|  |  |  |  |
| --- | --- | --- | --- |
| **CDN Incident Alert: 0001. TLP: CLEAR** | | | **Date** |
| **Title** | DE | Use the same title as the report. If no report is present, a suggestion is to use the format: Actor, doing what to who | 28/06/2024 |
|  | | | |
| **Summary –** Incident - 1-2 Sentences, Narrative – 1 sentence. Impact, DISARM TTPs, Recommendations | | | |
| - Summary of incident - 1-2 sentences  - Summary of narrative - 1 sentence  - Summary of impact  - Summary of DISARM TTPs  - Summary of recommendations. | | | |
|  | | | |
| **Incident** – When, Who, did what, to say what, to whom, why? | | | |
| Describe the scope of what you found. | | | |
|  | | | |
| **Narrative** - separate with ; | | | |
| Meta narrative: Degradation of the West; Technological progress endangers public safety. Sub-narratives: German government is failing its citizens by supporting Ukraine over domestic issues; EVs are unreliable and prone to explosions and accidents | | | |
|  | | | |
| **Impact** | | | |
| Reach (views, shares, likes etc):  Outcome (real-life event): | | | |
|  | | | |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Key Objectives and Behaviours (**[**DISARM Red Framework**](https://disarmfoundation.github.io/disarm-navigator/)**)** (Max 2 objectives and 4 TTPs). | | | | | |
| Objective: Title of objective TTP – justification.  Objective: Title of objective TTP – justification  TTP 1 - explanation.  TTP 2 - explanation.  TTP 3 - explanation.  TTP 4 - explanation. | | | | | |
|  | | | | | |
| **Recommendations and Actions Taken** (end each recommendation with a ;) | | | | | |
| Action taken (e.g. reported page to Meta, sent article to journalists, reported case to regulator):  Recommendations: | | | | | |
|  | | | | | |
| **Report** | **Threat Actor** | **Evidence** | **Authors** | **Platforms** | **Logo** |
| Link | Russia, China, etc. | Reference/link to report, external document, or folder. | Name, organisation | E.g. Facebook, X, YouTube. |  |

**Delete before sending!**

**One-page Template Guide**

**[TLP](https://www.cisa.gov/news-events/news/traffic-light-protocol-tlp-definitions-and-usage" \l ":~:text=TLP is a set of,not considered valid by FIRST.): Amber+Strict**

When we initially started developing the CDN, we spoke with responders about the challenges they face in their work. One of the key points raised was that they were being flooded by reports and findings, using different formats, definitions, and methodologies.

In those conversations, the methodology and one-page template were born.

The core purpose of the one-page template is to give a clear and quick standardised overview of a case or report, allowing a responder to quickly decide if it is relevant for them to read the full report, pass it on to someone else, or ignore it.

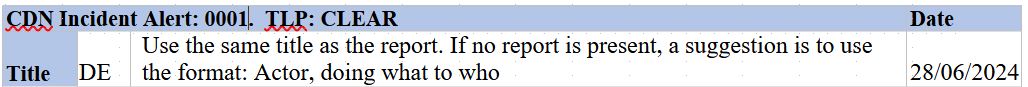
The one-page template can be longer than one page in specific circumstances, especially when there are a lot of contributors that need to be credited. We recommend that you do not pass two pages. You can always link to a longer report with all the details of your case.

The template's different components are explained below. The same text can be found in the one-page template.

Only the header, summary, and incident section of the incident alert are obligatory for you to fill out. You can also work with others to complete the other sections of the incident alert, including asking us for help. While the template comes with instructions on how to use it, consider these as recommendations. At times, parts of the information we request do not exist or are not within the scope of your research, which is fine.

Feel free to contact Sam (Saman Nazari) if you need any help filling out the template.

**Header**



Each header has 6 components:

 1. The type of template, in this case, a Counter Disinformation Network Incident Alert.

Currently, we use Incident Alert, to indicate that we are reporting on an urgent actionable case, and Report Summary, summarising a larger report not of an urgent nature.

2. The number of the one-pager, in this case 0001.

3. Traffic Light Protocol – indicating how publicly the one-pager can be shared.  
  
TLP: Red - Not for disclosure, restricted to individual participants only.  
TLP: Amber+Strict - Limited disclosure, restricted to participants’ organization.

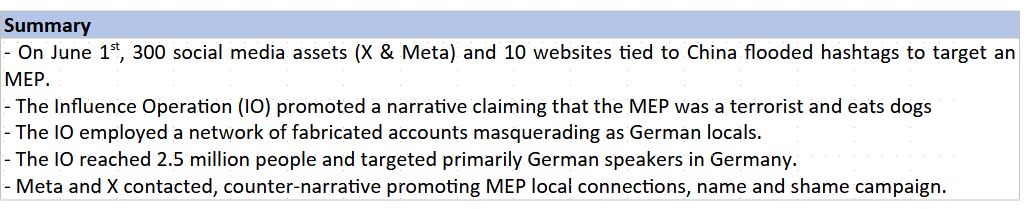
TLP: Amber - Limited disclosure, restricted to participants’ organization and its clients  
TLP: Green - Limited disclosure, restricted to the IO/disinformation-countering community  
TLP: Clear - Disclosure is not limited.

