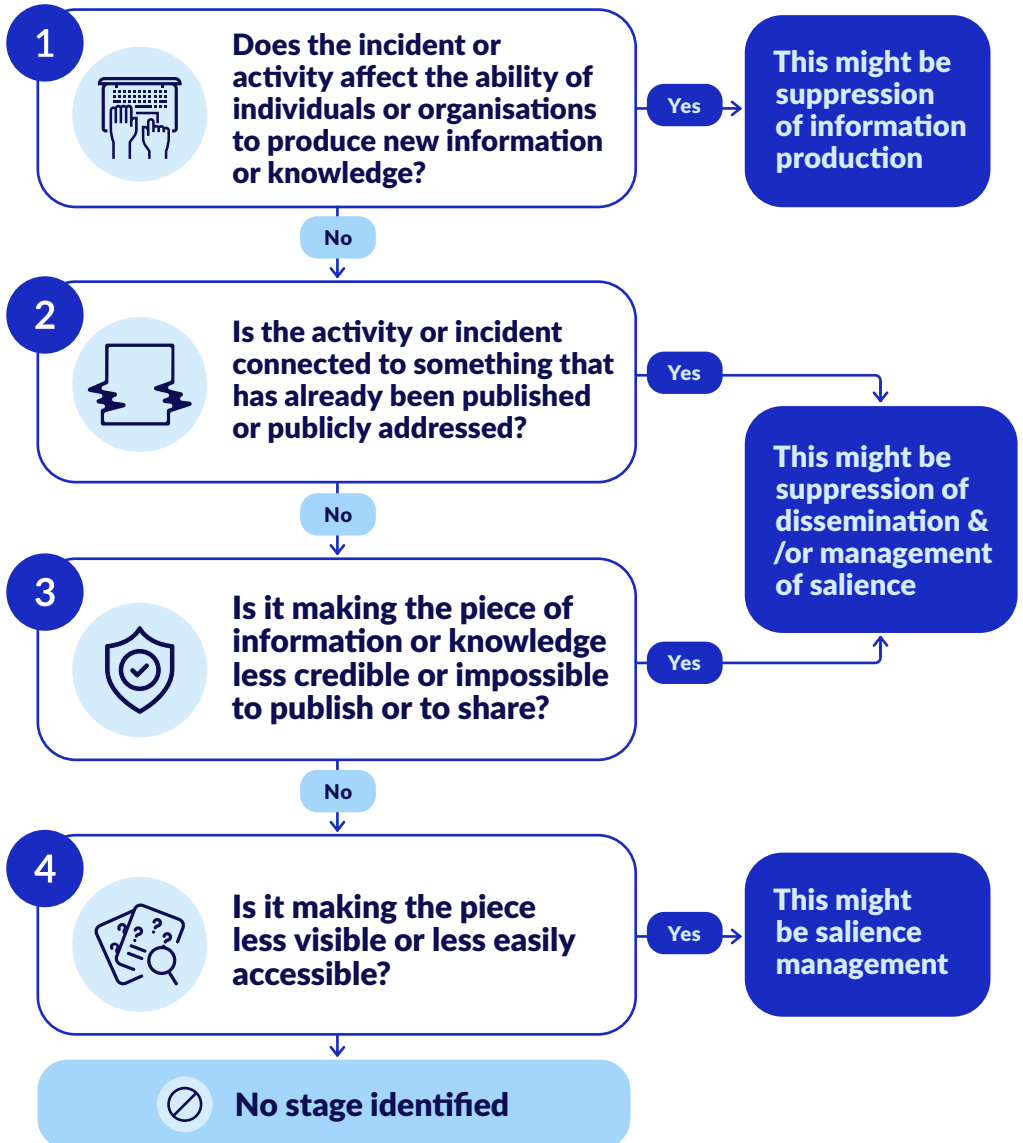


**This might be
information
suppression**

Next step



What stage of the information cycle is affected?



2 Assess

Once the incident or activity is identified as information suppression, it is necessary to assess what kind of threat the incident constitutes for the targeted piece of information/knowledge, and for the targeted individual/organisation. This will help in defining a response strategy based on the specific target of information suppression and on the severity of the incident.

The table on the following page is designed based on insights gained through analysing a wide range of incidents of information suppression, and based on our experience assessing risks and potential responses while investigating information suppression as a phenomenon. It is designed as a tool to help systematically assess how severe a specific incident is, to then better decide on possible responses. The table is cumulative: for example, if the target is an institution with support systems (low concern), but there appears to be an immediate danger (high concern), and the information that is suppressed is time sensitive (high concern), then the incident represents a high concern. Note that the following table is meant to help prioritise, but not to dismiss incidents on the basis that it represents an overall lower concern.



Summary

Once information suppression has been identified, assess how serious the incident is and how vulnerable the target may be.

