FIMI -ISAC

FDEI PROJECT

EU DISINFO LAB

FIMI MONITORING TEMPLATES

PART 01: Incident Qualification

Developed and authored by EU DisinfoLab

The goal of this template is to offer a triage tool that distinguishes FIMI incidents from non-FIMI, differentiates incidents from broader campaigns, and sets clear thresholds for case selection in monitoring activities.

PART 1 – Incident qualification

A. IS THIS FIMI?

EEAS definition: "FIMI is 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. Actors of such activity can be state or non-state actors, including their proxies inside and outside of their own territory."

1. FOREIGN ACTORS: *Check the foreign component and assess its role*[1]

Actors: The interference is performed by foreign "state or non-state actors, including their proxies inside and outside of their own territory."

Disclaimer: Although we recognise that attribution is challenging, the foreign component in the operation is a prerequisite for FIMI classification. Therefore, users of this template are free to begin the compilation process based on the information available (e.g., behavioural indicators). Still, ultimately, the involvement of foreign actors (state or non-state, directly or indirectly) is a conditio sine qua non for qualifying an incident as FIMI.

- Are foreign actors engaging in this incident/campaign?

If the answer is yes:

- Actor type (relevant for attribution): Are they state or **non-state actors**?
- Actor role: Are foreign actors the **initiators** of this incident/campaign?
- Actor role: Are foreign actors the **amplifiers** of this incident/campaign?

If foreign actors are the amplifiers:

- Is there evidence of a **direct connection** (e.g., funding, political) with the initiators?

→ Reminder: Endorsement is not attribution! Liking or resharing a post is not proof of FIMI by itselfz

[1] Useful references for this part: Attributing information and influence operations (Hybrid CoE); Counter Disinformation Network (Alliance4Europe); Countering state-sponsored proxies: Designing a robust policy (Hybrid CoE).

If the answer is no:

- If there is no evidence of foreign actor involvement, the incident or campaign is not FIMI.

2. BEHAVIOUR: *Check the manipulative, intentional, and coordinated behaviour components:*

Behaviour: FIMI is "manipulative in character, conducted in an intentional and coordinated manner."

2.1 MANIPULATION

- Manipulative behaviour: Does the incident/campaign show manipulative behaviour?

If the answer is yes:

- Disinformative element: Does the manipulation include disinformation?

  → Reminder: Disinformation is not essential for FIMI!

- Content: If the FIMI campaign includes disinformation, what is the narrative (and metanarrative) circulated?
- Cyberattack: Did a cyberattack precede or follow the distribution of (dis)information?
- TTPs: Does the incident/campaign use other TTPs for manipulative purposes?

  → Reminder: Check out the DISARM Red Framework (e.g., impersonation, obfuscation, artificial amplification)

2.2 INTENTIONALITY

- Intention: Does the incident/campaign show evidence of intentionality?

  → Reminder: FIMI is intentional. If the incident involves misinformation (unintentionally sharing false information believed to be true), there is no FIMI.

If the answer is yes:

- Intent: Is the purpose of the incident/campaign clear?

3.3 COORDINATION

- Coordination: Does the incident/campaign show evidence of coordination?

  → Reminder: Coordination is crucial to qualify an event as FIMI and to connect different incidents to a campaign.

3. IMPACT: *Check impact in terms of outreach and harm*[2]

Impact: FIMI "has the potential to negatively impact values, procedures and political processes."

- **Outreach:** Did the incident/campaign achieve **considerable outreach?**

→ Note: Define outreach explicitly and set a threshold within the working group or project.

We define "outreach" as the extent to which content appears on platforms or media, shaping user exposure – initially passive, often via feeds. Measurable by the number of platforms or media featuring the content, and in some cases, by views, especially if autoplayed. Key factors include mainstream media amplification, public figures endorsing the narrative, and multilingual or multi-format distribution, which enhance outreach.

