ADAC.iO
Attribution Data Analysis Countermeasures Interoperability

FOUR CASE STUDIES ON FOREIGN INFORMATION MANIPULATION AND INTERFERENCE

ADAC.IO Publication – Deliverable 4.2

Elsa Hedling, Lund University
Elsa Isaksson, Lund University
August Kyst, Lund University
Timo Lenk, TU Dortmund University
Hedvig Ördén, Lund University

Contact: rickard.andersson@iko.lu.se | adacio.eu

Co-funded by the European Union

ADAC.iO WP4 Deliverable 4.2

Four Case Studies on Foreign Information Manipulation and Interference

Table of Contents

Executive Summary: ADAC.iO WP4 Deliverable 4.2 – Four Case Studies on Foreign Information Manipulation and Interference

This report brings together four independent case studies produced under the EU-funded ADAC.iO project, each examining a different facet of how the online information environment is exploited to deceive, divide, or defraud through coordinated information operations. Throughout, the reports use the term Foreign Information Manipulation and Interference (FIMI) to refer to coordinated and deliberate efforts by foreign-linked actors to distort the information space of a target society in pursuit of strategic goals. A recurring concern across all four is the difficulty of cleanly separating genuinely foreign interference from domestic actors who partly draw on the same repertoire of tactics and techniques for their own ends. Together, the studies unveil an ecosystem of actors and activities that instrumentalise social grievances and wedge issues, exploit systemic vulnerabilities, and amplify the narratives of foreign and domestic actors alike.

The first report is a qualitative case study of manipulation targeting EU climate policy in the run-up to the 2024 European elections. Analysing thirty articles and blog posts in English, German, and Russian from the election week, it finds a blurred ecosystem in which Russian state media and EU-based far-right outlets deploy near-identical rhetoric and routinely cross-cite one another. Manipulative actors attached their messaging to highly salient events such as the 2024 farmers' protests and the assassination attempt on Slovak Prime Minister Robert Fico, casting climate policy as elite oppression of ordinary people. Its standalone contribution is the demonstration that "flooding" the information space with mutually reinforcing content can lend falsehoods plausibility through sheer repetition, an effect grounded in the psychological "illusory truth effect."

The second report addresses gendered disinformation, which weaponises gender, sexuality, and identity to silence and delegitimise individuals and to polarise societies. Its core contribution is conceptual and methodological: a typology distinguishing five patterns of "gendered FIMI", including targeted delegitimisation, gendered narrative warfare, wedge amplification through gender issues, gendered harassment, and synthetic or manipulated gender-related content such as deepfakes, paired with a vulnerability assessment. The report is candid that gendered disinformation is exceptionally hard to attribute to foreign actors, because it is so deeply embedded in domestic misogyny and authentic political debate, making it better understood, in many cases, as a societal vulnerability that FIMI can exploit rather than a discrete foreign operation.

The third report turns to financial fraud, analysing Facebook scam campaigns that impersonate the Swedish bank Swedbank. Its contribution is to test whether ADAC.iO's updated framework for the attribution of information influence operations is also practically applicable to a wider range of hybrid threats, including relatively apolitical financial crime. The answer is a qualified yes: the scams display markers of coordination similar to those of information influence operations, such as lookalike domains, reused multilingual templates, AI-generated endorsements, and funnels channelling victims toward off-platform deposits; yet the evidence points to financial extraction, not geopolitical aims.

The case usefully marks the analytical boundary of FIMI frameworks: coordination and political intent are not the same thing.
The fourth report examines cross-platform manipulation activities around two high-profile events: the 2025 Munich Security Conference (MSC) and, as a comparative case, the 2025 Moldovan parliamentary elections. The MSC analysis traces how actors seized on U.S. Vice President JD Vance's speech to advance anti-EU messaging through three behavioural clusters, including a "weak European leadership" framing based on the decontextualisation of authentic footage and censorship allegations that instrumentalised salient online debate. Its distinctive contribution is the concept of "agenda-surfing" or piggybacking: rather than running a tightly orchestrated campaign, opportunistic actors exploited an unfolding diplomatic éclat to inject their own grievances across platforms. It also confirmed the interplay of distinct platform functionalities in the disinformation ecosystem; Telegram, for example, functioned as a content reservoir and X drove rapid amplification, while downstream agenda-setting effects could be observed on Reddit.

In terms of shared themes and intersections, the most striking commonality is methodological. Three of the four reports apply the DISARM framework, a shared taxonomy of manipulation tactics and techniques, and the EU-elections and cross-platform cases specifically test its new "Observables" prototype (v2.0), which foregrounds directly observable behaviour over inferred intent. Reports two and three both build on the project's own framework for the attribution of influence operations, which triangulates content-related, behavioural, technical, and financial evidence. This methodological convergence is itself a distinct contribution of the four case studies: collectively, they road-test the consortium's tools and provide feedback toward concrete refinements. Accordingly, the reports share a recurring tactical vocabulary, including impersonation, coordinated amplification through inauthentic accounts, emotional manipulation, decontextualisation, and cross-platform funnelling. Russia recurs as a central actor in the first three, and all four wrestle with the same boundary problems along three dimensions, namely distinguishing foreign from domestic, coordinated from organic, and manipulation from legitimate expression.

What distinguishes the case studies is the axis each explores. The EU-elections study identifies the blurred line between foreign and domestic actors in their rhetoric; the gendered disinformation study locates the attribution problem in the observation that vulnerabilities and harm are structural issues, exploited by orchestrated foreign manipulation as an extension; the financial fraud study points to the problem of assuming a direct between coordination and intent, showing identical tactics serving non-political ends; and the cross-platform study points to the global scale of opportunistic, event-driven behaviour. Read together, they map a single phenomenon, the manipulation of public discourse, from four complementary angles, while collectively underscoring that the hardest analytical work lies not in spotting manipulation but in correctly attributing its source and concrete purpose.

Technocratic enforcers, strangled farmers, and the green tyranny: Strategic manipulation targeting EU climate policies in the context of the 2024 European elections

Executive Summary

This report presents a qualitative case study of manipulative communication targeting EU climate policies in the run-up to the 2024 European elections. Climate policy was selected because pre-research identified it as one of the most prominent themes of election-related disinformation, while Russian information interference in the campaign was a leading concern across EU member states. The study analyses a sample of 30 online articles and blog posts in English, German, and Russian, drawn from Russian state propaganda outlets and from right-wing to far-right media within the EU, with data collection concentrated on the week of the election (30 May – 9 June 2024). Findings are structured using the ABCDE framework (actors, behaviour, content, degree, effect) and tagged with the DISARM Red Framework to map specific manipulative techniques. A more extensive and theoretically grounded version of this analysis has been published in the peer-reviewed journal *Humanities and Social Sciences Communications* (https://doi.org/10.1057/s41599-026-06656-8).

The analysis reveals a blurred ecosystem in which Russian state media and EU-based far-right outlets deploy strikingly similar rhetoric against EU climate policies and routinely cross-cite one another, making a clean separation between foreign and domestic information manipulation difficult to sustain. Manipulative actors track the news cycle closely and attach their messaging to high-salience events such as the 2024 farmers' protests and the assassination attempt on Slovak Prime Minister Robert Fico, casting EU climate policy as elite oppression of "the common people." Content is frequently reused or copy-pasted across outlets and supported by decontextualised "kernels of truth"; in at least one observed instance, coordinated same-day publication across Russian-language sites points to back-end coordination. The dominant tactic is to saturate the information space so that mutually reinforcing manipulative messages gain plausibility through repeated exposure, an effect consistent with the illusory truth effect, and feed Eurosceptic echo chambers.

Applying the DISARM Framework alongside the ABCDE framework proved a productive combination for mapping techniques and structuring analysis. That said, working with the original DISARM Red Framework in the first coding round surfaced some tensions with the mutually-exclusive-and-collectively-exhaustive (MECE) principle in relation to certain techniques. An April 2026 re-tagging of the same case study using the new DISARM Observables Framework v2.0 suggests that its focus on observables encourages more conservative coding and helps reduce multiple tagging. At the same time, a few areas would benefit from further development: dedicated categories for framing and narrative perspective are not yet available, some techniques from the previous version (notably "Reuse Existing Content" and "Distort Facts") do not have a direct counterpart, and the framework would gain from a more intuitive vertical structure to support systematic browsing. Stronger semantic search functionality and a clearer organising logic, potentially modelled on Lasswell's classical communication scheme, could further enhance the framework's usability.

Introduction and approach

This short report presents results from a qualitative case study on manipulative communication targeting EU climate policies in the context of the 2024 European Elections. The topic of climate change mitigation was chosen as pre-research revealed that climate policies were among the most relevant targets of disinformation

ahead of the EU elections, according to EDMO reports[i]. At the same time, Russian interference into the elections by means of information manipulation targeting a wide range of topics was one of the main concerns in the run-up to the polls[ii,iii].

Manipulative communication practices are analysed in this case study applying techniques from the latest version of the DISARM Red Framework[iv]. The ABCDE-Framework[v] is applied to structure the results. The analysis includes manipulative communication carried out by both FIMI[vi] actors and domestic sources of manipulative content within EU member states. The analysis focuses not only on disinformation, that is, the deliberate spread of falsehoods, but applies the broader concept of information operations[vii]. In information operations, communication is used as a tool to exploit the social and psychological vulnerabilities of societies, like prevalent prejudices, social inequalities, and polarisation via the fabrication of disinformation, the spin-doctoring of half-truths, and pushing propaganda. Against this background, the report at hand applies the terms manipulative communication and manipulative content to refer to the communicative behaviours and outputs linked to information operations. Accordingly, the term manipulative actor is applied in contrast to the Cyber intelligence term threat actor to highlight the focus on communicative behaviours and outputs, as opposed to the broader field of threat actor behaviours covered in the DISARM Red Framework.

A brief pre-search was conducted to assess common disinformation and propaganda themes in the context of EU climate policies reported by EDMO[viii] and investigative media in order to obtain relevant themes and keywords. Data collection focussed on the time period immediately ahead of the elections, particularly on the last week including the election weekend (May 30 to June 9), following other research conducted on disinformation and fake news in election contexts[ix,x]. However, as there is no consensus on the exact time period to cover, and since the analysis at hand follows an explorative approach, some meaningful material outside of this one-week-period is also included. The partly automated data collection process was conducted with the support of two partners from the ADAC.iO consortium, Debunk.org and Alliance4Europe. Starting with a search for disinformation and propaganda themes on the two essential Russian propaganda channels sputnikglobe.com[xi] and rt.com[xii] as initial data sources, the range of sources was then increased by scraping and examining media sites and blogs for meaningful paragraphs using the Debunk-app and the Meltwater-app[xiii]. The final data sample consists of 30 online articles and blog posts by both Russian propaganda outlets and right-wing media outlets with no direct affiliation to Russia in English, German, and Russian language. These three languages were chosen to compare messages targeting different population groups while limiting the amount of data to a manageable degree. Also, Germany was expected to be one of the priority targets of Russian manipulation[xiv].

The weblinks added to the problematic online contents mentioned in the results section link to the Internet Archive, where they were stored in order to be able to retrieve them in case the original content would be deleted.

Results

The results shed light on a diverse disinformation and propaganda ecosystem blurring the lines between FIMI and domestic information manipulation. Highlighted tags refer to techniques listed in the DISARM Red Framework. The alphanumeric codes make the tags machine-readable. Text in Russian language was translated using a browser translation plugin. This is indicated in the following paragraphs with the note orig. Russian.

A (actors)

Russian propaganda outlets and right-wing to far-right media outlets within the European Union.

B (behaviour)

By producing and reproducing manipulative content on the topic of climate change mitigation, manipulative actors are targeting a highly polarising issue (Identify Wedge Issues [T0081.006]). Zooming in, it can be seen from the data that manipulative actors identify trending topics (Identify Trending Topics/Hashtags [T0080.003]) and tailor their content to benefit from these trends in the media attention cycle (Respond to Breaking News Event or Active Crises [T0068]). In this context, libel and slander are pushed, probably to feed into Eurosceptic echo chambers (Use Existing Echo Chambers/Filter Bubbles [T0102.001]). For example, Russian propaganda outlets as well as right-wing media outlets spin-doctor on the farmers' protests that took place in Germany, Poland, France, and Spain right before the election period to condemn EU climate policies as harmful: According to these depictions, farmers are "strangled by Brussels" (magyarnemzet.hu[xv]) by means of the EU's climate policies, which are "devastating to their livelihoods" (rt.com[xvi]). Now, farmers are "angry" (rossaprimavera.ru[xvii], orig. Russian) and becoming part of "a backlash against the climate agenda and its technocratic enforcers" (rt.com[xviii]).

