

"Observable" Analysis Canvas

Case Id: _____

Source URL: _____

1. Actor/Provenance



Actual individuals, groups, or organizations as well as classes of individuals, organizations, systems or groups (e.g., the finance sector) who publish/circulate the Observable and/or contribute to its content. Channel used to publish the content. The purpose of this component is to help assess the actor(s) involved in the case, and try to identify which kinds of actors produce and engage with the suspected disinformation. Sometimes actors disguise their origins and purposes, or disseminate suspicious content without malicious intent. **Guidelines:** Collect and analyze all available information to make an assessment, including secondary information, such as an attribution made by a digital platform or in a journalistic investigation, and clarify if actor(s) are:

- Individual(s): persons involved acting in their private capacity
- Nonstate actor(s): persons affiliated with private or NG organization
- Media platform: is the platform of distribution independent?
- Political actor(s): does the individual act on behalf of a recognized political entity?
- Foreign state(s): is the actor an agent or proxy of a foreign government?
- Trolls, impersonators, fake personas etc.

2. Content



What kinds of content is within this Observable? This line of questioning can help establish, for example, whether the information being deployed is deceptive or weaponized against specific target(s). The content of the incident provides details on the narratives used, the socio- political context where the incident takes place, which language, style, and content format are used. Stylistic and morphological features, along with sensational titles and writing, misleading framing of facts or the promotion of outright lies in the content can help identify if the Observable is circulated as part of disinformation campaigns. Questions to ask, include [Pamment, 2020]:

- Channel: What is the channel wherein is this content published?
- Truthfulness: Is the content verifiably untrue or deceptive?
- Vulnerability: Does the content exploit a particular vulnerability of its intended audience or target?
- Language(s): Which languages are used in the spread of the disinformation or other online content in question?
- Synthetic: Is the content manipulated or artificial?
- Expression: Is the content reasonable self-expression protected by fundamental freedoms?
- Harm: Is the content harmful?
- AI: Does the content appear to be drafted by generative AI?
- Micro-targeting: Does the content appear to be crafted for dissemination through micro-targeting platforms?
- Target: Is the content targeting a particular person, institution, organization or country?

3. Timing



What is the timing of this Observable's circulation? Are there any current events of relevance; for example election campaigns, major political developments or public controversies of relevance that may attract the attention of the public opinion?

5. Tactics, Techniques / Behavior



This component assesses to what extent deception, manipulation or other illegitimate communication techniques could be applied in the Observable under analysis. Also, it seeks to discover tactics used, which describe operational goals that threat actors are trying to accomplish. The component can also be used to analyze an actor's intent and evidence of manipulation or coordination, which are indicators of problematic behavior that could help shape potential countermeasures. Tactics, Techniques, and Procedures" are patterns of behaviour used by threat actors to manipulate the information environment with the intention to deceive. Tactics describe operational goals that threat actors are trying to accomplish. Techniques are actions describing how they try to accomplish it. 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

Guidelines: Apply different frameworks to identify the application of possible Tactics, Techniques, Procedures or Strategies used in disinformation campaigns. Add here tags describing the identified tactics and strategies. Please use:

- The DISARM framework analysis and taxonomy, which comprises a comprehensive definition of tactics, techniques and procedures used in disinformation campaigns
- The DEPICT analysis framework, which defines "Six degrees of manipulation" often found in disinformation campaigns
- CONSPIRE, the Conspiratorial Thinking Analysis framework, which defines key tactics used when exploiting conspiratorial thinking to spread and/or amplify disinformation
- Stereotypes prevalent in the social and political milieu of the targets of this Observable, which may be exploited to amplify the propagation and acceptance of the story at hand
- POLAR to determine polarizing entities and concepts from news articles, which may be weaponized by the Observable's content to attract or dismay target audiences
- Exploratory analysis of the content to identify whether the content at hand seeks to promotes/amplify its message using false dichotomies, scapegoating or fear-mongering

Kill-chain phase:

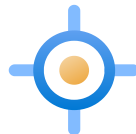
4. Context / Theme / Narrative



Based on the preliminary analysis of 1.Provenance/Actor, 2.Content and 3.Timing, what is a broader socio-political, economic context that could provide a plausible framing for the main points and/or targets of the Observable's message and/or story? Does the content align with known disinformation narratives, stereotypes against social, ethnic, racial, gender groups, conspiratorial thinking, explicit or hidden political objectives and agendas?

Contextualization and Narrative Analysis
Identify and classify the theme of the Observable's content into a broader theme of political, social, financial or cultural theme. Apply Narrative Theory to extract from the Observable's content its core narrative elements. Explore if identified narrative(s) align with known disinformation narratives?

6. Objectives



What are the presumed objectives of this Observable?
What is the evidence from blocks 1-5 that these Objectives are plausible? How are these objectives linked to narratives?
What are the manipulation objectives of this Observable?

Does the Observable seek to achieve one of the following objectives?

Dismiss
Distort
Dismay
Distract
Divide

Does the Observable pursues one or more of the following degrees of Manipulation?

Discredit opponents
Using Emotional Language to attract attention and/or support
Instigating inter-group polarization
Creating Moral Outrage to gather support and/or polarize
Building audience & follower base for fake accounts/impersonation
Spreading conspiracy theories
Evoke Outrage through Trolling

7. Target Audience / Degree



What is the distribution of the content? Which audiences were targeted and reached?

The degree dimension attempts to gauge and describe the way the Observable has travelled through the information environment, possibly crossing different channels (shared via Social Media, story picked-up by other news media, etc), targeting different linguistic, ethnic, social or age groups. This view on disinformation operations can reveal threat actor preferences with regards to targeted platforms and identify different roles of channels in a network as source, amplifier or link to other networks.

Examples
Societal/ethnic/political/national groups
Massive
Micro-targetting

8. Attribution



Is there any evidence about who is behind this Observable, whether it might align with known actors? Evidence can be derived from the profile of the Actor or prior information activities of or positions expressed by or credible analyses published for the Actor. Sometimes the attribution can be obvious, as for example when the Observable promotes stated and documented political objectives, if the originator is a state actor identifying with those objectives or even if its originator is not a state actor or an individual affiliated with the organization having those objectives.

9. Impact / Effect



What is the overall impact of the Observable and whom does it affect? This question can help establish the actual harms and severity of the case. The effect of an Observable (or the impact or severity) can be measured and assessed according to different parameters such as the reach, the reach outside of in-groups, engagement, harm or behaviour-change caused offline, longevity etc.

Reach
Immediate audience
Reach outside in-groups

Organic Engagement
Do the recipients of the Observable appear to engage with it, commenting or sharing it within its publication platform or beyond, in other channels?

Longevity
Does the Observable attract an interest from audiences that is persistent with time? For how long?

10. Countermeasures



Which steps can be taken to address the Observable at hand, if it contains misleading or manipulative content?

Possible Approaches
Debunking
Refutation
Steps to confine the circulation of the Observable
Expose TTPs
Raising awareness about misleading narrative

Glossary

According to the European External Action Service's definition, an **observable** is a "concrete element 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."

According to the European External Action Service's definition, **Foreign Information Manipulation and Interference (FIMI)** describes "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."