April 2023

FIMI: TOWARDS A EUROPEAN REDEFINITION OF FOREIGN INTERFERENCE

EU DisinfoLab

Publication Date: April 2023

Author: Nicolas Hénin, EU DisinfoLab

About EU DisinfoLab

As an independent non-profit organisation, EU DisinfoLab gathers knowledge and expertise on disinformation in Europe. Through putting together research, investigative work and policy acumen, EU DisinfoLab is an active member of, and supports, a passionate and vast community that helps to detect, tackle, and prevent information disorders endangering citizens' integrity, peaceful coexistence and democratic values.

You can find more information about our work on our website:

https://www.disinfo.eu/

E-mail: info@disinfo.eu

EU DISINFO LAB

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The acronym FIMI (Foreign Information Manipulation and Interference) has recently met a lot of success and is consequently increasingly used. It has become widespread in the European Union, within the European External Action Service (EEAS) and across the Member States. Therefore, it deserves to be well understood and cautiously defined. In fact, FIMI overlaps to a considerable extent with disinformation but some nuances need to be brought: **not all disinformation is FIMI, and FIMI is not only disinformation.** Eventually, the phenomenon pushes us to consider state-sponsored manipulations of information in a new light, at the crossroads of influence operations and cyber-security, to develop effective countermeasures better.

The main developments are three-fold:

- Firstly, a refocusing of interest on behaviour and operating methods;
- Secondly, increased use of terms and processes from cyber-threat intelligence (CTI);
- Thirdly, a holistic approach mobilising whole-of-society's resources, favouring the adoption of common terminology.

This evolution is welcome as it sets the bases for a better collective appropriation of threat terminologies and responses. However, it will have to translate from a descriptive effort to an actual operational framework to expand its impact on the information ecosystem and impose costs on disinformation actors.

I. PREVIOUS LITERATURE

The issue of foreign digital interference came to the attention of the EEAS in 2019 as a result of various incidents, as well as press reports and OSINT investigations covering the matter. At this point, the potential benefits of standardising the description of observed incidents and the terminology used by the community emerged. The Att&ck framework was taken as the model for "the core of the anti-disinformation community resilience building work" for the years to come.

This evolution has then developed into two documents. The first one is the EU toolkit for imposing costs on malicious actors. The second document is the Strategic Compass 2022 (pages 39 and 40), which mentions the hybrid toolbox, within which a dedicated FIMI toolbox would be developed. Finally, at the beginning of 2023, the Service published its first report on FIMI, which concludes this doctrinal evolution.

It can be noted that the choice to maintain a very clinical approach to FIMI, focused on operating modes and detached as much as possible from the content or the actors, also responds to strong political constraints and consensus requirements demanded by the different perspectives of the Member States and international partnerships.

However, this concept renewal is welcome, as disinformation was too often attached to the unfortunate term 'fake news'. In contrast, malicious actors have long understood that the best influence operations are not simply limited to false information.

II. DEFINITION

The FIMI definition offered by the EEAS is the following:

> "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."

This definition's wording is meaningful and is worth studying in full detail. Let's unpack it:

- **"Mostly non-illegal".** This makes it challenging to counter the phenomenon using the existing legal framework. Therefore, it pressures law-makers to establish new sets of rules. However, this is not the first time that platforms' policies have faced such a dilemma; "harmful content", as viewed by the Terms of Service of many platforms, is often not illegal per se.

- **"Pattern of behaviour".** While counter-disinformation activities often look at the content, tackling narratives, this definition **shifts the focus from content to behaviour,** as intentional information manipulation constitutes FIMI (a complete list of these behaviours is discussed below). The pattern of TTPs (Tactics, Techniques, and Procedures) also leads to actors, as we will see later. The EEAS report highlights that this approach "enables us to expand our toolbox of counter-measures in addition to the focus on strategic communication as well as pre- and debunking of misleading or false narratives".

This behaviour-centric focus is also a consequence of the European Commission's institutional difficulty in engaging with content, which is often very political by nature, and the need to be cautious towards actors (currently addressing only Russia and China). Consequently, in the "ABC", "ABCD", or "ABCDE" of disinformation, it is forced to focus on "B". It also mirrors the efforts of platforms to tackle behaviours, such as Coordinated Inauthentic Behaviour (CIB) - foreseen in Meta policies.

