

# EXAMPLE USING THE FIMI monitoring templates checklist

The three-fold checklist designed to help users apply the three FIMI monitoring templates is tested here on a concrete example to demonstrate its practical use. The selected incident comes from the report [“Assessment of Foreign Information Manipulation and Interference in the 2025 Czech Parliamentary Election”](#) produced by the project “FIMI Defenders for Election Integrity”, of which EU DisinfoLab is a partner.

More specifically, the case concerns the Russian state-affiliated outlet “neČT24”, which emerged in 2022 as the successor of Sputnik CZ. Since August 2025, the outlet has systematically spread disinformation and established its presence on Facebook, X, and Telegram, aiming to undermine trust in the 2025 Czech parliamentary elections.

The three-part checklist was completed using information from the abovementioned report and, where indicated, through responsible desk research and analytical support tools. This demonstrates that the checklist is accessible and easy to use even for non-expert users. All responses were cross-checked against reliable sources; nevertheless, the use of tool-supported inputs may entail a risk of inadvertent errors or omissions, hence users should exercise appropriate caution.

FDEI  
PROJECT

FIMI  
-ISAC



## Checklist for incident qualification (PART 1)

<b>A. IS THIS FIMI?</b>		
<b>1. FOREIGN ACTORS</b>		
Are foreign actors engaging in this incident/campaign?*	Yes	No
If yes, are they state or non-state actors? [Researchers found that neČT24 is a Russian state-affiliated outlet]	Yes	No
If yes, are they the initiators?*	Yes	No
If yes, are they the amplifiers?	Yes	No
If amplifiers, is there evidence of a direct connection with the initiators?*	Yes	No
*If the answer is no, then the incident/campaign is <u>NOT</u> FIMI.		
<b>2. BEHAVIOUR</b>		
<b>2.1 MANIPULATION</b>		
Does the incident/campaign show manipulative behaviour?	Yes	No
If yes, does it include disinformation?	Yes	No
If yes, what is the narrative circulated? Conspiracy claims of election fraud accusing the Czech Constitutional Court of wanting to manipulate the elections	Describe	
Did a cyberattack happen before or after the (dis)information was shared?	Yes	No
Does the incident/campaign use other TTPs for manipulative purposes? Leveraging conspiracy (T0022) and existing narratives (T0003), posting across platforms (T0119.002), directing users to alternative platforms (T0122), demographic segmentation (T0072.002), news outlet persona (T0097.202), develop own media assets /T0095), etc	Yes	No
<b>2.2 INTENTIONALITY</b>		
Does the incident/campaign show evidence of intentionality?	Yes	No
Is the purpose of the incident/campaign clear? Discrediting Czech democracy, distorting the reality of the electoral processes	Yes	No
<b>2.3 COORDINATION</b>		

Does the incident/campaign show evidence of coordination? <i>Ratio: presence on multiple platforms</i>	<b>Yes</b>	No
<b>3. IMPACT</b>		
Did the incident/campaign achieve considerable outreach?*** <i>Ratio: thousands of views</i>	<b>Yes</b>	No
Did the incident/campaign achieve considerable engagement?*** <i>Ratio: few likes across platforms</i>	Yes	<b>No</b>
Does the incident/campaign harm/criticise/attack the core values of EU societies? <i>Ratio: attack on democracy</i>	<b>Yes</b>	No
Does the incident/campaign harm/criticise/attack the core procedure of EU societies? <i>Ratio: attack on electoral processes</i>	<b>Yes</b>	No
<i>**Define concepts of outreach and engagement explicitly and set a threshold within the working group or project</i>		
<b>4. INFRINGEMENT***</b>		
Does the incident/campaigns constitute a law violation? <i>Yes</i>	<b>Yes</b>	No
If yes, does it violate national regulations? <i>e.g., obstruction of elections (Section 351 of the Czech Criminal Code), spreading alarming news (Section 357 of the Czech Criminal Code), potential circumvention of EU sanctions against Russian state media (implemented via Act No. 69/2006 Coll.) (Disclaimer: this answer was compiled using desk research – including the “<a href="#">Czechia: Country Election Risk Assessment</a>” report and the <a href="#">Czech disinformation landscape factsheet</a> – as well as AI tools, consulting the cross-checking outputs against reliable sources.)</i>	<b>Yes</b>	No
If yes, does it violate international regulations? <i>Likely yes, considering direct links to sanctioned outlet Sputnik CZ, systemic risks for election integrity and foreign interference</i>	<b>Yes</b>	No
If not, does it constitute a harmful activity? <i>Regardless of legal qualification, the report poses a risk for elections</i>	<b>Yes</b>	No
If not, does it violate the platform's Terms of Service? <i>Yes, platforms demand compliance with applicable law</i>	<b>Yes</b>	No
<i>***No prior legal background is needed. Where helpful, desk research and analytical support tools may be cautiously used to guide the process, always cross-checking and validating outputs against reliable sources.</i>		
<b>FINAL ASSESSMENT</b>		