Furthermore, manipulative actors exploit social vulnerabilities by fuelling existing suspicions against the European Union (Identify Existing Conspiracy Narratives/Suspicions [T0081.005]). To do so, they are drawing on a common leitmotif in populist rhetoric: EU policy makers are depicted as elites "trying to turn the truth on its head" (europeanconservative.com[xix]), deceiving and oppressing the common, hardworking people, like farmers, workers, and coal miners, who constitute "the foundation of pyramid who hold society together" [sic] (globalresearch.ca[xx]), and who are now "fighting the EU's green tyranny" (spiked-online.com[xxi]).

spiked-online.com[xxii]

rt.com[xxiii]

rossaprimavera.ru[xxiv] (orig. Russian) inosmi.ru[xxv] (orig. Russian)

Fig. 1 - Screenshots of headlines and pictures from analysed propaganda sites depicting the farmers protests in EU countries as a broad and unified act of civil defence against the EU's dangerous climate policies.

As information operations do not only rely on blatant lies, i. e. disinformation, but on a broader set of techniques, manipulative actors also add kernels of truth to their communication (Seed Kernel of Truth [T0042]): messages targeting the EU climate policies are accompanied by decontextualised and vague statements of fact with no source or evidence provided, such as that "according to the German Chamber of Commerce and Industry, the management of more than half of the enterprises in Germany has a negative attitude to the energy transition" (gazeta.ru[xxvi], orig. Russian). Although there certainly is some dissent on climate policies, mainly on how to implement the energy transition, this depiction lacks any nuances and detail. Additionally, this statement is not backed by any source, and no additional context is given.

C (content)

A technique recurringly applied by Russian propaganda outlets is to amplify existing disinformation and propaganda stories (Amplify Existing Narrative [T0118]). This is done by quoting nationalist and right-wing politicians and media sources from within the EU who are criticising climate policies or questioning the legitimacy of EU policies altogether. Also, political statements are appropriated to condemn the Green Deal (Appropriate Content [T0084.004]). For example, the assassination attempt on Robert Fico, prime minister of Slovakia, that took place right before the elections on May 15, 2024, was instrumentalised by rt.com[xxvii] to present a selection of (alleged) quotes by Fico on topics such as the Russian invasion in Ukraine, national sovereignty, and EU policies - all with anti-Western and pro-Russian sentiment. According to one alleged quote reproduced on rt.com[xxviii], "the fanatic implementation of the Green Deal is killing our economies", that is, the economies of the member states.

Another example are statements spread on inosmi.ru[xxix] (orig. Russian) from an interview with Rafał Foryś, a politician running for the 2024 European elections representing the far-right political alliance Konfederacja Wolność i Niepodległość in Poland, who is cited as an "expert" stating that "the European Commission is laying a clock bomb under the EU" with its Green Deal.

Besides amplifying existing narratives, manipulative actors also reuse existing content (Reuse Existing Content [T0084]). A good example is an article from the right-leaning Italian tabloid Il Giornale[xxx], stating that as a consequence of the alleged "deindustrialisation" of Europe caused by the EU's Green Deal, "a third of industrial companies that are fleeing Europe have already left Germany", which is echoed in Russian newspapers like

news-front.su[xxxi] (orig. Russian) and stoletie.ru[xxxii] (orig. Russian). This is a strong example of the distortion of facts (Distort Facts [T0023]) for purposes of sensationalism and in order to create a sentiment of decay. In case of the abovementioned outlets, the websites simply copy and paste the content in question (Use Copypasta [T0084.001]). Coordinated publications on the same date of May 30, 2024, also hint at back-end coordination going on - a strong sign indicating problematic behaviour[xxxiii].

With regards to the **D** (**degree**) and **E** (**effect**) as the remaining categories of the ABCDE-Framework, this case study does not analyse the diffusion or impact of manipulative content directly. Hence, possible effects on individuals and society at large have to be inferred from the available data:

D (degree)

On the whole, the manipulative behaviour analysed in this case study shows signs of flooding the online information environment with as much malicious content as possible (Flood Information Space [T0049]), as also identified in the Russian Operation Overload campaign[xxxiv]. In this way, the content is supposed to become omnipresent. This tactic is based on the assumption that at least some disinformation or conspiracy myths will stick. This technique pursued by the re-use of existing content from other websites (as described above) and the sharing of web-articles on social media. For example, a spiked-online.com post on X[xxxv] shared the aforementioned article on protests of polish workers as a movement against "EU's green tyranny". This tweet was reposted several dozen times before the election and gained several thousand views.

E (effect)

From a psychological perspective, such a repeated exposure to certain messages potentially increases their perceived truthfulness, according to the illusory truth effect[xxxvi]. Against this background, creating an ecosphere of mutually coherent manipulative content presents itself as a highly promising approach from the perspective of manipulative actors.

Summary and concluding remarks

In sum, this short report shows that both Russian state propaganda media and far-right channels use similar rhetoric in their attacks against EU climate policies, sometimes cross-citing each other (**A**). In this regard, manipulative actors are attentive to trending topics (Identify Trending Topics/Hashtags [T0080.003]) and jump on breaking news (Respond to Breaking News Event or Active Crises [T0068]), in order to fuel prevalent conspiracy myths (Identify Existing Conspiracy Narratives/Suspicions [T0081.005]), poison public debate, and exploit the social vulnerabilities of the digital communication sphere, like polarisation (Identify Existing Fissures [T0081.004]) (**B**). Content is oftentimes re-used (Reuse Existing Content [T0084]), unsubstantiated by sources, and vague (**C**). It seems reasonable to assume that one major aim is to flood the public sphere with as much manipulative content as possible (Flood Information Space [T0049]) to saw division and foster Euroscepticism (**D**). Against this background, establishing an internally coherent parallel universe of misleading information might increase the perceived truthfulness of such harmful messages, feeding into Eurosceptic echo chambers (Use Existing Echo Chambers/Filter Bubbles [T0102.001]) (**E**).

From the analyst's point of view, applying the DISARM Red Framework proves a versatile tool for mapping threat actor techniques and the ABCDE-Framework proves as powerful for structuring analysis and report. However there arose some issues with respect to the M and the E as part of the MECE principle[xxxvii]. That is, it was not always clear which DISARM-techniques fall into which ABCDE-category. For example, reproducing existing manipulative communication (Amplify Existing Narrative [T0118] is to be considered an illegitimate communication technique and should, accordingly, fall into the **B** category. At the same time, however, aligning

messages to known disinformation is described under the **C** category[xxxviii]. Moreover, using existing content (Reuse Existing Content [T0084]) can be considered a technique of content (re-)production and should, accordingly, fall into the **C** category. However, it is also a means of disseminating malicious content, which is described under the **D** category. Mapping the DISARM-categories more systematically onto the ABCDE-categories would suite the objective of interoperability in the ADAC.io project.

April 2026 Update

The case study presented above was tagged with the DISARM Framework at an early stage of the project. Since autumn 2024, the framework has undergone substantial revision – most notably with the release of the prototype of the DISARM Observables Framework v2.0, which separates directly observable techniques from the tactics and goals inferred from them[xxxix]. This update re-tags the case study using v2.0 and reflects on the resulting usability improvements relative to the standard DISARM Navigator used in the original analysis.

Re-tagging of the report using the DISARM Observables Framework v2.0

A - Russian propaganda outlets and right-wing to far-right media outlets within the European Union.

B - By producing and reproducing manipulative content on the topic of climate change mitigation, manipulative actors are targeting a highly polarising issue (Identify Wedge Issues [T0081.006]). Zooming in, it can be seen from the data that manipulative actors identify trending topics (Identify Trending Topics/Hashtags [T0080.003]) and tailor their content to benefit from these trends in the media attention cycle (Respond to Breaking News Event or Active Crises [T0068]) (Produce Content [T0169.000]) (Respond to Breaking News Event or Active Crises [T0068.000]). In this context, libel and slander are pushed, probably to feed into Eurosceptic echo chambers (Use Existing Echo Chambers/Filter Bubbles [T0102.001]). For example, Russian propaganda outlets as well as right-wing media outlets spin-doctor on the farmers' protests that took place in Germany, Poland, France, and Spain right before the election period to condemn EU climate policies as harmful: According to these depictions, farmers are "strangled by Brussels" (magyarnemzet.hu) by means of the EU's climate policies, which are "devastating to their livelihoods" (rt.com). Now, farmers are "angry" (rossaprimavera.ru, orig. Russian) and becoming part of "a backlash against the climate agenda and its technocratic enforcers" (rt.com) (Respond to Breaking News Event or Active Crises [T0068.000]).

Furthermore, manipulative actors exploit social vulnerabilities by fuelling existing suspicions against the European Union (Identify Existing Conspiracy Narratives/Suspicions [T0081.005]). To do so, they are drawing on a common leitmotif in populist rhetoric: EU policy makers are depicted as elites "trying to turn the truth on its head" (europeanconservative.com), deceiving and oppressing the common, hardworking people, like farmers, workers, and coal miners, who constitute "the foundation of pyramid who hold society together" [sic] (globalresearch.ca), and who are now "fighting the EU's green tyranny" (spiked-online.com) (Content Presentation [T0178]) (Discriminatory Content [T0180.009]).

As information operations do not only rely on blatant lies, i. e. disinformation, but on a broader set of techniques, manipulative actors also add kernels of truth to their communication (Seed Kernel of Truth [T0042]): messages targeting the EU climate policies are accompanied by decontextualised and vague statements of fact with no source or evidence provided, such as that "according to the German Chamber of Commerce and Industry, the management of more than half of the enterprises in Germany has a negative attitude to the energy transition" (gazeta.ru, orig. Russian) (Context Removed from Content [T0168.007]). Although there certainly is some dissent on climate policies, mainly on how to implement the energy transition, this depiction lacks any nuances and detail. Additionally, this statement is not backed by any source, and no additional context is given (Context Removed from Content [T0168.007]).

C - A technique recurringly applied by Russian propaganda outlets is to amplify existing disinformation and propaganda stories (Amplify Existing Narrative [T0118]) (Amplify Content [T0157.000]). This is done by quoting nationalist and right-wing politicians and media sources from within the EU who are criticising climate policies or questioning the legitimacy of EU policies altogether. Also, political statements are appropriated to condemn the Green Deal (Appropriate Content [T0084.004]) (Quote Post [T0157]). For example, the assassination attempt on Robert Fico, prime minister of Slovakia, that took place right before the elections on May 15, 2024, was instrumentalised by rt.com to present a selection of (alleged) quotes by Fico on topics such as the Russian invasion in Ukraine, national sovereignty, and EU policies – all with anti-Western and pro-Russian sentiment. According to one alleged quote reproduced on rt.com, "the fanatic implementation of the Green Deal is killing our economies", that is, the economies of the member states (Content Presented as Produced by Third Party [T0178.002]).

Another example are statements spread on inosmi.ru (orig. Russian) from an interview with Rafał Foryś, a politician running for the 2024 European elections representing the far-right political alliance Konfederacja Wolność i Niepodległość in Poland, who is cited as an "expert" stating that "the European Commission is laying a clock bomb under the EU" with its Green Deal (Amplify Content [T0157.000]).

Besides amplifying existing narratives, manipulative actors also reuse existing content (Reuse Existing Content [T0084]). A good example is an article from the right-leaning Italian tabloid Il Giornale, stating that as a consequence of the alleged "deindustrialisation" of Europe caused by the EU's Green Deal, "a third of industrial companies that are fleeing Europe have already left Germany", which is echoed in Russian newspapers like news-front.su (orig. Russian) and stoletie.ru (orig. Russian) (Amplify Content [T0157.000]) (Cross-Posting [T0119.000]). This is a strong example of the distortion of facts (Distort Facts [T0023]) for purposes of sensationalism and in order to create a sentiment of decay. In case of the abovementioned outlets, the websites simply copy and paste the content in question (Use Copypasta [T0084.001]). Coordinated publications on the same date of May 30, 2024, also hint at back-end coordination going on - a strong sign indicating problematic behaviour.

D - On the whole, the manipulative behaviour analysed in this case study shows signs of flooding the online information environment with as much malicious content as possible (Flood Information Space [T0049]) (Amplify Content [T0157.000]). In this way, the content is supposed to become omnipresent. This tactic is based on the assumption that at least some disinformation or conspiracy myths will stick. This technique pursued by the re-use of existing content from other websites (as described above) and the sharing of web-articles on social media. For example, a spiked-online.com post on X shared the aforementioned article on protests of polish workers as a movement against "EU's green tyranny". This tweet was reposted several dozen times before the election and gained several thousand views (Concurrent Networked Action [T0159.001]).