- **"Threatens or potentially impacts values, procedures, and political processes".** FIMI is strategic by nature and menaces the citizens' perception of political integrity.

If the EU definition of FIMI aims primarily at political disinformation, it also includes any information manipulation that may cause public harm, especially on topics such as health, the environment, or security. Therefore, four main domains are prioritised:

  - o Political disinformation that either tends to favour one side of the competition or undermines trust in institutions or the democratic process;
  - o Health disinformation, which endangers communities;
  - o Environmental disinformation, especially related to climate;
  - o Disinformation that may pose a security threat or disrupt the public order.

- **"Manipulative, intentional, and coordinated".** FIMI operations use manipulatory tactics aimed at misleading, deceiving, and destabilising their target. These targets are often democratic societies, but foreign interference and interference are to be found worldwide, including in developing countries.

To conclude, the essential points to remember are that in their FIMI operations, threat actors: (1) use deception, (2) intent to harm, (3) can be identified as groups or entities, and (4) follow patterns.

III. A FRAMEWORK TO MAP AND CHARACTERISE INFORMATION INCIDENTS

Another approach to document information attacks within the FIMI framework is to identify behavioural patterns that could support counter-measures or identify signatures of specific threat actors.

3.1. TACTICS, TECHNIQUES, AND PROCEDURES (TTPS)

In the acronym "TTPs", Tactics describe the operational goals that the threat actors try to achieve, Techniques are the actions depicting how they try to accomplish them, and Procedures are the specific combination of techniques across multiple tactics (or stages of an attack) that indicate intent and may be unique for different threat actors.

3.1.1. TACTICS

As developed in the EEAS report, they are often described using the "5D model":

- **Dismiss** allegations and denigrate the source, like the claim that Kyiv orchestrated the Bucha massacre to discredit the Russian army.
- **Distort** the narrative and twist the framing, as in the conspiracy that the discovery of alleged US biolabs in Ukraine would justify the Russian "special military operation".
- **Distract**, to shift attention and blame to a different actor or narrative, e.g., stating that the West demonises Vladimir Putin and is responsible for hindering negotiations.
- **Dismay** to threaten and frighten opponents, as shown by the way Russian political opponents, dubbed as a "fifth column", face murder, intimidation, and draconian laws.
- **Divide** to generate conflict and broaden divisions within or between communities and groups, for instance, spreading the hoax that a Ukrainian court has ordered the demolition of an Orthodox church.

3.1.2. TECHNIQUES

Techniques can be sorted according to the stage of the operation, i.e., plan, preparation, and execution. In order to work with common terminologies, specific codebooks have been developed in the past years.

This DISARM framework is "the open-source, master framework for fighting disinformation through sharing data and analysis and coordinating effective action. The framework has been developed, drawing on global cyber-security best practices. It is used to help communicators, from whichever discipline or sector, to gain a clear shared understanding of disinformation incidents and to immediately identify defensive and mitigation actions that are available to them". It provides a set of possible counter-actions to every hostile act, divided into the four typical phases of an attack: plan, prepare, execute, and assess (see Figure 3 on page 18).

It updates and replaces the former Adversarial Misinformation and Influence Tactics and Techniques (AMITT) framework for describing disinformation incidents. FIMI threat analysts and strategic communications practitioners within governments, international organisations, platforms, academia, private industries, and civil society recommend its use.

The European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE) issued a report showing the application of the DISARM framework to a specific case, Operation Ghostwriter, in order to provide an example of its implementation.

The table below shows examples provided in the last EEAS report. A distribution of TTPs can be used whenever an influence operation is detected. To exemplify their practical use, we highlighted some of the different techniques found in the Doppelganger operation uncovered by the EU DisinfoLab in September 2022 (in bold in the table below).

PLAN	PREPARE	EXECUTE
• **Degrade adversary** • **Discredit credible sources** • Facilitate state propaganda • **Geographic segmentation**	• **Develop image-based content** • **Develop video-based content** • Formal diplomatic channels • **Reframe context** • **Develop text-based content** • **Leverage existing narratives** • **Respond to breaking news events or active crisis** • **Prepare assets impersonating legitimate entities** • **Appropriate content** • **Distort facts** • Aggregate information into evidence collages • Develop new narratives • **Deceptively edit images (cheap-fakes)** • Obtain private documents • **Leverage existing inauthentic news sites** • Reuse existing content • Co-opt trusted sources • **Use hashtags** • Create inauthentic documents • **Create inauthentic websites** • **Amplify existing conspiracy theory narratives** • Develop AI-generated videos (deep-fakes) • Develop memes • Create hashtags and search artifacts • Deceptively labelled or translated	• **Post across platform** • Flooding the information space • Call to action to attend • Post across groups • Continue to amplify • Dox • Encourage attendance at events • **Cross-posting** • **Inauthentic sites amplify news and narratives**

Table 1. Techniques of FIMI collected in the first EEAS report on FIMI (page 14). Bolded expressions are elements encountered in the Doppelganger operation.