4. The country or region being targeted, in this case, Germany (DE). Can also be larger geographical areas, like the EU.  
  
5. A title. Up to you to decide.

6. The date of the incident’s publication, in this case, 28/06/2024.

**Body**

Summary



While this will be the first text facing the reader, it will be the last text you will write. This section of the one-pager is meant to summarise the rest of the alert. Each sentence should be a summary of the different parts of the one-pager. There are no strict rules around how the different sentences should look, but we recommend that you write the summary in the same order as the information is presented in the rest of the one-pager.

When possible, we believe that the most efficient way of using the summary is to in the first sentence try to clearly include the platforms used in the influence operation, in this case, X and Meta, the size of the influence operation, in this case, 300 social media assets and 10 websites, who is behind it, in this case, China, and its targets, in this case, a Green MEP.

The second line can indicate the key narrative.

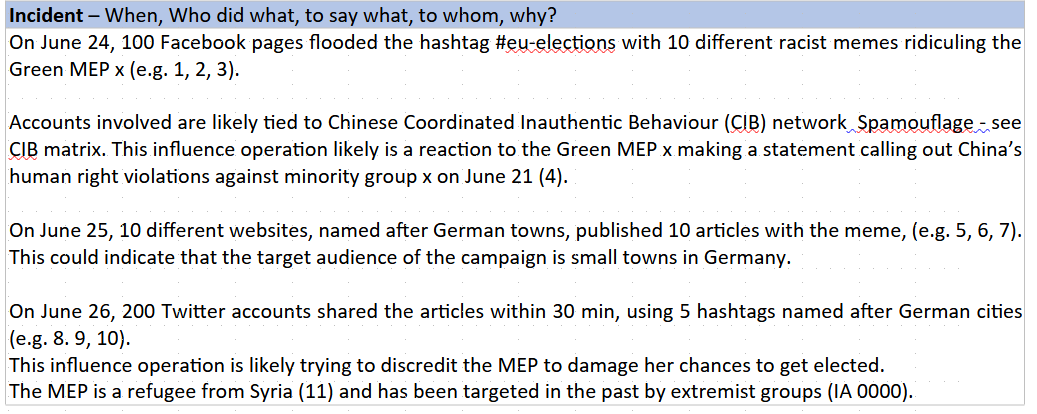
The third line can indicate the key DISARM tactics and techniques.

The fourth line can indicate the impact.

The last line can indicate actions taken and recommendations.

Inciedent

The incident section of an alert should begin with the date of the first observed activity or piece of content. It should specify when someone did something to say something to whom and the reason for doing so. As long as you include these components, it’s up to you to decide what format of writing works for you.



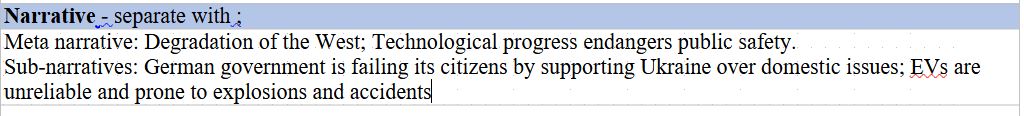
In this section, you can provide contextual information about who is behind the activity, and why it is happening right now. You can specify which platforms are being used by the threat actor and the scale of things, e.g. how many accounts did something.

When possible, you can reference old cases including the same target or the same threat actor using the same technique.

Make sure to have in-text references for all your claims using archived links. When not possible due to the amount of links or type of evidence, attach a link to an external document with the evidence included. You can also use Hunchly to record the evidence.

If the one-pager is summarising a larger report, feel free to leave out the sources as long as you provide them in the report itself.

Narrative



To describe the narratives, please include the overall narrative, which we call the meta-narrative.  
Then indicate the sub-narratives building up that meta narrative.

We recommend that you focus on one or two meta-narratives. You can also choose to focus on only meta- or sub-narratives, depending on the scale and scope of the case you are covering.

A larger influence operation such as Doppelganger can involve many narratives. You can either reference the key ones that stand out or are new, or list them all if you have the space. Remember that you can always publish a larger report with all the narratives in them and that the alert should act as a summary.

You should avoid having overlap between these narratives.

Meta narratives are overarching ideas or concepts that the threat actors are trying to sell us, such as the West is falling, U.S. is corrupt, and the government is not prioritising its’ citizens.