E - From a psychological perspective, such a repeated exposure to certain messages potentially increases their perceived truthfulness, according to the illusory truth effect. Against this background, creating an ecosphere of mutually coherent manipulative content presents itself as a highly promising approach from the perspective of manipulative actors.

Reflection on usability improvements

By foregrounding observables, the revised framework discourages researchers from jumping to conclusions and encourages a more conservative assessment of the phenomenon under investigation. The narrower set of techniques and the emphasis on what is directly observable should also reduce multiple tagging, since fewer techniques are likely to apply to any given passage and the room for interpretation is correspondingly limited.

At the level of individual techniques, however, the Observables Framework currently lacks a category, or subcategories, addressing framing and narrative perspective. Although such dimensions inevitably involve interpretation, a subcategory under "Content Presentation" (T0178) flagging strongly negative emotional language would fit naturally alongside the other forms of distorted presentation already grouped there and would capture a core indicator of manipulative narratives. In this regard, it would be worthwhile to explore potential synergies with the EU-funded PROMPT project (Predictive Research on Misinformation and Narratives Propagation Trajectories)[xl], whose codebook combines linguistic elements, rhetorical devices, and information manipulation techniques to identify and deconstruct disinformation narratives, and which therefore offers a well-developed conceptual basis for integrating a narrative perspective into the DISARM Framework. Initial contact between both projects has already been established, and a more systematic exchange constitutes a further step worth pursuing.

Two further omissions are worth noting. “Reuse Existing Content” (T0084), present in the original DISARM Red Framework, has no real counterpart in v2.0: the closest equivalent, “Repost Post” (T0157.001), is narrower in scope, even though direct reproduction of specific statements is itself a verifiable observable. Similarly, “Distort Facts” (T0023) – the misleading alteration of information through exaggeration, omission, or selective framing – has no clear successor. The v2.0 subcategories under “Edited Content” (T0168), such as “Cropped Content” (T0168.002) or “Element Edited In to Content” (T0168.004), describe related behaviours but are more technical and less attentive to the message itself.

The practical tagging process raises a second set of concerns. The search function remains relatively static; a fuzzy, semantic search, potentially AI-supported, would substantially improve usability for analysts who do not already know the precise technique they are looking for. This matters especially for occasional users, who must otherwise navigate the framework's structure directly, and that structure is not yet intuitive. The original kill-chain logic of four phases (plan, prepare, execute, assess) was rightly abandoned, having been criticized for forcing “a sequential kill chain structure to the information environment” (Smith et al., 2025, p. 6) that analysts could rarely populate beyond the prepare and execute stages (ibid.). Its replacement, however, does not yet offer a clear vertical organising principle – for example, a division into infrastructures, content, dissemination techniques, and platform responses – that would make systematic browsing possible without recourse to the search bar.

One alternative worth exploring is Harold Lasswell's classical communication model, which reduces the communication process to five questions: “Who?”, “Says What?”, “In Which Channel?”, “To Whom?”, “With What Effect?” The model's linear conception of communication is of course open to criticism, but it identifies the central analytical dimensions in a clear and intuitive sequence, and it has already been applied successfully to structure descriptions of Russian state communication activities in the context of the war in Ukraine[xli].

References

[1] European Digital Media Observatory. (2024). EU-related Disinformation Peaks in April. Monthly brief no. 35 – EDMO fact-checking network. In *edmo.eu*. Retrieved March 10, 2026, from https://edmo.eu/wp-content/uploads/2024/05/EDMO-35-Horizontal.pdf#page=2

[1] Trellevik, A., & Cieśla, W. (2024, March 21). Russian interference unnerves Europe as elections near. *EUobserver*. https://euobserver.com/31861/russian-interference-unnerves-europe-as-elections-near/

[1] Garner, I. (2024, March 29). *The West is still oblivious to Russia’s information war*. Foreign Policy. https://foreignpolicy.com/2024/03/09/russia-putin-disinformation-propaganda-hybrid-war/

[1] The DISARM Red Framework is an open framework offering a systematisation of threat actor behaviours to be applied for the purpose of disinformation and FIMI analysis. The Framework is maintained and advanced by the DISARM Foundation.

[1] Pamment, J. (2020) The ABCDE Framework from The EU's Role in Fighting Disinformation: Crafting A Disinformation Framework on JSTOR. https://www.jstor.org/stable/resrep26180.6

[1] Foreign Information Manipulation and Interference, as defined in the first EEAS FIMI report

[1] Krieg, A. (2023). Subversion: The Strategic Weaponization of Narratives. Georgetown University Press.

[1] The European Digital Media Observatory is the EU's largest network of fact checkers dedicated to debunking and correcting disinformation https://edmo.eu/

[1] Baptista, J. P., & Gradim, A. (2020). Online disinformation on Facebook: the spread of fake news during the Portuguese 2019 election. Journal of Contemporary European Studies, 30(2), 297–312. https://doi.org/10.1080/14782804.2020.1843415

[1] Recuero, R., Soares, F. B., & Gruzd, A. (2020). Hyperpartisanship, disinformation and political conversations on Twitter: The Brazilian presidential election of 2018. International AAAI Conference on Weblogs and Social Media, 14, 569–578. https://doi.org/10.1609/icwsm.v14i1.7324

[1] Sputnik – a news agency and radio broadcast service owned by the Russian state

[1] RT – an international news television network funded and controlled by the Russian government

[1] The Meltwater app is a web app for the professional monitoring of media coverage and sentiment on specific topics

[1] Trellevik, A., & Cieśla, W. (2024, March 21). Russian interference unnerves Europe as elections near. *EUobserver*. https://euobserver.com/31861/russian-interference-unnerves-europe-as-elections-near/

[1] Magyar Nemzet – a major Hungarian newspaper published in Hungary, very close to the party of Viktor Orbán (https://web.archive.org/web/20240708115416/https%3A%2F%2Fmagyarnemzet.hu%2Fenglish%2F2024%2F06%2Fthe-choice-is-war-or-peace)

[1] https://web.archive.org/web/20240708124342/https%3A%2F%2Fwww.rt.com%2Fbusiness%2F596093-eu-green-agenda-legitimacy%2F

[1] Rossaprimavera.ru – a Russian news agency (https://web.archive.org/web/20240708132727/https%3A%2F%2Frossaprimavera.ru%2Fnews%2Ff68ade5c)

[1] https://web.archive.org/web/20240708124342/https%3A%2F%2Fwww.rt.com%2Fbusiness%2F596093-eu-green-agenda-legitimacy%2F

[1] The European Conservative – a pan-European conservative, traditionalist, reactionary, and right-wing English-language publication registered in Budapest, Hungary (https://web.archive.org/web/20240708120011/https%3A%2F%2Feuropeanconservative.com%2Farticles%2Fcommentary%2Fdont-blame-the-russians-when-europe-votes-right%2F)

[1] Globalresearch.ca – an anti-Western and anti-globalisation website regularly publishing conspiracy myths. Privately edited by Michel Chossudovsky (https://web.archive.org/web/20240708133930/https%3A%2F%2Fwww.globalresearch.ca%2Fpsychological-battle-truth-power-farmers-uprising%2F5853661)

[1] Spiked Online – a British, right-libertarian Internet magazine focusing on politics, culture and society (https://web.archive.org/web/20240708114338/https%3A%2F%2Fwww.spiked-online.com%2F2024%2F05%2F31%2Fpolish-workers-are-fighting-the-eus-green-tyranny%2F)

[1] https://web.archive.org/web/20240708114338/https%3A%2F%2Fwww.spiked-

online.com%2F2024%2F05%2F31%2Fpolish-workers-are-fighting-the-eus-green-tyranny%2F

[1] https://web.archive.org/web/20240708124342/https%3A%2F%2Fwww.rt.com%2Fbusiness%2F596093-eu-green-agenda-legitimacy%2F

[1] https://web.archive.org/web/20240708132727/https%3A%2F%2Frossaprimavera.ru%2Fnews%2Ff68ade5c

[1] https://web.archive.org/web/20240708133139/https%3A%2F%2Finosmi.ru%2F20240603%2Fevroparlament-269065204.html#pv=g%3D269065204%2Fp%3D268488771

[1] Gazeta.ru – a Russian news site based in Moscow (https://web.archive.org/web/20240708131606/https%3A%2F%2Fwww.gazeta.ru%2Fbusiness%2Fnews%2F2024%2F06%2F08%2F23202793.shtml)

[1] https://web.archive.org/web/20240708123842/https%3A%2F%2Fwww.rt.com%2Fnews%2F597672-fico-slovak-pm-quotes%2F

[1] https://web.archive.org/web/20240708123842/https%3A%2F%2Fwww.rt.com%2Fnews%2F597672-fico-slovak-pm-quotes%2F

[1] inoSMI – a Russian media project i. a. translating Western news into Russian. Part of RT (https://web.archive.org/web/20240708133139/https%3A%2F%2Finosmi.ru%2F20240603%2Fevroparlament-269065204.html#pv=g%3D269065204%2Fp%3D268488771)

[1] Il Giornale – an Italian conservative populist newspaper owned by Paolo Berlusconi, brother to the former Prime Minister Silvio Berlusconi

[1] NewsFront – a Russian news site based in occupied Crimea. It uses the top-level domain for the Soviet Union (.su) which remained in use after the collapse of the Soviet Union under control of the Russian state to the present day. Author's comment: The fact that a Russian online news site based in Crimea uses this top-level domain cannot but being interpreted as an imperialist gesture. (https://web.archive.org/web/20240708113316/https%3A%2F%2Fnews-front.su%2F2024%2F05%2F30%2Fstaryj-kontinent-povtorjaja-oshibki-rimskoj-imperii-mozhet-povtorit-i-ee-sudbu%2F)

[1] Stoletie – a Russian newspaper (https://web.archive.org/web/20240708113316/https%3A%2F%2Fnews-front.su%2F2024%2F05%2F30%2Fstaryj-kontinent-povtorjaja-oshibki-rimskoj-imperii-mozhet-povtorit-i-ee-sudbu%2F)

[1] Pamment, J. (2020) The ABCDE Framework from The EU's Role in Fighting Disinformation: Crafting A Disinformation Framework on JSTOR. https://www.jstor.org/stable/resrep26180.6

[1] Atanasova, A., Lesplingart, A., Poldi, F., & Kuster, G. (2024). Operation Overload. In *Reset.Tech & CheckFirst*. Retrieved March 10, 2026, from https://checkfirst.network/wp-content/uploads/2024/06/Operation_Overload_WEB.pdf

[1]

https://web.archive.org/web/20240708123420/https%3A%2F%2Fx.com%2Fspikedonline%2Fstatus%2F1796602619395223722

[1] Hassan, A., & Barber, S. J. (2021). The effects of repetition frequency on the illusory truth effect. Cognitive Research, 6(1). https://doi.org/10.1186/s41235-021-00301-5

[1] The MECE principle requires of systems of taxonomies to contain mutually exclusive and collectively exhaustive categories; Each category needs to be distinct from all other categories, and the sum of all categories should be sufficient to describe all elements of the phenomenon in question.

[1] Pamment, J. (2020) The ABCDE Framework from The EU's Role in Fighting Disinformation: Crafting A Disinformation Framework on JSTOR. https://www.jstor.org/stable/resrep26180.6

[1] Smith, V., Campbell, S., & Maunder, A. (2025). A Comprehensive Review of DISARM Framework and its

Compatibility with Related Frameworks used to Model Foreign Information Manipulation and Interference. In adacio.eu. Retrieved March 10, 2026, from https://adacio.eu/wp-content/uploads/2025/01/ADAC.io-Publication-–-A-Comprehensive-Review-of-DISARM-Framework-and-its-Compatibility-with-Relevant-Frameworks.pdf

[1] PROMPT – Predictive Research on Misinformation and Narratives Propagation Trajectories. European Narrative Observatory funded by the European Commission. Project website: https://disinfo-prompt.eu/ (accessed 13 May 2026).