3.1.3. PROCEDURES

Crossing tactics and techniques allows us to identify procedures, which can be visually represented through TTPs frequency heat charts as the one reported below, which is taken from the EEAS report. Based on the data analysed, FIMI is mostly intended to distract and distort and is mainly image-based. However, generalisations invite caution as these conclusions are drawn from a limited number of 100 incidents over a few weeks (from October to December 2022).

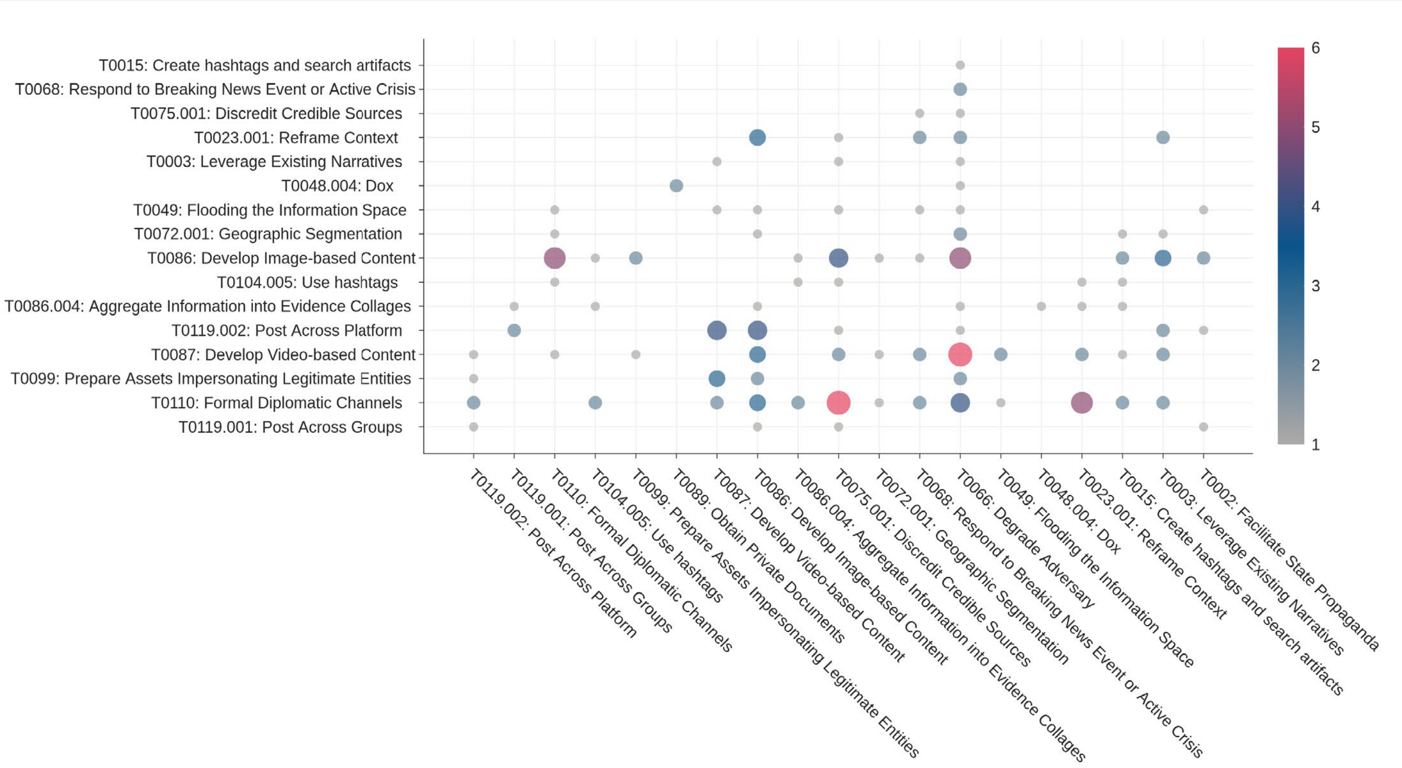

Figure 1. Combination of TTPs identified in the first EEAS report on FIMI and their frequency (page 15)

If, in the same way that malware is connected to APTs (Advanced Persistent Threats) in cyber-security, influence operations can be linked to actors that are a kind of "informational APTs", it could be possible to make attributions using patterns or signatures. The distribution of the points on the graph and their size could let recognise routines in the operator procedures.