<ul style="list-style-type: none"> <li>• Low certainty: There is no evidence that the incident is part of a FIMI operation.</li> <li>• Medium certainty: Several of the conditions are met and supported by evidence. The investigator strongly believes the incident is FIMI, but there is not enough evidence to confirm it.</li> <li>• High certainty: All conditions are met and backed by evidence. The investigator can confidentially confirm the incident is part of a FIMI operation.</li> </ul>		
<b>B. SINGLE INCIDENT OF PART OF A CAMPAIGN?</b>		
Does the incident/campaign show evidence of coordination? Ratio: presence on multiple platforms and coordinated posting, in addition to links (confirmed by the Czech Intelligence Service) to Sputnik CZ	Yes	No
Does the single incident show evidence of coordination among foreign actors? If yes, this is a FIMI incident	Yes	No
Do multiple incidents show evidence of coordination among each other? If yes, this is a FIMI campaign	Yes	No
<b>FINAL ASSESSMENT:</b>		
<ul style="list-style-type: none"> <li>• Single incident: There is currently no evidence that the incident is part of a broader FIMI campaign.</li> <li>• Part of a campaign: Multiple incidents indicate that the activity is part of an ongoing FIMI campaign.</li> </ul>		

## Checklist for (systemic) violations (PART 2)

Disclaimer: Using this checklist 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.

### Shorter version:

Incident ID	When was the incident created and registered? The website dates back to 2022, but the Facebook page, X account, and Telegram channel were created in August 2025, while the case was reported in November 2025. Ideally, we would create a separate checklist for each platform, but for the purpose of this exercise we will combine them into a single checklist	Describe	
Assessing the violation	Does the incident/campaign constitute a violation?	Yes	No
Assessing the type of violation	If yes, is it a violation of national or international/EU law? E.g., obstruction of elections (Section 351 of the Czech Criminal Code), spreading alarming news (Section 357 of the Czech Criminal Code), potential	Yes	No

	<p>circumvention of EU sanctions against Russian state media (implemented via Act No. 69/2006 Coll.).</p> <p>(Disclaimer: this answer was compiled using desk research – including the <a href="#">“Czechia: Country Election Risk Assessment”</a> report and the <a href="#">Czech disinformation landscape factsheet</a> – as well as AI tools, consulting the cross-checking outputs against reliable sources.)</p>		
	<p>If yes, is it a violation of the platform's Terms of Service?</p> <p><a href="#">Meta's</a> and <a href="#">X's</a> ToS demand compliance with applicable law, so posting content from a sanctioned entity would constitute a violation.</p> <p>Interestingly, the actions described are not explicitly prohibited by Meta's <a href="#">misinformation</a> or <a href="#">policies and safeguards for elections</a>, or X's <a href="#">civic integrity policy</a></p>	Yes	No
Assessing systematicity [inaction]	<p>Are you aware of platform inaction regarding the incident?</p> <p>The <a href="#">Facebook page</a>, <a href="#">X account</a>, and <a href="#">Telegram channel</a> are still available</p>	Yes	No
Assessing systematicity [inconsistency]	<p>Are you aware of platform inconsistency regarding the incident?</p> <p>We are not aware of any action taken by platforms</p>	Yes	No
Assessing systematicity [recurrence]	<p>Are you aware of the same/a similar incident occurring on the platform?</p> <p>Multiple posts were made on Facebook, X, and Telegram</p>	Yes	No