[1] Kuzmenko, H. (2024). Russia's Strategic Commuication in the Full-scale Russo-Ukrainian War: Analysis Using Lasswell's Model of Communication. Обрії Друкарства, 2(16), 185–196. https://doi.org/10.20535/2522-1078.2024.2(16).319282

Expanding the FIMI Framework: The Challenge of Addressing Gendered Disinformation

Elsa Hedling & Hedvig Ördén

Executive Summary

Gendered disinformation is a form of identity-based disinformation that weaponizes gender, sexuality and intersectional identities as well as structural vulnerabilities related to gender inequality. This type of disinformation is a problem for democratic pluralism. It is also a growing democratic vulnerability that may be exploited by foreign actors seeking to drive a wedge between traditional values and progressive policies in European democracies. At the same time, gendered disinformation has emerged as a difficult issue to address. This is partly due to the increased politicization of gender rights issues across European Member states, making gender equality a contentious topic. Since gendered disinformation is often embedded in broader patterns of systemic misogyny or threat frames, distinguishing disinformation from foreign information manipulation and interference (FIMI) is also an analytical challenge. This calls for an adjustment of existing FIMI frameworks and attention to growing vulnerabilities.

This report aims to advance policy and practice on gendered FIMI. The report is divided into three parts. First, it outlines a **typology of gendered disinformation** and demonstrates how this typology can be operationalized within an attribution framework. Second, it shows the analytical value of the typology, the report then operationalizes it within an **attribution framework for gendered FIMI.** Third, it introduces a **vulnerability assessment** for gendered FIMI.

The **typology of gendered disinformation** serves the aim of promoting a shared terminology across the defender community. It is based on a set of distinguishable behavioral and contextual drivers and technical evidence. Behavioral drivers include the Tactics Techniques and Procedures (TTPs) employed for gendered disinformation. Distinguishable behavioral features include for instance the use of deepfakes, coordinated abuse and trolling and the exploitation of gender wedge issues. Contextual drivers are outlined in relation to key targets, key narratives and strategic effects. Distinct features which set gendered disinformation apart include the targeting of LGBTQ+ communities or individuals and women in politics and public life through narratives promoting delegitimation and sexualized harassment which serves to deter the targets from public participation. The typology of actors spreading gendered disinformation, based on technical evidence, includes state actors, non-state organized actors and algorithmic amplifiers on large

platforms. This wide range of actors demonstrates the diffuse actor landscape related to gendered disinformation which contributes to the persistent challenges in addressing the problem. Genderedisinformation becomes gendered FIMI when gendered narratives, harassment or manipulated content are deliberately and coordinately mobilized by foreign-linked actors to pursue strategic objectives.

The **attribution framework for gendered FIMI** aims to facilitate the identification of patterns, actors and mechanisms of influence. The framework serves to better disentangle domestic disinformation from FIMI and thus exclude vulnerabilities related to gender. Five types of gendered FIMI are outlined based on distinct combinations of behavioral and contextual features: *targeted gendered delegitimization*; *gendered narrative warfare*; *wedge amplification through gender issues*; *gendered harassment* and *synthetic and manipulated gendered content*. By mobilizing this framework together with available technical evidence, actors in the defender community can strengthen their attribution assessments of gendered FIMI.

The **vulnerability assessment** outlines the growing vulnerabilities to gendered FIMI across European democracies. Drawing on existing academic research and public reports, three core vulnerabilities are pinpointed: *financial enablers* include foreign and domestic funding streams and material support which sustain transnational networks promoting anti-gender agendas; *domestic political vulnerabilities,* which are linked to the rise of illiberal values and the mobilization of gendered disinformation by domestic political actors for strategic gain; *societal and structural vulnerabilities*, including societal opposition to gender equality as well as vulnerabilities related to the governance structures of digital platforms. These vulnerabilities interact and reinforce each other but are unevenly distributed across European democracies. To enhance situational awareness of potential gendered FIMI across the defender community, the report suggest the development of a *vulnerability index* drawing on the identified factors shaping resilience to the threat.

Introduction

Gendered disinformation refers to the intersection of disinformation, understood as intentional efforts to mislead or deceive an audience, and gendered forms of discrimination and abuse, often on social media platforms in the form of online gender-based violence (OGBV). It is a form of identity-based disinformation (European External Action Service, 2024b) that explicitly mobilizes gender identities, although often in combination with other identities (intersectional identities). The intersection is broad, and it encompasses both legitimate political positions and illegitimate forms of abuse ranging from expressions of conservative values and misogyny to fraudulent imagery, harassment and hate speech. It has become increasingly salient in the Foreign Information Manipulation and Interference (FIMI) context as it encompasses a broad range of expressions that can be weaponized to amplify both its reach and harm. This broad range of expressions makes it difficult to identify gendered disinformation as a single, coherent behavioral pattern within FIMI. Rather, it is better understood as an umbrella term that captures the vulnerabilities and threats arising from the mobilization of gendered stereotypes and structural inequalities in the information sphere.

As a threat to democratic societies, gendered disinformation is especially potent in its intersections with the advancements of anti-gender movements in Europe (Kuhar and Paternotte 2017; Righetti 2025). Its force lies in the ability to mobilize entrenched gender norms and conservative values within societies, which makes it both urgently pressing and structurally difficult to counter (Hedling 2024). Gendered disinformation does not necessarily rely on false information, rather it weaponizes certain attitudes and prejudices with malign intent to fuel polarization or mistrust. Whereas conservative opinions about gender roles, sexual and reproductive health and rights (SRHR) or sexual minority rights do represent authentic political positions in European democratic debates, we know that polarization around these issues have been exploited by FIMI actors that deliberately seek to drive a wedge between traditional values and progressive policies in in European democracies (European External Action Service, 2023). In similarity to other known tactics, techniques and procedures (TTPs), efforts to exploit polarization around these issues often fall in the grey zone of legitimate political influence and under the threshold of legal frameworks. In contexts of polarization around issues such as abortion rights, transgender rights or gender-based violence, the result is therefore often a successful amplification of dissent and incited anti-gender attitudes.

Among the reasons for the urgency of addressing this issue are the reported increase in FIMI cases targeting LGBTQ+ communities. A report by the European Digital (EDMO) published in May 2023 highlighted that mis- and disinformation targeting the LGBTQ+ community is one of the most persistent patterns of FIMI targeting European Union (EU) member states. This pattern has been confirmed in the annual reports on FIMI threats by the EEAS (European External Action Service, 2024a, 2025, 2026). Moreover, alongside the increasing flow of external funding of Europe's anti-gender movement, most notably from Russia as its largest state sponsor (Datta 2025),

gendered disinformation constitutes a significant threat to the EU's value-based cohesion among its member states. The anti-gender movement in Europe is not a new target of foreign interference, transnational lobby groups have mobilized to counter so-called "gender ideology" in Europe since the 1990s (Kuhar and Paternotte 2017). In recent years, the transnational anti-gender movement has mobilized to build coalitions spanning advocacy and lobbying against progressive policies in ways that mimics grassroot activism through disinformation tactics, effectively turning gender rights into a battleground of geopolitical contestation (Datta 2025, 143). The steady rise in foreign funding to the anti-gender movement in Europe, combined with escalating reports of attacks on LGBTQ+ communities in the EU captured through FIMI mapping, points to the growing severity of this threat.

The nature of this threat is its effective targeting of the contestation of gender norms and values in the European Union as a systemic democratic vulnerability (Hedling 2024). It is therefore essential to acknowledge that gendered disinformation gains traction and is amplified across social media platforms in Europe, as the moral narratives and stereotypes that it mobilizes resonate with some European publics. This resonance, combined with the role of gender rights as a polarizing issue in the EU's public and political sphere, makes it particularly difficult to address this threat. Efforts to map and attribute this form of FIMI risk politicization and may inadvertently provoke backlash against gender rights by framing opposition as foreign and externally driven (Mhajne 2025). Moreover, gender equality has increasingly become politicized across the political spectrum, where it is often contrasted with other policy priorities such as migration, particularly in framings of Islam as a threat to gender equality in Europe (Edenborg 2022) and militarization, where rearmament is correlated with gender inequality (Hoijtink and Muehlenhoff 2020). Consequently, attempts to examine, map, or attribute gendered disinformation are embedded in a politicized context of contestation, which frequently produces dynamics of avoidance.

In this report, we begin by mapping the landscape of gendered disinformation within the EU defender community through a scoping review of published reports and documented incidents since 2019. Drawing on a meta-analysis of these sources, we develop a typology of gendered disinformation that distinguishes its various forms in relation to key behavioral and contextual drivers, while also promoting a shared terminology across the defender community. In a second step, we demonstrate how this typology can be operationalized within an attribution framework, illustrating its analytical value for identifying patterns, actors and mechanisms of influence. We end this report by reflecting on the challenges encountered in our efforts to test the attribution framework in this area and how these challenges may also be instructive to understanding the exceptional status of gendered disinformation as a threat to European democracies. We therefore suggest ways forward in both policy and practice.

Scope and Methodology

This report adopts a broad understanding of gendered disinformation. The terms "gendered disinformation" and "gender-based disinformation" are used interchangeably by governments, organizations and activists to describe the intersection of disinformation and OGBV (Hedling 2024). In a widely cited report introducing the problem of gendered disinformation, Lucina Di Meco (2020) defined it as "the spread of deceptive or inaccurate information and images used against women political leaders, journalists, and female public figures, following storylines that draw on misogyny and stereotypical gender roles". Whereas US based organizations have tended to follow Di Meco's definition focusing on the targeting of women (Jankowicz et al. 2021), the EU's definition has expanded to gender non-conforming individuals and other marginalized groups, including LGBTQ+ communities. In the EEAS report from 2023 FIMI targeting the LGBTIQ+ community is defined as:

> A non-illegal pattern of behaviour that threatens and causes direct or indirect harm to members of the LGBTIQ+ community, affects values and disrupts the political process. It is often based on misleading narratives with a strong moral appeal involving gender, sexuality, family, reproduction or child protection. These narratives are fabricated, adapted, presented and disseminated in different contexts and territories with different political objectives. Such activities may or may not have the LGBTIQ+ community as their ultimate target (e.g., when authorities and institutions are associated with the LGBTIQ+ community with the aim of damaging their reputation), but they still rely on biases about the community to achieve other political goals while undermining the rights, well-being, dignity and safety of LGBTIQ+ people. Like other forms of FIMI, this type is manipulative in nature and is conducted in a deliberate and coordinated manner by state and non-state actors, including their proxies inside and outside their own territory. Intentionality can be demonstrated through the behavioural analysis of Tactics, Techniques and Procedures (TTPs) (European External Action Service, 2023, 10).

In a FIMI context, it is important to note the emphasis on foreign rather than domestic sources of gendered disinformation. We focus here not on gendered disinformation as global phenomenon that encompass both foreign and domestic sources of malign intent but on gendered disinformation as a vulnerability to and threat of foreign interference. While this distinction is important for the purposes of this report and the ADAC.IO project, we acknowledge the difficulty in empirically upholding this distinction at the level of content and narratives. Whereas the FIMI and attribution framework provides a method for attributing foreign threat actors, it is particularly difficult to trace these actors in the context of gendered disinformation owing to the combination of orchestrated disinformation campaigns and large sale funding schemes that effectively has established a network of domestic proxy actors in Europe (Datta 2025). To uphold the integrity of the FIMI framework, we have therefore limited our discussion to individual cases and campaigns involving

incidents of verified information manipulation, based on the analysis of TTPs in the defender community, in which actors outside the EU were involved, while acknowledging that this issue extends beyond these instances.

Our analysis in this report is based on a scoping review of available research on and reported incidents of gendered disinformation in a FIMI context. A scoping review is a form of evidence synthesis that aims to map the breadth and nature of research and documented evidence on a given topic, rather than to systematically assess the quality of individual studies. It is particularly suited to emerging or complex fields where concepts, definitions and evidence are still evolving, which is the case in FIMI reporting of gendered disinformation. This report is based on a secondary analysis of data provided by Debunk.org, a partner in the ADAC.io consortium. Debunk.org conducted an AI-assisted scoping review of available research and reported incidents concerning gendered disinformation in a foreign information manipulation and interference (FIMI) context. The review brought together material from academic literature, policy and civil society reporting and documented cases to map the emerging evidence base on this issue. The initial dataset included 72 sources published between 2024-2026.

To complement this dataset, we reviewed and assessed the categorization of the AI-assisted data collection, and we conducted additional more targeted data collection. This included identifying relevant recent publications, policy reports and documented incidents that were not captured in the original dataset, as well as reviewing all sources to ensure contextual completeness and topical relevance. This step was particularly important given the need to establish the boundaries of gendered disinformation in a FIMI context. For instance, we found that many of the reported instances of gendered disinformation would not be classified as FIMI in accordance with the current standard attribution frameworks.