3.2. ASSESSING THE IMPACT OF AN INCIDENT

The assessment of a FIMI incident's impact determines its response. Measuring the impact of an influence operation is challenging and sometimes controversial. The relation between reach and impact is not obvious, as some hoaxes may be viral but drive no to minimal offline consequences.

Previous efforts to measure the impact of a disinformation campaign count on Ben Nimmo's "Breakout scale", which considers its capacity to spread outside its original platform and community. Focusing on single hoaxes, EU DisinfoLab's Raquel Miguel elaborated a multi-factor "impact-risk index", considering, among other factors, whether the deception includes a call to action. An impact assessment should generally consider elements as the reach – i.e., how accessible the message is inside and outside of the reference group; the engagement it has generated; or the offline harm, e.g., a call to action. Overall, this assessment will determine a counter-measure's need, format, and scale.

IV. DESIGNING COUNTER-MEASURES TO MITIGATE FIMI OPERATIONS

Just like a malware is attributed to an APT that produced or used it, FIMI actors should be considered and classified as APTs. The counter-measures envisioned so far are in line with this vision.

4.1. "COURSE OF ACTION": A TYPOLOGY OF RESPONSES

If, based on the impact assessment, the relevant stakeholder (e.g., a state actor, platform, media, or civil society) decides to respond to an incident, the EEAS report lists as possible actions:

- Refusing the claims of the incident by issuing a statement ("statement of refutal");
- Fact-checking or debunking the claims;
- Deleting the content or limiting access to it;
- Deleting the channels or accounts involved or restricting or suspending access to them.

4.2. OTHER COUNTER-MEASURES TOOLBOXES

Countering FIMI operations highlights the necessity to enhance the interoperability of frameworks (i.e., their ability to connect and communicate in a coordinated way) and standards of reference, hence establishing a common taxonomy to address the issue. Several concepts were recently explored in this regard, many of which are inherited from the field of cyber-security.

The EEAS report includes a series of frameworks in its counter-measures toolbox, which are recapped as follows.

- **The DISARM framework.** In the previous section on TTPs, we showed the table summarising all the manoeuvres that a hostile actor carrying out an influence operation is likely to use at each stage of its process. For each stage, the DISARM model proposes a range of possible responses, labelled as the "Blue Framework".

- **The "kill chain".** Based on the observation that threat actors performing an information operation follow a series of steps to deploy their attack, similar to a cyber-attack, the kill chain concept invites one to understand the attacker's behaviour and anticipate it in order to "kill" the attack by blocking the operation at any of these steps. In a recent article, Meta's leading researchers Ben Nimmo and Eric Hutchins have described how a kill chain model can be adapted to malicious influence operations.

V. CURRENT LIMITS AND POTENTIAL EVOLUTIONS

5.1. A LIMITED SCOPE OF ACTORS FOR EU INSTITUTIONS

According to the EEAS definition, FIMI operators “can be state or non-state actors, **including their proxies inside and outside** of their own territory”.

States remain central FIMI threat actors. They can act directly through their governmental and diplomatic channels (though routine diplomatic influence alone, which is not associated with disinformative tactics and is not FIMI, as we explained here). They may act using state-controlled media or channels that are linked to them (e.g., organisations politically aligned with their interests), or private contract organisations that have no political design but perform disinformation-for-hire (like the “Team Jorge” revealed by Forbidden Stories).

However, the EEAS admits that its mandate and strategic priorities have limited the focus on influence operations conducted by two state actors, namely Russia and China. Significant differences emerge in the aims and processes of these two threat actors. On the one hand, Russia primarily seeks to divide the foreign public, creating or reinforcing divisions between and within countries. This divide et impera strategy wishes to reduce the ability of the international community to oppose the Kremlin's strategic designs. This tactic was especially noticed in the framework of the war in Ukraine. On the other hand, China makes greater use of its economic power to silence dissenting voices via state-controlled media with inflated audiences or paid influencers.