- **Engagement:** Did the incident/campaign achieve **considerable engagement?**

  → Note: Define engagement explicitly and set a threshold within the working group or project.

  We define "engagement" as the user's active engagement with the content, including shares, views, likes, and comments.

- **Values:** Does the incident/campaign harm/criticise/attack the core **values** of EU societies (e.g., freedom, democracy, equality, etc)?
- **Procedures:** Does the incident/campaign harm/criticise/attack the core procedures of EU societies (e.g., fair elections, welfare, defense, etc)?

  → Note: We acknowledge that FIMI is not limited to the EU and hope that the templates can also be applied beyond the European Union. Nevertheless, these templates have been primarily developed and used for EU-focused monitoring, which reflects our area of expertise.

---

[2] Useful references for this part: Breakout scale (Ben Nimmo), Impact-risk index (EU DisinfoLab, a *calculator* is also available).

4. INFRINGEMENT: *Check for infringement to assess the presence of illegal activities*

Legal grounds: FIMI is "a mostly non-illegal pattern of behaviour". Therefore, in most cases, it will be harmful but legal ("awful but lawful"), but it can also be illegal.

Disclaimer: Compiling this section does not require any prior legal background. Where helpful, desk research and analytical support tools may be used to guide the process. However, such tools should be used cautiously, and outputs should be cross-checked and validated against reliable sources.

- Does the incident/campaign constitute a **law violation?**

If the answer is yes:

- Does the incident/campaign violate **national regulations** (e.g., fraud, identity theft, slander, etc)?
- Does the incident/campaign violate **international regulations** (e.g., AI Act, DSA, GDPR, etc)?

  → Reminder: Check out ongoing *investigations* and *sanctioned* entities.

If the answer is no:

- Does the incident/campaign constitute a **harmful** activity?
- Does the incident/campaign violate a **platform's** Terms of Service (e.g., disinformation, coordinated inauthentic behaviour, etc)?

FINAL ASSESSMENT:

- **Low certainty:** There is no evidence to prove that the incident is part of a FIMI operation.

- **Medium certainty:** Most of the abovementioned conditions are met, and there is evidence to prove them. Therefore, the investigator strongly suspects that the incident is FIMI but does not have sufficient evidence to prove it.

- **High certainty:** All of the above conditions are fulfilled, and there is evidence to prove them.

B. IS THIS A SINGLE INCIDENT OR PART OF A CAMPAIGN?

To recap:

- FIMI requires coordination.
- For a single incident to qualify as FIMI, threat actors must coordinate in its development.
- When coordination between threat actors is proven, a campaign will consist of different incidents.

- **Coordination:** Does the incident/campaign show evidence of **coordination?**

  → Reminder: Check actors, narratives, TTPs, platforms, etc.

- **FIMI incident:** Does the **single incident** show evidence of coordination among foreign actors?

If the answer is yes, this is a FIMI incident.

- **FIMI campaign:** Do **multiple incidents** show evidence of coordination among each other?

If the answer is yes, this is a FIMI campaign.

FINAL ASSESSMENT:

- **Single incident:** There is no evidence to prove that the incident is part of a FIMI campaign.

  → Reminder: This assessment can change in the future if more evidence is available.

- **Part of a campaign:** One coordinated incident or multiple incidents prove to be part of a FIMI campaign (e.g., similar attack patterns, similar narratives, shared production/amplification infrastructure, or other kinds of coordination indicators).

APPENDIX

A. IS THIS FIMI?

1. FOREIGN ACTORS

FOREIGN COMPONENT INDICATORS:

- Check for poor language, it might indicate (automated) translation and non-native speakers.
- Check for foreign words in the post, caption, and code.
- Check for foreign names in account names and user handles.
- Check for high activity during "rush hours" in other time zones.
- Check for metadata (in photos and videos) showing other time zones.