The combined dataset was then analyzed to identify key themes, recurring narratives, target groups, tactics and impacts associated with gendered disinformation in FIMI contexts. The primary aim of this analytical process was to develop a typology of gendered disinformation, capturing the different forms, functions and strategic uses of gendered narratives within information manipulation campaigns and enabling its integration with existing attribution frameworks. Our analytical approach focused on synthesizing patterns across both the AI-compiled material and the supplementary sources, with particular attention to how gendered narratives are constructed, adapted and operationalized, as well as how they may support or obscure attribution efforts in FIMI analysis.

Applying the Attribution Framework to Gendered Disinformation

The attribution framework has been developed to facilitate the identification of information influence operations (IIOs)(Palmertz, Isaksson, and Pamment 2025). In comparison to similar

frameworks applied in the cyber security domain, it places a heavier emphasis on evidence assessed through communications analysis.

The framework includes three distinct dimensions: *technical evidence*, *behavioral evidence* and *contextual evidence*. Technical evidence refers to digital evidence that can be collected from either open sources, proprietary sources or classified (state intelligence) sources, such as web domain ownership, IP addresses and economic ties. Behavioral evidence focuses on the communication methods and strategies used by threat actors. This can be the use of trolling, inauthentic video material (deepfakes), use of hashtags and cross-posting between platforms. Contextual evidence, finally, focuses primarily on the content of campaigns. This includes an analysis of narratives and discourses which can give insight into intended target audiences, who benefits from a campaign ('*cui bono*'), intended goals and effects.

The below attribution framework for gendered disinformation is based on a meta-analysis of secondary sources and draws on published reports mapping gendered disinformation operations. The focus lies on behavioral and contextual evidence.

Step 1. Introducing gendered disinformation in the attribution framework

The tables below outline gendered disinformation, focusing on behavioral, contextual and technical evidence for attribution. In the table outlining behavioral aspects of gendered disinformation, we have also related the evidence to the DISARM Framework, widely used by the defender community. The DISARM Framework collates TTPs used in FIMI campaigns, with the goal of providing a common language and enabling better collaboration between FIMI defender organizations.

The main differences between gendered disinformation and other IIOs can be pinpointed on the level of *contextual evidence*. In relation to key targets, gendered disinformation targets individual women in public positions, LGBTQ+ individuals and movements as well as broader gender wedge issues across societies. In terms of strategic purpose and effect, gendered disinformation aims to silence and delegitimize voices and further polarize societies through the exploitation of gendered issues. While many of the communication strategies pinpointed in the *behavioral dimension* are shared with other forms of IIOs and cannot in themselves be said to constitute gendered disinformation, strategies such as the use of deepfakes is a modality which lends itself particularly well to the promotion of sexualized content.

While contextual evidence is key for pinpointing gendered disinformation, it also constitutes the most uncertain category in the attribution framework (Palmertz, Isaksson, and Pamment 2025, 15). Successful IIOs commonly target wedge issues and seek to exploit already existing grievances, making it difficult to distinguish between authentic content and content intended to influence audiences by considering narratives or potential effects alone. Moreover, gendered disinformation currently operates as a broad analytical category that extends beyond gendered FIMI,

encompassing forms of gendered harm that are not necessarily foreign, coordinated or manipulative in intent. Consequently, relying on contextual and behavioural evidence alone may conflate distinct phenomena, heightening the risk of attributing gendered disinformation to FIMI actors where such attribution is not warranted.

Table 1: Behavioral evidence

I. Behavioral			
Communication method	**Mechanism**	**Illustrative Example**	**Disarm v 1.7.**
Coordinated abuse/trolling	Coordinated abuse and trolling targeting women or sexual minorities in public roles	Mass harassment campaigns against female journalists	T0048.002: Harass People Based on Identities
Meme-based communication	Images and memes used for viral spread	Memes mocking feminist leaders	T0115.001: Share Memes, T0135.001: Smear
Fabricated videos/deepfakes	Use of deepfakes and deep porn to discredit women or sexual minorities	Deepfake videos targeting female politicians	T0166.001: Deepfake Impersonation, T0166.002: Sexual Deepfake Impersonation
False labelling of authentic content	Adding false labels to visual material portraying sexual minorities	Using authentic videos portraying LGBTQ+ individuals with false claims	T0162.008: Context Reframed by Edits to Media, T0160.002: Information is False
Doxxing	Publishing identifying information about female users	Doxxing female voices	T0048.004: Dox
Exploiting wedge issues	Targeting gender wedge topics	Bots to manipulate debate	T0081.006: Identify Wedge Issues, T0049.003: Bots Amplify via Automated Forwarding and Reposting
Pseudo-journalistic / Fake news sites	Websites mimicking legitimate news outlets	Fake articles about women's rights	T0085.003: Develop Inauthentic News Articles

Social media architectures	Using mainstream platforms, and available features, to enable rapid spread	Twitter, Facebook, TikTok campaigns	T0151.001: Social Media Platform, T0151.008: Microblogging Platform

Table 2: Contextual evidence

II. Contextual		
Key targets	**Key narratives**	**Strategic purpose/effect**
Women in politics and public life	Sexualized harassment and abuse targeting credibility and morality	Silencing, intimidation, and deterrence from public participation
LGBTQ+ individuals, members and allies of the LGBTQ+ movement.	Framing gender equality advocacy as illegitimate, deviant or ideologically driven	Polarization, norm contestation, and social division
Organized gender equality initiatives and protests	Discrediting actors promoting gender equality as biased, extremist or externally influenced	Reputational damage and erosion of trust
Intersectional identities	Amplifying stereotypes of emotional instability, irrationality or lack of fitness for leadership	Marginalization and reduced political legitimacy
Political authorities, institutions and multilateral organizations (for instance EU/WEF)	Gendering opponents by ascribing femininity or homosexuality as markers of weakness	Dehumanization, masculinized norm enforcement and delegitimization
Progressive policies	Describing gender equality and "gender ideology" as a societal threat/ threat to national identity	Politicization and delegitimization of policy agendas
Transgender rights	Circulating false or misleading claims about transgender rights (e.g. threat narratives)	Dehumanization, fear mobilization, and policy backlash
Diversity, equity and inclusion (DEI)	Depicting DEI and gender mainstreaming as coercive, discriminatory or anti-meritocratic	Undermining institutional legitimacy and increasing politicization

The two tables above show the limits of integrating gendered disinformation into the existing DISARM Framework. The DISARM Framework primarily focuses on behaviors and actors, and the central position of key targets and narratives in relation to gendered disinformation creates problems with successful alignment.

A final category of the attribution framework is *technical evidence* linked to actors. As noted in academic research, a key challenge of attributing gendered FIMI is amplified by the complex interaction between external threat actors and internal vulnerabilities, producing what has been described as a 'diffuse actor landscape' (Saner 2026, 605). Assessments of actors disseminating gendered disinformation in secondary sources – presented in Table 3 below – confirm this pattern.

Table 3: Key actors spreading gendered disinformation

III. *Key actors*	State-sponsored actors	Government-linked entities disseminating gendered narratives	State media promoting anti-feminist discourse
	Non-state organized actors	Coordinated groups such as troll farms or ideological/religious networks	Troll networks targeting women and LGBTQ+ activists
	Platform/Algorithmic amplifiers	Digital platforms that amplify harmful content through algorithms	Recommendation systems promoting misogynistic content

While state-sponsored actors are responsible for disseminating gendered FIMI, a large portion of gender-based disinformation is spread by non-state actors such as religious and ideological networks located within EU member states. For instance, whereas many country reports released by EU vs Disinfo feature gendered disinformation, the sources of these campaigns are often domestic conservative and far-right political parties or organizations (Kotowska 2024). Harassment campaigns using misogynic language or targeting women in public positions may also emerge organically in a domestic context characterized by gendered political wedge issues. Such campaigns may be further amplified through the technological architectures of social media (Regehr et al. 2024). In these cases, misogynistic narratives and other forms of gendered disinformation can be best understood as a vulnerability factor (in terms of opportunities for FIMI weaponization), rather than an instance of FIMI.

To address these issues, the attribution framework points to the importance of integrating *technical evidence* as part of the analysis in addition to behavioral and contextual evidence (Palmertz, Isaksson, and Pamment 2025). However, technical evidence is also where the framework's limitations become most visible when applied to gendered FIMI. Limitations are partly tied to an unevenly distributed capacity for technical attribution across the defender community. For instance, the use of technical evidence originating from proprietary and even classified sources features only in rare cases. A report by the European External Action Service (2023) for example indicates the use of technical evidence for attribution which allows them to demonstrate close links between channels disseminating LGBTQ+ gendered FIMI and foreign state intelligence agencies. However, most civil society actors in the defender community must rely exclusively on publicly accessible data (domain ownership, IP addresses) for attribution. Information from publicly accessible data can greatly facilitate the attribution of gendered FIMI in cases where gendered disinformation is spread directly by government representatives and state-controlled media channels. It may however present challenges when foreign state actors employ covert means for influence and interference, when the actor landscape is complex, and when platform-driven amplification plays a key role.

The boundary problem also becomes problematic in relation to technical evidence of gendered FIMI in the form of *financial linkages*. In an environment where gendered disinformation is deeply embedded in broader patterns of systemic misogyny, financial linkages may point more clearly to shared ideologies, enabling structures and systemic vulnerabilities than to operational intent related to gendered FIMI.

An illustrative case is a recent report by Neil Datta, Executive Director and founder of the *European Parliamentary Forum for Sexual and Reproductive Rights* (EPF) which pinpoints Russia as the largest funder of anti-gender movements in Europe alongside other state and non-state financiers. While financial flows have decreased significantly due to EU sanctions, the country contributed the equivalent of US$ 211,9 million in funding between 2019 and 2023 (Datta 2025). Previous EU recipients of financial support include a broad range of civil society advocacy and lobbying organizations targeting gender issues and LGBTQ+ rights (Datta 2025, 76). Many of these organizations have a strong online presence, and are active in spreading gendered disinformation (Datta 2025, 120).

From an attribution perspective, this type of financial evidence shows the limits of drawing clear boundaries between ideological alignment and attributed foreign interference. In line with attribution frameworks, financial evidence should be interpreted together with behavioural and contextual indicators (Palmertz, Isaksson, and Pamment 2025). Although financial links can be substantiated, they rarely provide sufficient evidence of operational intent into FIMI activities, messaging control or campaign orchestration on their own. Within a diffuse actor landscape characterised by widespread domestic anti-gender sentiment, financial links may function even less reliably as indicators of direct foreign interference. In many cases, this form of technical evidence may therefore better be treated as evidence of enabling structures, and as a means of informing vulnerability assessments, rather than as singular proof of gendered FIMI.

Taken together, these dynamics suggest that the attribution framework's contextual and behavioural dimensions require further refinement to better distinguish the narrower set of cases. Below, we propose a typology adjusted to capture gendered FIMI. Focusing on the attribution of gendered FIMI rather than gendered disinformation allows us to separate FIMI from other forms of misogynic communication, potentially organic in nature.

Step 2. A typology of gendered FIMI: when gendered disinformation becomes FIMI?

Having established that gendered FIMI activates both contextual and behavioral dimensions of the attribution framework yet still presents challenges in terms of disentangling domestic disinformation from FIMI we propose a typology that clarifies five distinct patterns of gendered FIMI. Whereas table 1 and 2 outline the differences and overlaps between contextual and behavioral dimensions in the ways in which gender is mobilized in FIMI tactics and table 3 highlights actors, the typology illustrated in table 4 below clarifies distinct patterns of what we

label as gendered FIMI. This means that whereas step one captures vulnerabilities and cases of gendered disinformation that could be or evolve into FIMI ('potential for harm' see Freelon and Wells 2020), our typology identifies distinct strategic patterns of threat thereby avoiding overlap at the level of types despite recurrent behavioural mechanisms. While overlaps persist at the level of tactics, the typology differentiates between cases based on their strategic objectives.

The five types of gendered FIMI that we have identified are 1) *targeted gendered delegitimization*, 2) *gendered narrative warfare*, 3) *wedge amplification through gender issues*, 4) *gendered harassment* and 5) *synthetic and manipulated gendered content*. These types of gendered FIMI are often observed in combination with each other but reflect internal differences that are relevant to the attribution of orchestrated campaigns.

