Disinfo. Incident Analysis Canvas.

TITLE :

Incident Id:

1. Description

What is this Incident **about**?
What is the **story** conveyed by the Incident's Observable(s)?
What are the apparent **targets** of the disinformation attack?

Associated events: what real-world events this Incident refers to or associate with?

Consider:

- *Electoral events*
- *Military or security incidents*
- *Diplomatic negotiations*
- *Communication by public figures*
- *Political summits*
- *Public policy outputs*
- *Observances*

Timeline of Incident:

- **What is the timeframe** that this incident occurred?

List of Observable(s)

Provide a list of:

- *ObservableID, Description, Format*

2. Target

What is the target of the attack behind this Incident?

Consider:

- *Individual Person*
- *Cultural / Religious / Ethnic /Professional Group*
- *Institution*
- *Organization*
- *Country*
- *International Alliance*

3. Context / Theme

What is the **broader socio-political, economic context** that could provide a plausible framing for the main points and/or targets of this Incident?
What themes, stated or implied political and other agendas have the same target with the Incident and provide a reasonable frame for it?

4. Narrative

What is the key Narrative promoted and/or amplified through this Incident, based on its Description, the apparent Target of the attack, and the identified Context?
What known narratives, stereotypes against social, ethnic, racial, gender groups, or conspiracy theories, explicit or hidden political objectives and agendas?

Perform Contextualization and Narrative Analysis:

- *Apply Narrative Theory to extract from the Incident's description and target its core narrative elements.*
- *Identify and classify the Incident's narrative into a broader frame of political, social, financial or cultural theme.*
- *Explore if identified narrative(s) align with known disinformation narratives?*

5. Tactics, Techniques, Procedures

How are the actor(s) of this Incident trying to manipulate the information environment with the intention to deceive their target audience(s)? *Consider:*

- *The extent to which deception, manipulation or other illegitimate communication techniques appear to be applied in the Incident under analysis.*
- *The tactics used, which describe operational goals that threat actors are trying to accomplish.*
- *Analyzing an actor's intent and evidence of manipulation or coordination, which are indicators of problematic behavior that could help shape potential countermeasures.*
- *Discovering **Tactics**, which describe operational goals threat actors are trying to accomplish.*
- *Discovering **Techniques**, which describe how actors try to accomplish their operational goals.*
- *Analyze possible **Procedures,** namely specific combination of techniques across multiple tactics (or stages of an attack) that indicate intent and may be unique for different threat actors.*

DISARM: use the DISARM framework analysis and taxonomy to map the TTPs identified

DEPICT: select one or more degrees of manipulation identified in this Incident:

☐ Discrediting ☐ Emotion ☐ Polarization
☐ Impersonation ☐ Conspiracy ☐ Trolling

CONSPIRE: use the CONSPIRE framework of analysis to identify conspiratorial techniques applied in the Incident at hand:

☐ Contradictory ☐ Nefarious Intent ☐ Persecuted Victim
☐ Overriding Suspicion ☐ Something must be wrong ☐ Immunity to Evidence
☐ Re-interpreting randomness

KNOWN MISINFORMATION STRATEGIES: identify if known strategies apply in this Incident

☐ Moral Outrage ☐ Impersonation ☐ Amplifying Stereotypes
☐ False Dichotomies ☐ Scapegoating
☐ Fear Mongering ☐ Spreading Conspiracies

Kill-chain Analysis: explore if the incident can be mapped to one of the kill-chair analysis' phases:

☐ Step 1: Find the cracks ☐ Step 5: Conceal your hand
☐ Step 2: Seed distortion ☐ Step 6: Cultivate Useful idiots
☐ Step 3: Wrap narratives in the kernel of truth ☐ Step 7: Deny involvement
☐ Step 4: Build audiences ☐ Step 8: Play the long game

6. Objectives

Explain **why** are the attack(s) captured in this incident launched?
What are the presumed objectives of this Incident based on evidence and analysis collected from blocks 1-5 ?
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, as identified in block 5?
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. Attribution / Actor

Identify **who** could be behind this incident?
Actual individuals, groups, or organizations as well as classes of individuals, organizations, systems or groups (e.g., the finance sector) who appear to have a motive to orchestrate this Incident and/or contribute to its content and narrative.
Guidelines: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.
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.

8. Channels

Where has this Incident been manifested?
Which channels were targeted and reached?
Where has this Incident gained traction?
How different platforms have been weaponized to support the attack behind the incident?

Channel list (non-exhaustive)

☐ Web
☐ Facebook
☐ Twitter
☐ TikTok
☐ Instagram
☐ Reddit

9. Audience / Degree

Which is the audience(s) targeted and reached by the attack behind this incident?
What is the distribution of the content?

The degree dimension attempts to gauge and describe the way the Incident 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.

10. Vulnerabilities

How do the objectives, the narrative, and the TTPs of the attack behind this incident resonate with vulnerabilities of the target audience(s).

Provide a list of vulnerabilities, which may have been weaponized to propagate and/or amplify a particular narrative.

Vulnerabilities can be identified through ethnographic studies, polls and questionnaires, media analysis, etc.

Consider vulnerabilities such as:

- Stereotypes about and distrust towards particular social, ethnic, religious, gender etc groups
- Distrust towards authorities, politicians, "the system"
- Common beliefs
- Polarized thinking and affective polarization
- Popularity of conspiracy theories
- Suspicion towards media, the political and judicial system

11. Impact / Effect

What is the overall impact of the Incident and whom does it affect?
This question can help establish the actual harms and severity of the case. The effect of an Incident (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.

Establish metrics and gather quantitative and qualitative evidence regarding impact through measurements, polls, etc. For example:

- *Has the incident penetrated national media?*
- *Has it become a matter of discussion and/or conflict in political fora?*
-

12. Countermeasures

Which steps or combination of measures can be taken to address the Incident at hand, if it contains misleading or manipulative content?

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

Glossary

European Union's External Action Service defines a FIMI **incident** as "an action perpetrated by one or more threat actor(s) pursuing specific objectives and carried out with the intent to deceive. It is composed of a combination of observables and TTPs. Multiple related incidents can be part of a campaign."

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."