Consider:

- Who is being targeted
- Who appears to be behind the incident
- Whether there is immediate danger
- How time-sensitive the information is
- Whether the harm can be reversed
- Whether responding could create additional risks

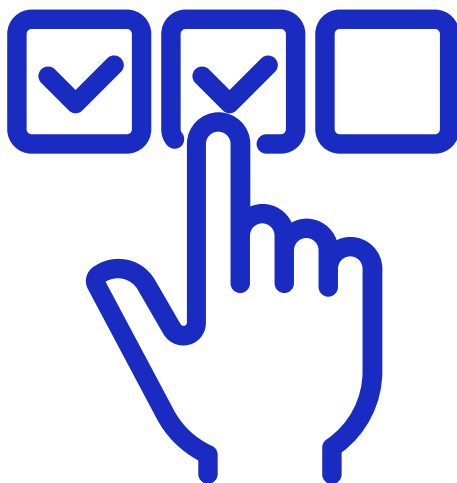
Relevant dimensions of incident

Relevant dimensions of incident	Level of concern		
	Low	Medium	High
Who is targeted?	Institution (or associated individual) with support systems in place	Small organization or individual with fewer support systems	High-risk journalist, human rights defender, dissident, source, or a family member, particularly if the individual has connections with diasporas
Who appears to be behind the incident?	Isolated individual	Non-state actors more or less organised, with looser connections to a foreign state	Foreign state actors, or organised non-state actors with clear connections to a foreign state
Is there immediate danger?	No clear threat or danger	No immediate danger, but the incident makes it more difficult to continue producing or disseminating information or knowledge	Arrest, threat of violence, doxxing, legal action, or pressures on family members
Is the information time-sensitive?	No	Somewhat	Yes, the public needs access now to specific information
Is harm reversible?	Easily corrected	Partly reversible	Long-term chilling effect or irreversible harm
Could response increase risk?	Unlikely	Possible	Likely without adequate safeguards

3 Respond

Once an incident has been identified as information suppression and it has been assessed, it is time to decide on the most appropriate response strategy. Depending on the level of concern and the level of exposure of targeted individuals and of the information being suppressed, responses can range from strategic silence to an open and very public response. Specifically, strategic silence can be necessary if a public response would expose the targeted individual or organisation to further suppression efforts. By contrast, openly and publicly responding to an incident can help garner support from others and combat suppression through the courts, or by increasing the visibility of the information/knowledge that is targeted.

To respond to an incident, it is important to consider three aspects: documenting the incident, protecting the target of suppression, and responding more directly, for example through the court system, advocacy, or by continuing information/knowledge work. Each of these aspects can be done while seeking publicity or, by



contrast, by maintaining strategic silence.

First, it is important to document the case of information suppression by recording evidence and creating a report that can be shared within the organisation, with the relevant authorities, with partners, or made public depending on the level of publicity that one wishes for. Such a report should be started at the identification stage, and can usefully use the DISARM framework to make it easier to communicate with other institutions. The assessment of the level of concern created by the incident can also be included.

Second, it is also necessary to consider protecting the targeted individual, organisation, and/ or piece of knowledge.

This can involve ensuring the targeted information or knowledge is safeguarded

and cannot easily be reached by perpetrators, via making and securely storing data for example. It can also consist in limiting the exposure of the individual who has been targeted, for example by stopping the use of social media for a period of time. For cases where serious threats are involved, it might be necessary to consider reporting the incident to the relevant authorities. It can also consist in making the incident as public as possible, in cases where publicity can act as a form of protection from retaliation.

Third, more direct action should be considered, for example via forming coalitions with like-minded organisations to develop stronger capabilities to continue working on producing the kind of targeted information. If a more public strategy is desired, it can be relevant to engage in legal procedures, and/or to expose the incident and those behind it and to advocate for change. It is important to note that responses should be in line with human rights principles, including freedom of expression and the right to information, and **adopt a “do no harm” approach**, to avoid exposing targeted individuals and others.

Of course, strategic silence as a strategy of documenting, protecting, and directly

acting against a suppression incident can also form the basis of a more public strategy, when the time appears right for more exposure. This depends on the assessment of the incident and its potential consequences.

Summary

Choose a response that reflects both the severity of the incident and the risks facing the target.

A response should consider:

- **DOCUMENTING** – record what happened and preserve relevant evidence.
- **PROTECTING** – safeguard targeted people, organisations, sources and information.
- **ACTING** – consider appropriate direct action, including coalition-building, legal action, advocacy or continuing the targeted information work.
- **GOING PUBLIC** – decide whether strategic silence or a more public response is likely to reduce, rather than increase, risk.
- **THROUGHOUT**, follow a do-no-harm approach.

Additional resources

To understand information suppression:

- [Working paper defining information suppression as FIMI](#)
- [Comparative working paper](#)
- [Catalogue of TTPs of information suppression identified by the ARM project](#)

To analyse information suppression and other FIMI incidents:

- [The DISARM framework](#)
 - As of September 2026, version 1.7 is available at the link above.
 - [Tutorial to use version 1.7 of the Disarm Framework Navigator](#)
- [Version 2.0 of the DISARM framework, which includes information suppression, and is currently being finalised](#)
- [accompanying Playbook on using the framework to identify tactics and techniques of information suppression](#)
 - [Playbook on how to use the framework to write specific procedures of information suppression](#)
 - [Working paper describing how DISARM 2.0 was developed](#)

[EU DisinfoLab's FIMI toolkit](#): it does not cover information suppression, but provides examples of how to use the DISARM framework to identify and monitor FIMI incidents and countermeasures.

For your notes:

CMI CHR. MICHELSEN INSTITUTE



UNIVERSITY OF HELSINKI



RĪGA STRADIŅŠ UNIVERSITY



LUNDS UNIVERSITET

UNIVERSITY OF BERGEN



Maastricht University



UiT The Arctic University of Norway



UNIVERSITY OF TARTU



Hertie School
Centre for
Digital Governance

WZB



Wissenschaftszentrum Berlin
für Sozialforschung



arm-project.eu



arm-project.eu



media@arm-project.eu

CONTACT