First**, targeted gendered delegitimization** refers to coordinated influence campaigns that seek to undermine the credibility, authority or legitimacy of specific individuals by mobilizing gendered narratives and stereotypes. These campaigns may target women, men or LGBTQ+ individuals, and often operate by exploiting or constructing perceived deviations from socially dominant gender norms. Common tactics include sexualized disinformation, feminization or emasculation of male targets, insinuations about sexuality or questioning of competence. Within FIMI contexts, such strategies are deployed to weaken trust in public figures and by extension, the institutions they represent. Whereas in extreme communities on platforms like Telegram and Rumble (Taylor, Hannah, and Hattotuwa 2022) these narratives are known to assert the moral and intellectual inferiority of women, more mainstream narratives often focus on women's alleged lower intelligence due to too much emotions and their rights and responsibility to be mothers rather than pursuing careers (Kotowska 2024).

In 2021, German party leader and former minister of foreign affairs, Annalena Baerbock was the target of coordinated disinformation campaigns that combined sexualized rumors, scrutiny of her appearance and family life and claims questioning her competence and credibility (Brady 2021). Such content was amplified through networks of inauthentic accounts and pseudo-journalistic outlets, including ecosystems linked to Russian foreign influence operations such as Storm-1516 (European Digital Media Observatory, 2025a). The campaign leveraged gender stereotypes portraying her as inexperienced, emotional or unfit for leadership to undermine her legitimacy and reduce public trust in both the individual and the institutions she represents. Since then, similar patterns of amplified gendered criticism against political candidates have been detected in FIMI reports (FIMI-ISAC 2024). For example, President of the European Commission Ursula von der Leyen has been subjected to attacks marked by misogynistic undertones. These narratives frequently suggest that she attained her position through personal connections or opaque backroom arrangements rather than merit, while simultaneously casting doubt on the competence of women in political leadership more broadly (Global Disinformation Index 2024). Moreover, the persistent pro-Kremlin portrayal of von der Leyen as "unelected" in combination with misogynist frames, despite her formal election in 2019 and reelection in 2024 by the European Parliament, serves to

delegitimize her authority and by extension, to undermine the democratic foundations of the European Union (EUvsDisinfo, 2024a).

Targeted gendered delegitimization also targets men, often through feminization, emasculation or insinuations of sexual deviance that frame them as deviating from dominant norms of masculinity. For instance, Emmanuel Macron has been the subject of recurring disinformation narratives questioning his masculinity and sexuality, portraying him as weak, controlled or morally suspect. Such narratives are frequently embedded within broader influence operations that depict Western political leaders as degenerate or unfit and are amplified through coordinated networks of inauthentic accounts and aligned media ecosystems (Vilmer 2019). In 2021, a new conspiracy theory began to spread about Brigitte Macron, Macron's wife and First Lady of France, claiming that she was transgender. This narrative has since been spread by both domestic (foremost in Hungary) and foreign actors (in Russia and the United States) in efforts to delegitimize the Macrons including fabricated proof and footage of the death of the alleged surgeon (European Digital Media Observatory, 2025b) and linked her to plans of a "transgender a coup d'etat" in France (EUvsDisinfo, 2025).

In February 2026, VIGINUM, the French government body responsible for detecting and countering foreign online interference, identified a coordinated disinformation campaign involving the creation of a website impersonating France-Soir, a controversial media outlet. The spoofed site published a fabricated article falsely alleging that Emmanuel Macron was implicated in the Epstein affair. According to VIGINUM, the content was subsequently amplified on X, indicating a coordinated effort to increase its reach and visibility. VIGINUM attributed the operation, with a high degree of confidence, to the "CopyCop" modus operandi, a technique based on impersonating legitimate media outlets to disseminate false information. This method has been linked to John Mark Dougan, a former U.S. law enforcement officer who has been living in Russia since 2016. According to the agency, Dougan is involved in registering and maintaining parts of the digital infrastructure associated with the Storm-1516 information operation (Le Monde, 2026). In similarity to cases targeting high-profile women, the objective is not only to discredit the individual, but also to undermine trust in political leadership and democratic institutions more broadly.

Gendered narrative warfare refers to the systematic promotion and circulation of ideologically charged narratives about gender, sexuality and family values as part of coordinated influence operations. Rather than targeting specific individuals or discrete policy issues, this type of operation functions at the societal level. It seeks to shape collective perceptions by framing gender equality, feminism and LGBTQ+ rights as threats to cultural, moral or national order (Mercereau 2024). The narrative of "gender ideology" is itself a derogatory construct developed and mobilized by opponents of gender equality and LGBT+ rights, both within and beyond EU debates (European External Action Service, 2023). Its deliberate dissemination to mislead the public therefore

constitutes a form of disinformation that often intersect with moral conservatism and religiosity.[1] In fact, by tapping into existing gender conservatism, threat actors such as Russia can effectively reach broad conservative audiences and amplify illiberal claims (Stolze 2026). Gendered disinformation thus often overlap with the anti-gender movement in ways that position moral conservatism as vulnerability (Righetti 2025). By portraying gender equality and LGBTQ+ rights as societal threats or as conspiracies driven actors can strategically strengthen their own moral and political agendas (NGO Report, 2023). For example, a dominant narrative explicitly portrays the promotion of LGBTIQ+ rights as a form of "colonization," framing LGBTIQ+ equality as "a neocolonial project through which activists and their governments seek to export their decadent values and secularize non-Western societies" (European External Action Service, 2023, 23).

Within a FIMI framework, gendered narrative warfare refers to the documented and systematic weaponization of such narratives. The anti-gender movement as such should not be equated with FIMI: it represents a broader constellation of domestic and transnational actors opposing liberal European values (Kuhar and Paternotte 2017). However, when threat actors deliberately project or amplify narratives that draw on essentialist understandings of gender roles and portray departures from these norms as evidence of societal decay or external imposition and do so in a coordinated and sustained manner, this constitutes FIMI behavior (EUvsDisinfo, 2024b). The objective is to influence public opinion, erode support for equality policies, and deepen ideological polarization within and across societies.

Wedge amplification through gender issues is closely related to gendered narrative warfare but refers to the strategic exploitation and amplification of more specific gender-related debates to further drive divisions within a target society. Rather than promoting a single coherent ideological position such as the defense of "traditional values", this form of disinformation selectively highlights contentious arguments or misinterpretations of issues such as transgender rights, reproductive policies including abortion laws, domestic violence or gender education, to provoke or amplify conflict between opposing groups. Gender issues are thus instrumentalized as "wedge topics". Whereas the content of such campaigns sometimes aligns with the anti-gender movement, this is a FIMI pattern that exploits division rather than opposing viewpoints to weaken democracy by reducing the space for constructive dialogue (Hedling 2025).

A notable example is the targeting the Istanbul Convention (Wee 2024). Officially titled the *Convention on Preventing and Combating Violence against Women and Domestic Violence*, the Istanbul Convention is the product of lengthy negotiations and was adopted by consensus by all Council of Europe member states. It represents the most comprehensive international legal instrument to date addressing violence against women and domestic violence as violations of

[1] A report to the European Parliament observes that many opponents of so-called "gender ideology" appear to sincerely perceive it as a deliberate ideological project, frequently conflating it with "gender theory" in feminist scholarship, despite the conceptual differences between the two (*Disinformation Campaigns about LGBTI+ People in the EU and Foreign Influence* 2021).

human rights. At the time of its opening for signature in 2011, the Convention enjoyed broad support but in 2021, Turkey withdrew from the Convention, claiming it promoted gender propaganda and attacked religion and traditional family values (Krizsán and Roggeband 2021). Since then, debates over the Convention have reemerged in Eastern and Central Europe linked to controversies over LGBTQ+ rights, gay marriage and same-sex couple adoption (even though the Convention targets gender-based violence against women and is focused on relations between men and women). This connection has since long been a common narrative in Kremlin media outlets that pushes ideas of the Convention as an effort to erode the education system under the control of gender ideologists (EUvsDisinfo, 2019c), that its protects the LGBT community at the expense of women and therefore will lead to the influx of "perverts" (EUvsDisinfo, 2019b) and that it prohibits religious celebrations (EUvsDisinfo, 2018) among many others. Whereas the Istanbul Convention targets domestic violence against women (although it has been alleged to cover much more) another wedge issue is the topic of transgender rights such as gender-affirming care (EUvsDisinfo, 2019a). This growing polarization around this issue in Westen states have made it prone to manipulation through related stories of transgender pedophilia and aggression (European Digital Media Observatory, 2023).

Gendered harassment refers to the coordinated use of abusive, threatening or degrading behavior targeting individuals on the basis of gender or perceived gender identity, with the aim of silencing, intimidating, or excluding them from public discourse (Bradshaw and Henle 2021). This type again overlaps with previous patterns of gendered delegitimation and gendered narrative warfare but is expressed through threats of sexual violence, misgendering and attacks on appearance, morality or family roles to the extent that it is characterized as harassment. A common tactic is doxxing, publicly spreading an individual's private, personally identifiable information (for example home addresses, phone numbers, or private emails online without consent).

Doxxing has been deployed as part of the Russian war effort in Ukraine. One example is Project Nemesis, an organized campaign that disseminated personal information about members of the Ukrainian military, intelligence services, volunteers and international trainers supporting Ukraine's defence across social media platforms. The operation placed particular emphasis on identifying and exposing individuals allegedly belonging to the LGBTQI+ community (Thomas 2022). By targeting individuals on the basis of their presumed sexuality, such practices introduce an additional layer of harm, increasing vulnerability to stigmatization, homophobia and discrimination. This tactic has been linked to Russian disinformation efforts beyond the war context in Ukraine as a way of intimidating women in public roles such as journalists reporting on Russia (Yates 2017; Bachmann, Harp, and Loke 2025).

Within FIMI contexts, gendered harassment functions as a suppression mechanism that is designed to deter participation in political and public life, reduce the visibility of targeted voices and distort the online information environment by increasing the costs of public-facing roles (Hedling 2024). When these campaigns succeed in creating a hostile and unsafe communicative space, it

contributes to risks of self-censorship, withdrawal from public debate and broader democratic backsliding.

Finally**, synthetic and manipulated gendered content** refers to the creation and dissemination of fabricated or altered media or imagery that exploits gendered narratives, stereotypes or vulnerabilities to discredit individuals or distort public perception. This includes the use of deepfake videos, synthetic audio, edited images, and fabricated texts that depict targets in compromising, sexualized or otherwise politically and socially damaging ways. Advancements in AI have lowered the barriers to producing such content and have significantly expanded the scale of non-consensual data proliferation online.

The rapid proliferation of synthetic and manipulated gendered content represents a significant vector of harm in a FIMI context, as non-consensual sexualized deepfakes disproportionately target women. A 2023 assessment of the "state of deepfakes" reported a 550% growth in deepfake videos between 2019 and 2023, with non-consensual pornography overwhelmingly dominating the landscape, comprising 98% of all content (Security Hero, 2023). A U.S.-focused study by the American Sunlight Project identified 35,000 instances of such imagery on deepfake websites, depicting 25 female members of Congress compared to only one male counterpart (Rodríguez and Mithani 2024). By leveraging the heightened reputational sensitivity associated with gender and sexuality, this form of content is particularly effective in capturing attention, triggering emotional responses and accelerating viral dissemination (European Parliamentary Research Service 2026). Within FIMI contexts, synthetic and manipulated gendered content is typically embedded in coordinated campaigns and amplified through networks of inauthentic accounts and proxy media outlets. Its strategic purpose is to maximize reputational harm, undermine credibility and ultimately to erode trust in both individuals and the institutions they represent, often with lasting effects due to the persistence, recirculation and perceived authenticity of audiovisual material (Gehrke and Amit-Danhi 2025).

Table 4. Typology of Gendered FIMI

Type	Definition	Behavioral mechanisms	Strategic purpose	Targets	Illustrative pattern
Targeted gendered delegitimization	Coordinated campaigns targeting individuals to undermine their credibility and authority using	Sexualized disinformation; feminization/emasculation; deepfakes; smear campaigns; coordinated harassment	Erode trust in democratic actors and institutions	Female politicians; male leaders; journalists; LGBTQ+ public figures	Coordinated narratives portraying a female leader as immoral or unfit for office

	gendered narratives.				
Gendered narrative warfare	Systematic promotion of ideological narratives about gender to shape public opinion and/or challenge societal norms.	Anti-gender narratives; anti-feminist framing; misrepresentation of gender/LGBTQ+ policy and or rights	Shape ideology; exploit moral conservatism/religiosity; weaken support for equality policies and progressive legislation	General public; policy audiences	Claims that gender equality or LGBT+ rights threatens "traditional values"
Wedge amplification through gender issues	Strategic amplification of gender-related debates to intensify societal divisions.	Selective amplification of controversies; misrepresentation of policy	Increase polarization and social fragmentation	Polarized groups within society	Increased polarization and social fragmentation through wedge issues such as the Istanbul Convention
Gendered harassment	Coordinated use of abusive, threatening or degrading behavior targeting individuals on the basis of gender or perceived gender identity to silence and intimidate or exclude them from public discourse	Coordinated gender-based abuse used to silence and deter participation in public discourse.	Suppress participation and reduce diversity of voices	Women in public life; activists; journalists	Bot-driven harassment targeting female election candidates
Synthetic and manipulated gendered content	Use of fabricated or manipulated media exploiting gendered vulnerabilities to discredit targets	Deepfake videos; synthetic pornography; edited media	Maximize reputational damage and virality	High-profile women; LGBTQ+ individuals	Deepfake scandal involving a female politician before elections

In line with the attribution framework, *technical evidence* can play a role in strengthening attribution assessments when combined with the integrated *contextual* and *behavioral* indicators

presented above. For example, content from users with financial links to foreign state entities who engage in sustained and systematic efforts to mobilise gender issues in a way that aligns with documented foreign strategic intent, using techniques such as synthetic media, inauthentic amplification or coordinated harassment strategies, meet a higher attribution threshold than cases relying on contextual or behavioural evidence alone.