### Checklist for countermeasures (PART 3)

<b>A. COUNTERMEASURES IN PLACE</b>			
<b>1. STAKEHOLDERS INVOLVED</b>			
Who has taken action (e.g., researchers, platform, victims, etc)		Describe	
<a href="#">Researchers</a> exposed the case and the <a href="#">Czech Intelligence Service</a> confirmed a direct link with Sputnik CZ			
<b>2. ACTION TAKEN</b>			
Were they exposure-related countermeasures?		Yes	No
<a href="#">The incident was covered in reports</a>			
Were they community engagement-related countermeasures?		Yes	No
<a href="#">There seems to have been some information-sharing around the incident between civil society and Czech authorities</a>			
Were they distribution-related countermeasures?		Yes	No

We are not aware of any measures in that sense		
Were they infrastructure-related countermeasures? We are not aware of any measures in that sense	Yes	No
Were they sanctions and legal-related countermeasures? We are not aware of any measures in that sense	Yes	No
Were they media literacy-related countermeasures? We are not aware of any measures in that sense	Yes	No
<b>3. IMPACT</b>		
Did the countermeasures raise awareness of the incident? The report certainly made more people aware of the incident	Yes	No
Did they impact the threat actor capabilities to produce/distribute disinformation? The campaign is ongoing	Yes	No
Did they trigger other actions by the defender community or threat actor(s)? The campaign is ongoing	Yes	No
Did they reinforce the attribution of the incident? It is known that this is a Russian state-linked entity with the same editorial team and operational mandate as Sputnik CZ	Yes	No
Did they deter the threat actor(s)? The campaign is ongoing	Yes	No
<b>4. LEGAL GROUNDS</b>		
Are the countermeasures based on national law, international law, or platform Terms of Service? Currently, there are no legally-grounded countermeasures in place	Yes	No
<b>B. POTENTIAL ADDITIONAL COUNTERMEASURES</b>		
Is there anything more that could be done to stop/mitigate the incident? Reporting the incident(s) through platform mechanism in order to activate a series of DSA provisions against Facebook and X (e.g., Art. 6 on hosting liability, Art. 16 on notice-and-action); enforcement of EU provisions on sanctioned entities, and enforcement of DSA Art. 14 on Terms of Service, which would prevent platforms to host content from sanctioned media	Describe	

A large blue circle containing the text "EU DISINFO LAB" in white. The word "LAB" is enclosed in a white speech bubble shape. A thin black line extends from the top of the circle towards the center of the page.

EU DISINFO LAB

This template was created as part of EU DisinfoLab's contributions to the [FIMI-ISAC FIMI Defenders For Election Integrity \(FDEI\) project](#), an initiative that brought together 10 European organisations to collaboratively detect and respond to FIMI in electoral processes. The project aims to bolster democratic institutions by providing tools, establishing response teams, and creating an operational handbook.

A dark blue circle containing the text "FDEI PROJECT" in white. The "F" is stylized with a grid of dots to its left. A thin black line extends from the top of the circle towards the center of the page.

FDEI  
PROJECT

A black circle containing the text "FIMI-ISAC" in white. To the left of the text is a logo consisting of three overlapping concentric circles. A thin black line extends from the top of the circle towards the center of the page.

FIMI  
-ISAC