But a restriction to specific actors leaves out large grey areas. For instance, the malign actors recently exposed by the Forbidden Stories journalistic collective reveal profiles – affiliated or unaffiliated to a state – that are much more varied than those linked to Russia and China alone. Moreover, a single actor-based approach could prevent analysts from identifying new behaviours or doctrine evolutions, as FIMI operators evolve in their playbook, constantly responding to counter-measures implemented by platforms or other stakeholders.

The qualification of FIMI is also disrupted by a phenomenon that has been increasingly observed in recent years: the domestication of influence operations. A foreign threat actor has a strong interest in conducting its operations via local proxies as much as possible, which allows it to gain efficiency – as local agents know local cultural codes – and make any attribution more complicated. Ideally, the threat actor has only loose ties to their proxies and manages to command them from afar as long as they propagate favourable narratives.

5.2. INCLUDING REGULATION MEASURES IN THE RESPONSE FRAMEWORK

The current response framework is mainly oriented towards the observation of content responses or platform actions. This constitutes a classic response from EU institutions as the mandate to respond to information incidents is not always defined, as shown in the past point touching on actor focus.

However, in this field, policy and regulation responses are unfolding, especially around the Digital Services Act, regulation on political advertisement or AI, and other sanctions. Therefore, it would make sense to update the framework response to include these mitigation measures which go beyond content moderation responses. Response frameworks could also integrate actions that allow a better identification of actors, for instance, as well as identify current flaws.

Such efforts are already being integrated in the DISARM matrix, including a "Green" framework, which could be envisioned as workaround measures a FIMI operator would implement to evade accountability.

5.3. WORKING COLLECTIVELY ON FIMI: BUILDING A COMMUNITY OF DEFENDERS

As mentioned earlier, the potential of this framework would be to foster better collective and cooperation efforts beyond EU institutions.

The Structured Threat Information Expression (STIX™) is an open-source language and serialisation format used to exchange cyber-threat intelligence (CTI). The EEAS started encoding FIMI incidents in the Structured Threat Information Expression (STIX™) format, which aims to develop a structured language for describing cyber-threat information to share, store, and analyse in a consistent manner. The advantage of breaking FIMI incidents into its different building elements is that even partial information helps increase situational awareness.

The EEAS has tasked a consortium to develop an Information Sharing and Analysis Centre (ISAC) to adapt DISARM and STIX to FIMI, allowing to encode and share research via interoperable data standards, but also flag findings and use cases not represented in commonly shared standards and taxonomies to the respective maintainers of these frameworks.

VI. CONCLUSION

FIMI is a growing political and security challenge highlighting the need for a common defence framework. Adopting a whole-of-society approach will be needed to enhance resilience and leverage the broadest capacities and competencies. However, this can be realistically achieved only if the large variety of actors engaged in countering FIMI speak a common language. Initiatives such as the DISARM and STIX frameworks constitute that common language, set up to normalise the monitoring, analysis, assessment, and response to FIMI operations.

This process must still be developed and mainstreamed, which will involve training cohorts of researchers and raising awareness among practitioners and policy-makers. Moreover, although domestic influence operations are, by essence, not FIMI, the tools designed to fight the latter can help tackle the challenges of the former. This is all the more important as the boundary between domestic and foreign operations is often blurred, even deliberately blurred, by threat actors that exploit the infrastructures of their targeted countries as proxies.

However, the shift in doctrine initiated by the EU will raise new questions. While the change of focus from content (and the obsession with the ill-named "fake news") to behaviour is refreshening, it should not be exclusionary, nor should it sacrifice the analysis of narratives, the verification of facts, or the understanding of the political motivations of actors. Similarly, it would be illusory to think that the solutions and frameworks provided by cyber-security professionals will suffice to solve the challenges posed by information manipulation magically. As for the commendable role of civil society, this is a welcome move but will require quite some training in new complex processes and coordination.

Finally, we welcome prioritising a whole-of-society approach that includes different stakeholders – e.g., civil society, academia, the media, and the private sector – to create a strong community of resilient defenders against informational attacks. Learnings from the past teach that most of the actions to counter-influence operations are actually undertaken before them, and consist in reinforcing the community's natural immunity through media and information literacy, a healthy media landscape, and above all, effective regulation (and enforcement).