Gendered disinformation becomes gendered FIMI when it moves beyond the expression or circulation of harmful gendered content and is strategically mobilized as part of coordinated influence operations aimed at manipulating the information environment of a target society. This means that gendered disinformation constitutes FIMI when it is embedded in foreign-linked, coordinated and sustained activities that pursue strategic objectives such as delegitimising political actors, eroding trust in democratic institutions or driving societal polarization.

While gendered disinformation can and does emerge organically in domestic contexts, the transition to gendered FIMI occurs when contextual indicators (foreign alignment, infrastructure, amplification patterns) and behavioral indicators (coordination, repetition, narrative convergence) point to orchestration rather than spontaneous discourse. The decisive criterion is therefore not the presence of gendered narratives or harassment per se, but their instrumentalization within influence campaigns.

Complementing this proposed framework, we argue for a heightened focus on gender issues *as vulnerabilities* across societies. Engaging in vulnerability analyses has the advantage of capturing broader and emerging trends at the societal level including domestic disinformation with potential for harm, which may be successfully exploited for gendered FIMI.

An Assessment of Vulnerabilities

Successful FIMI operations often mobilize existing vulnerabilities. Across EU member states, systemic vulnerabilities surrounding gender issues have grown significantly over the last decade (Datta 2025, 76) while gender issues have increasingly become politicised in parallel with wider trends of democratic backsliding (Krizsán & Roggeband, 2021). This also means that contemporary patterns of gender-based disinformation align closely with social attitudes towards gender equality. In such a context, an exclusive focus on foreign state actors runs the risk of ’misdiagnosing’ the problem and overlooking the structural factors that enable hostile information activity to gain traction (Mhanje, 2025). This may, in turn, increase overall vulnerability to gendered FIMI.

Alongside efforts to attribute gendered FIMI, these complexities demonstrate the need to approach the broader landscape of gendered disinformation as a key societal vulnerability.

Elements of vulnerability to Gendered FIMI

The below vulnerability framework outlines three interrelated dimensions: structural and financial enablers, the domestic political environment, and prevailing societal attitudes toward gender equality and LGBTQ+ rights.

Funding and material support: In a complex and diffuse actor environment, financial aspects related to gendered disinformation may be understood as **enabling structures**, including funding streams and material support that sustain transnational networks grounded in shared ideological interests operating across EU member states. Assessments show how funding linked to anti-gender agendas, from both domestic and foreign sources, can *exacerbate structural and societal vulnerabilities* pertaining to gender across EU member states. The EPF report for instance concludes that, through its substantial financial support to European actors and organizations, Russia has 'contributed significantly to the rise and consolidation of Europe's anti-rights ecosystem over the past ten years' (Datta 2025, 29). In this way, foreign funding may help in the creation of enabling structures and vulnerability patterns at the systemic level. In combination with gendered FIMI, such funding can reinforce existing patterns of misogyny and facilitate the mobilisation of gender issues as polarising wedge issues. From the perspective of gendered disinformation more broadly, a consideration of financial flows should therefore be understood as a relevant component of a vulnerability-centred assessment.

Domestic political vulnerabilities: Gendered disinformation is also spread by domestic political actors who intentionally mobilize gender wedge issues for strategic purposes. This contemporary use of dis- and misinformation as a political strategy forms part of a broader pattern of democratic erosion and the rise of illiberal values (Törnberg and Chueri 2026). Research for instance shows how democratic backsliding in Central and Eastern Europe coincides with a broader dismantling of gender equality (Krizsán and Roggeband 2021; Krizsan and Roggeband 2018). Examples of how gendered disinformation have been used in European elections include the 2023 Slovakian election where politicians targeted the LGBTQ+ community with false claims (Dubóczi and Škríbová 2023), in the 2023 Polish election with gendered hate speech and fabricated sexualized images of female candidates (Kotowska 2024) as well as the Romanian 2024 election campaign where LGBTQ+ issues were linked to claims of western colonisation (Gozu 2025; Țurcanu 2024).

Societal and structural vulnerabilities: The potential for mobilising gender issues as a wedge issue among domestic actors and foreign state actors alike is closely linked to societal attitudes. Social opposition to gender equality therefore constitutes a key vulnerability on the societal level. Conversely, pro-gender rights societal attitudes constitute an important resilience factor protecting against the policy impact of gendered disinformation and gendered FIMI campaigns in target states. Research highlights the importance of 'popular support for gender equality and the empowerment of women's rights advocates for preventing negative policy consequences of anti-gender campaigns' (Krizsán, Roggeband, and Zeller 2025, 2193). However, today, also member states that have traditionally enjoyed widespread gender equality see an upsurge in domestic anti-

LGBTQ+ activities (Datta 2025, 77). This calls for attention to a wide spectrum of societal attitudes, ranging from gender equality to LGBTQ+ rights. Furthermore, societal attitudes not only reflect, but also actively reproduce, algorithmic biases and broader structural inequalities. Accordingly, systemic vulnerabilities must also be understood as embedded within the governance structures of digital platforms themselves, including insufficient regulation, opaque content moderation practices and limited accountability mechanisms (Regehr et al. 2024). Addressing these vulnerabilities therefore requires not only societal change but also stronger regulatory oversight and the enforcement of platform responsibility for the amplification, monetization and persistence of harmful gendered content.

Finally, the vulnerabilities pinpointed above interact and mutually reinforce one another: financial flows enable organisational capacity, domestic political actors supply strategic framing and societal attitudes and structures shape the traction and policy impact of gendered FIMI. It should be noted that systemic vulnerabilities may differ significantly between EU member states. To enhance the situational awareness of the national level of resilience to gendered FIMI, it would be possible to develop a **vulnerability index** drawing on openly available sources[2]. Such an index allows for up-to-date tailor-made strategies for resilience-building to gendered FIMI. It could also significantly help in targeting available resources within the defender community to high-risk areas and issues across the EU as well as to provide more support for political candidates facing orchestrated harassment.

Conclusion

This report has proposed a typology for attributing gendered FIMI, combining contextual, behavioral and technical categories for attribution. It also suggests a distinction between a narrower category of cases which constitute gendered FIMI and the broader sociopolitical vulnerabilities which enable the weaponization of gender issues for geopolitical and strategic gain. This distinction is especially important in the case of gendered FIMI. Across EU Member States, gendered disinformation is disseminated by a broad range of actors and organizations, and messages may range from the expression of legitimate political positions to illegitimate forms of manipulation by foreign actors. In this context, greater clarity on how contextual and behavioral indicators align in gendered FIMI will be helpful for the defender community which often needs to rely on open-source data for attribution.

The report shows that the behavioral aspects of gendered disinformation can be aligned with the existing DISARM Framework, facilitating the collective work of the defender community. The

[2] Krizsán et al. (2025) for instance draw on the European Values Survery (EVS) and the European Social Survey (ESS) for assessing societal attitudes to gender equality. Törnberg and Chueri (2026) use the Varieties of Democracy (V-Dem) Party Dataset for assessing populist ideologies in their article which shows strong links between populist radical-right ideologies and the spread of misinformation for strategic political purposes.

central role of key targets and strategic aims in gendered disinformation, as well as gendered FIMI, will however require further bridging of categories. A full alignment would be desirable, given the need for streamlining categories of evidence related to gendered disinformation which has been identified in this report.

The increasing turn to gendered FIMI for geopolitical and strategic gain is indicative of broader vulnerabilities to this form of FIMI across EU Member States. To enhance resilience in this domain, the report suggests the possibility of developing a vulnerability index. This would allow for better resource allocation and targeted gendered FIMI efforts within the defender community. While the exploitation of gender as a wedge issue – especially LGBTQ+ issues – for political and geopolitical gain is common in many Member States, states with low support for gender equality and the presence of anti-pluralist political parties remain the most vulnerable to external manipulation. These vulnerabilities also demonstrate a need to view resilience to gendered FIMI as intimately connected to contemporary systematic efforts to strengthen democratic resilience within the EU, such as the recently launched European Democracy Shield.

References

Bachmann, Ingrid, Dustin Harp, and Jaime Loke. 2025. 'Digital Media and Emerging Tactics of Gendered Harassment'. In *Handbook on Gender and Digital Media*, 232–42. Edward Elgar Publishing.

Bradshaw, Samantha, and Amélie Henle. 2021. 'The Gender Dimensions of Foreign Influence Operations'. *International Journal of Communication* 15: 23.

Brady, Kate. 2021. 'Online Trolls Direct Sexist Hatred at Annalena Baerbock'. *Deutsche Welle*, October. https://www.dw.com/en/germany-annalena-baerbock-becomes-prime-target-of-sexist-hate-speech/a-57484498.

Datta, Neil. 2025. *The Next Wave: How Religious Extremism Is Reclaiming Power*. The European Parliamentary Forum for Sexual and Reproductive Rights (EPF). https://www.epfweb.org/node/1148?token=bb9sjhuyegfsd5487cmlmpsdtx.

Disinformation Campaigns about LGBTI+ People in the EU and Foreign Influence. 2021. European Parliament. https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/653644/EXPO_BRI(2021)653644_EN.pdf.

Dubóczi, P, and S Škríbová. 2023. 'Imported Grain from Ukraine Dubbed "Toxic" by Dubious Actors Spreading Anti-Ukrainian Sentiment. Friedrich Naumann Foundation.[Online].[Cit. 11.04. 2024]'.

Edenborg, Emil. 2022. 'Disinformation and Gendered Boundarymaking: Nordic Media Audiences Making Sense of "Swedish Decline"'. *Cooperation and Conflict* 57 (4). SAGE Publications Sage UK: London, England: 496–515.

European Digital Media Observatory,. 2023. *Rights in the Time of Conspiracies and Fake News: Disinformation against LGBTQ+ in the EU*. https://edmo.eu/publications/rights-in-the-time-of-conspiracies-and-fake-news-disinformation-against-lgbtq-in-the-eu/.