INITIATIONS/AMPLIFIERS INDICATORS:

- Check (on multiple platforms) if the incident is the earliest publication available.
- Check if the account spreading the incident is directly involved in content production (e.g., evidence that it purchased domains).
- Check if the account spreading the incident plays a central role in the amplification loop.

PROXIES INDICATORS:

- Check for direct links between the domestic actor and a foreign power (e.g., evidence of funding).
- Check if the domestic actor is a subsidiary of a foreign organisation/institution/authority (e.g., official accounts of embassies of culture institutes).
- Check if there is a relationship/partnership between the domestic actor and a foreign organisation/institution/authority.
- Check if there is a strong ideological connection between the domestic actor and a foreign organisation/institution/authority. Reminder: This can simply suggest endorsement!
- Check if there are common interests between the domestic actor and a foreign organisation/institution/authority.

LINK TO STATE ACTORS INDICATORS:

- Check if institutions/authorities/governments are involved (including depending entities).
- Check if state media or other organisations depending on or funded by institutions/authorities/governments are involved.

2. BEHAVIOUR

MANIPULATION INDICATORS + DISINFORMATION:

- Check if the narrative/image/video shared in the incident has already been debunked by fact-checkers or flagged as false.
- Check if the incident contains false/misleading/decontextualised information, doctored/AI-generated content, scams, etc.
- Check if the narrative causes harm to an individual or group.

OTHER KINDS OF MANIPULATION:

- Check for malinformation, i.e., real information leaked with malicious intent.
- Check for cyberattacks, social engineering practices, or espionage (i.e., actions to extract sensitive information to be used with malicious intentions).
- Check for inauthentic actors/accounts.
- Check for deceptive behaviour (e.g., coordinated inauthentic behaviour, including fake engagement).

INTENTION INDICATORS:

- Check for contextual information (e.g., elections, war, government or economic crises, etc).
- Check if the narrative/TTPs cause harm to an individual or group.
- Check if there is a clear purpose (e.g., get-rich-quick schemes, influencing votes, etc).

COORDINATION INDICATORS *(Check out the CIB Detection Tree):*

- Check for temporal indicators: e.g., similar timestamps for account creation/posting, synchronised engagement.
- Check for narrative alignment, including posting similar hashtags/visuals/texts in different languages/across different platforms/focusing on a single topic.
- Check for relational indicators, e.g., similar profile/cover photos and tightly interconnected clusters of accounts that mostly follow each other.
- Check for technical indicators, e.g., multiple accounts sharing the same IP address, analytics IDs, devices, and configurations.
- Check for automation indicators, e.g., bots and automated publication practices.

3. IMPACT

IMPACT AS OUTREACH INDICATORS:

- Check if the content is translated into multiple languages.
- Check if the content is spread in multiple formats (e.g., videos, photos, texts, etc).
- Check for cross-platform amplification.

- Check for media amplification.
- Check for public figures amplification.
- Check for relevant interactions (e.g., likes, shares, views, etc).

IMPACT AS HARM INDICATORS:

- Check for calls to offline action (e.g., strikes, protests, etc).
- Check for harmful and illegal online actions (e.g., doxing, harassment, data leaks, etc).
- Check for relevant statements/declarations, such as an attacker reclaiming responsibility or calling out specific targets.

4. INFRINGEMENT

ILLEGALITY INDICATORS:

- Check relevant laws against impersonation (e.g., copyright, trademark, identity theft, and fraud).
- Check laws against disinformation, including electoral disinformation.
- Check advertisement laws (e.g., against unfair/deceptive advertising).
- Check laws related to foreign agents operating in a country.
- Check laws against cyber-criminal offenses.
- Check laws against violence, including hate speech, hate crimes, and gender violence.

HARM INDICATORS

- Check the Terms of Service of platforms and technological supports (e.g., misinformation, coordinated inauthentic behaviour, election integrity, advertising standards, etc).

B. IS THIS A SINGLE INCIDENT OR PART OF A CAMPAIGN?

- Check for COORDINATION INDICATORS (see A.2)