Sub naratives are the smaller narratives that build up the meta narratives, such as U.S. government officials gives government contracts to their friends, the government priorisises funding refugees instead of helping their population, the government is prioritising trans people instead of retired people.

As we lack an unified narrative framework for the community, we want to start listing the narratives we see in our research and start developing a common taxonomy.

The centre of this development is our Narrative tracker, which can be found [here](https://docs.google.com/spreadsheets/d/1tJdZkz9m4NKnpVD25WC36ydELk2_D-EKASvSnGwSvkI/edit?gid=0" \l "gid=0).

As a starting point, we will also use a slimmed down version of Debunk.org’s narrative framework.

We will be using a separate document to create a narrative framework based on our empirical findings. We can collectively develop this framework by adding new narratives to the document as we see them.

The document has three tabs: the first outlines the meta narratives, the second outlines the sub narratives, and the third that has a slimmed down version of Debunk.org’s narrative framework, focusing on narratives that can be used during elections.

Whenever you see a narrative in your cases that can be identified in Debunk.org’s framework, use it and move it to the first or second tab, attributing the author of the narrative as Debunk.org.

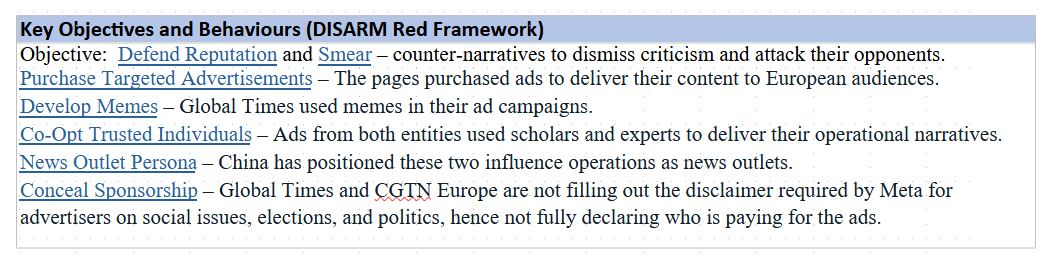
Impact



Impact assessments are tricky. We recommend that you use whichever matrix that works best for you. Examples of proxies for impact include views and interactions, quotations, backlinks, and the spread of a narrative throughout a society.

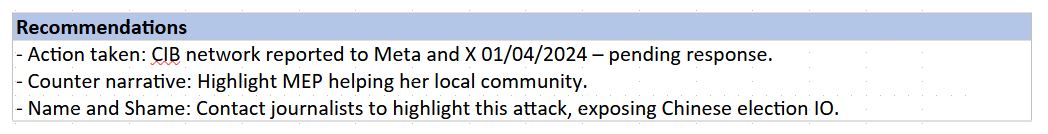
We also recommend you highlight if the influence operation you observed managed to break into public discourse or cause offline events.

Key Objectives and Behaviours



Outline the key objectives (max 2), and manipulative behaviours (max 4) using the [DISARM Framework](https://disarmfoundation.github.io/disarm-navigator/).  
  
Focus on the key manipulative behaviours that made the influence operation successful or interesting to study. Please link to the page of the technique so the reader also can read the definition of the TTP. Techniques can be used to observe the vulnerabilities used in influence operations, helping us shape our recommendations.

Recommendations

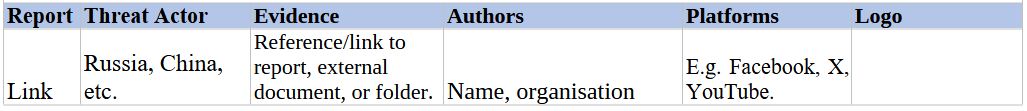


Outline which actions you took to counter the issue yourself, e.g. reporting the network to Meta and X. Alliance4Europe is happy to help you promote your report to responders who potentially can act upon your findings.

By recording when this action was taken, we can also record when and whether the platforms responded or took any actions, allowing us to evaluate the platforms based on if they are following up on their commitments. This data can be sent to the DSA enforcement team at the European Commission, allowing them to take action against the platforms if they do not follow through on their obligations.

Also, provide other recommendations that come to mind. E.g. Counternarratives, name and shame campaigns through media, and recommendations for further research or targeted communication campaigns.

Footer

****

The report section of the footer allows us to link to a larger report that the incident alert has summarized.  
The Topic section can include the 3-4 key topics covered in the incident.

Evidence should contain links to external evidence sheets. In this fictional case, it contains a fictional link to an evidence sheet and a fictional link to a sheet that provides justification for why we are claiming that the network of accounts is a CIB network.

Authors include all contributors to the report and their organisations.  
Platforms include which platforms were used to conduct the influence operation.

Logo allows an organisation to add their own logo.