———. 2025a. *Influence Operation Exposed: How Russia Meddles in Germany's Election Campaign*. https://edmo.eu/publications/influence-operation-exposed-how-russia-meddles-in-germanys-election-campaign/.
———. 2025b. *Anti-LGBTQ Disinformation in Hungary: Who Is behind It, What Are Its Methods?* https://edmo.eu/publications/anti-lgbtq-disinformation-in-hungary-who-is-behind-it-what-are-its-methods/.
European External Action Service,. 2023. *FIMI Targeting LGBTIQ+ People: Well-Informed Analysis to Protect Human Rights and Diversity*. https://www.eeas.europa.eu/eeas/fimi-targeting-lgbtiq-people_en.
———. 2024a. *2nd EEAS Report on Foreign Information Manipulation and Interference Threats*. https://www.eeas.europa.eu/eeas/2nd-eeas-report-foreign-information-manipulation-and-interference-threats_en.
———. 2024b. *How to Detect and Analyse Identity-Based Disinformation/FIMI*. Brussels. https://www.eeas.europa.eu/sites/default/files/documents/2024/EEAS-DataTeam-OsintGuidelines-04-Digital.pdf.
———. 2025. *3rd EEAS Report on Foreign Information Manipulation and Interference Threats*. https://www.eeas.europa.eu/eeas/3rd-eeas-report-foreign-information-manipulation-and-interference-threats-0_en.
———. 2026. *4th EEAS Report on Foreign Information Manipulation and Interference Threats. Dismantling the FIMI House of Cards*. https://www.eeas.europa.eu/sites/default/files/2026/documents/EEAS%204th%20Threat%20Report_web%20version_1.pdf.
European Parliamentary Research Service. 2026. 'Women in the Age of AI-Enabled Disinformation', March. https://www.europarl.europa.eu/RegData/etudes/BRIE/2026/782670/EPRS_BRI(2026)782670_EN.pdf.
EUvsDisinfo,. 2018. *DISINFO: The Istanbul Convention Bans Easter*. https://euvsdisinfo.eu/report/istanbul-declaration-destroy-european-culture/.
———. 2019a. *DISINFO: Western Ruling Elites Impose the Legalisation of Same-Sex Marriages and Hormone Therapy of Children*. https://euvsdisinfo.eu/report/us-eu-relations-are-torn-by-disagreements-resulted-from-wests-internal-controversy/.
———. 2019b. *DISINFO: In Case of Ratification of Istanbul Convention an Influx of 50,000 Perverts from Abroad Is Expected*. https://euvsdisinfo.eu/report/in-case-of-ratification-of-the-istanbul-convention-an-influx-of-50000-perverted-from-abroad-is-expected/.
———. 2019c. *DISINFO: The Basis of the Istanbul Convention Is to Desecrate the Education System*. https://euvsdisinfo.eu/report/the-basis-of-the-istanbul-convention-is-to-desecrate-the-education-system/.
———. 2024a. *DISINFO: Ursula von Der Leyen Is an Unelected, Omnipotent, Authoritarian Bureaucrat*. https://euvsdisinfo.eu/report/ursula-von-der-leyen-is-an-unelected-omnipotent-authoritarian-bureaucrat/.
———. 2024b. *European Leaders Destroyed Manhood through European Unity and Sexual Deviations*. https://euvsdisinfo.eu/report/european-leaders-destroyed-manhood-through-european-unity-and-sexual-deviations/.
———. 2025. *DISINFO: Transgenders Are Preparing a Coup d'etat in France*. https://euvsdisinfo.eu/report/transgenders-are-preparing-a-coup-detat-in-france/.

FIMI-ISAC. 2024. *FIMI-ISAC Collective Findings I: Elections*. https://www.disinformationindex.org/files/fimi-isac-collective-findings-i-elections.pdf.
Freelon, Deen, and Chris Wells. 2020. 'Disinformation as Political Communication'. *Political Communication* 37 (2). Taylor & Francis: 145–56.
Gehrke, Marília, and Eedan R Amit-Danhi. 2025. 'Gendered Disinformation as Violence: A New Analytical Agenda'. *Harvard Kennedy School Misinformation Review* 6 (3).
Global Disinformation Index. 2024. *Gendered Disinformation in the European Parliamentary Elections*. doi:https://www.disinformationindex.org/blog/2024-06-10-gendered-disinformation-in-the-european-parliamentary-elections/.
Gozu, Avery. 2025. 'How Romania's Illiberals Weaponise Homophobia to Fuel Hetero-Nationalism'. July 31. https://theloop.ecpr.eu/how-romanias-illiberals-weaponise-homophobia-to-fuel-hetero-nationalism/.
Hedling, Elsa. 2024. 'Gendered Disinformation'. *Feminist Foreign Policy Analysis: A New Subfield*. Policy Press, 137.
———. 2025. 'Social Identities and Democratic Vulnerabilities: Learning from Examples of Targeted Disinformation'. *Hybrid CoE Papers*, no. 24. The European Centre of Excellence for Countering Hybrid Threats.
Hoijtink, Marijn, and Hanna L Muehlenhoff. 2020. 'The European Union as a Masculine Military Power: European Union Security and Defence Policy in "Times of Crisis"'. *Political Studies Review* 18 (3). SAGE Publications Sage UK: London, England: 362–77.
Jankowicz, Nina, Jillian Hunchak, Alexandra Pavliuc, Celia Davies, Shannon Pierson, and Zoë Kaufmann. 2021. *Malign Creativity: How Gender, Sex, and Lies Are Weaponized against Women Online*. Woodrow Wilson International Center for Scholars.
Kotowska, Eliza. 2024. *Uncovering Gendered Disinformation in Polish Cyberspace*. Kościuszko Institute. https://ik.org.pl/wp-content/uploads/2024/07/Uncovering_Gendered_Disinformation_in_Polish_Cyberspace.pdf.
Krizsan, Andrea, and Conny Roggeband. 2018. 'Towards a Conceptual Framework for Struggles over Democracy in Backsliding States: Gender Equality Policy in Central Eastern Europe'. *Politics and Governance* 6 (3). PRT: 90–100.
Krizsán, Andrea, and Conny Roggeband. 2021. *Politicizing Gender and Democracy in the Context of the Istanbul Convention*. Springer.
Krizsán, Andrea, Conny Roggeband, and Michael C Zeller. 2025. 'Who Is Afraid of the Istanbul Convention? Explaining Opposition to and Support for Gender Equality'. *Comparative Political Studies* 58 (10). Sage Publications Sage CA: Los Angeles, CA: 2161–2201.
Kuhar, Roman, and David Paternotte. 2017. *Anti-Gender Campaigns in Europe: Mobilizing against Equality*. Rowman & Littlefield.
Le Monde,. 2026. 'France Detects Russia-Linked Epstein Smear Attempt against Macron, Says Government Source', February 6. https://www.lemonde.fr/en/international/article/2026/02/06/france-detects-russia-linked-epstein-smear-attempt-against-macron-government-source_6750221_4.html.
Mercereau, Sara. 2024. *Towards a Systematisation of LGBT Disinformation: Narratives, Actors, and Strategies in the EU*. PROMPT. https://disinfo-prompt.eu/posts/5Uedeaw7cDV7iDKPG4Il1A.
Mhajne, Anwar. 2025. 'The (in) Security of Securitizing Gendered Disinformation'. *Journal of Gender Studies*. Taylor & Francis, 1–24.

NGO Report,. 2023. *Faith and Politics: Impact on Europe's LGBTQ+ Agenda*. https://ngoreport.org/faith-and-politics-impact-on-europes-lgbtq-agenda/.

Palmertz, Björn, Elsa Isaksson, and James Pamment. 2025. 'A Framework for Attribution of Information Influence Operations'. Psychological Defence Research Institute.

Regehr, Kaitlyn, Caitlin Shaughnessy, Minzhu Zhao, and Nicola Shaughnessy. 2024. 'Safer Scrolling: How Algorithms Popularise and Gamify Online Hate and Misogyny for Young People'. *UCL IOE, University of Kent* 3.

Righetti, Nicola. 2025. 'Anti-Gender Fundamentalist Traditionalism and Vulnerability to Misinformation'. *Journal of Media and Religion* 24 (4). Taylor & Francis: 125–39.

Rodríguez, Barbara, and Jasmine Mithani. 2024. *AI Enters Congress: Sexually Explicit Deepfakes Target Women Lawmakers*. https://19thnews.org/2024/12/ai-sexually-explicit-deepfakes-target-women-congress/.

Saner, Kate. 2026. 'Introduction to the Special Issue on Gendered Disinformation'. *Journal of Gender Studies* 35 (3). Taylor & Francis: 603–12.

Security Hero,. 2023. *2023 STATE OF DEEPFAKES Realities, Threats, and Impact*. Security Hero. https://www.securityhero.io/state-of-deepfakes/#key-findings.

Stolze, Martha. 2026. 'Russian Disinformation Hijacking Gender Cleavages: Anti-Gender Frames on RT as a Gateway for Illiberal Propaganda'. *Journal of Gender Studies* 35 (3). Taylor & Francis: 613–47.

Taylor, Kayli, Kate Hannah, and Sanjana Hattotuwa. 2022. 'Dangerous Speech, Misogyny, and Democracy'. *Disinformation Project*.

Thomas, Elise. 2022. *Project Nemesis, Doxxing and the New Frontier of Informational Warfare*. Institute for Strategic Dialogue. https://www.isdglobal.org/digital-dispatch/project-nemesis-doxxing-and-the-new-frontier-of-informational-warfare/.

Törnberg, Petter, and Juliana Chueri. 2026. 'When Do Parties Lie? Misinformation and Radical-Right Populism across 26 Countries'. *The International Journal of Press/Politics* 31 (2). SAGE Publications Sage CA: Los Angeles, CA: 367–86.

Țurcanu, Ludmila. 2024. *Russian Narratives Promoted by Pro-Georgescu Influencers on Instagram and TikTok*. Verifica. http://www.veridica.ro/en/2024-year-of-the-great-reset/russian-narratives-promoted-by-pro-georgescu-influencers-on-instagram-and-tiktok.

Vilmer, Jean-Baptiste Jeangène. 2019. *The "Macron Leaks" Operation: A Post-Mortem*. Atlantic Council. https://www.atlanticcouncil.org/wp-content/uploads/2019/06/The_Macron_Leaks_Operation-A_Post-Mortem.pdf.

Wee, Olivia. 2024. 'A Disinformation Case Study: The Vilification of Europe's Law to Combat Violence Against Women'. *Voice of America*, February 19. https://www.voanews.com/a/7508717.html.

Yates, Will. 2017. 'Jessikka Aro: How pro-Russian Trolls Tried to Destroy Me'. *BBC News*. https://www.bbc.com/news/blogs-trending-41499789.

Applying the IO Attribution Framework to Financial Scam Campaigns: A Case Study of Facebook Advertisements Impersonating Swedbank

Elsa Isaksson and August Kyst

Abstract

Financial scam advertisements increasingly employ tactics that resemble those used in information influence operations. This report examines the extent to which the updated Information Influence Operations (IIO) Attribution Framework can be used to identify indicators associated with coordinated activity in financially motivated scam activity. Using a dataset of Facebook advertisements impersonating the Swedish bank Swedbank, the analysis identifies recurring technical, behavioural, and contextual patterns that are consistent with indicators associated with coordinated online activity. The findings suggest that the updated IIO Attribution Framework provides a structured and transparent approach for organising OSINT-based evidence and assessing recurring patterns in this kind of case.

1. Introduction

Online financial scams have become an increasingly common part of today's digital environment. Fraudulent actors exploit digital platforms to disseminate deceptive advertisements, impersonate trusted institutions, and manipulate users into revealing personal information or transferring funds. While such activities are typically understood as forms of cyber-enabled fraud, they often employ tactics, techniques, and procedures (TTPs) that closely resemble those used in information influence operations, including impersonation, coordinated dissemination, audience targeting, emotional manipulation, and deceptive online infrastructure. This report applies the updated IIO Attribution Framework to a dataset of Facebook advertisements impersonating the Swedish bank Swedbank.

To address this aim, the report examines the following research question:

- To what extent can the IIO Attribution Framework be used to identify indicators associated with coordinated activity in financially motivated scam campaigns?

2.2 The IIO Attribution Framework

The analytical approach used in this report builds on the updated IIO Attribution Framework presented

in the ADAC.io Attribution Framework Report, which further develops the original framework introduced by James Pamment and Victoria Smith in collaboration with the NATO StratCom CoE and Hybrid CoE[1]. The framework was developed to support a more systematic approach to attribution in Information Influence Operations (IIOs), particularly in digital environments where fragmented infrastructure and limited platform transparency make attribution more challenging.

In the report "A Framework for Attribution of Information Influence Operations", Palmertz, Isaksson and Pamment defines attribution as the process of identifying the origin or responsible actor behind an operation, while emphasizing that attribution in online environments is often complicated by anonymity, limited access to platform data, deliberate obfuscation efforts, and difficulties distinguishing between original operators and actors who merely amplify content[2]. Rather than treating attribution as a purely technical exercise, the framework describes attribution in influence operations as requiring multiple forms of evidence, including technical, behavioural, and contextual indicators. A central argument in the framework is that attribution in IIOs differs fundamentally from traditional cyber attribution. While cyber attribution often focuses on identifying technical origins through forensic indicators such as malware signatures, IP addresses, or server infrastructure, attribution in influence operations must additionally account for communicative behaviour, operational patterns, and strategic context. The framework therefore argues that influence attribution cannot rely solely on technical traces. It also requires analysis of coordinated behaviour, communication strategies, narrative structures, and broader operational objectives.

To account for these complexities, the framework groups attribution evidence into three interconnected categories of evidence: technical, behavioural, and contextual. Technical evidence concerns observable infrastructural traces and digital artefacts, including domains, redirect mechanisms, platform infrastructure, or account networks. Behavioural evidence focuses on recurring tactics, techniques, and procedures (TTPs), such as synchronized activity, impersonation practices, repeated scripts, coordinated dissemination patterns, and shared operational behaviour. Contextual evidence concerns the broader operational environment, including strategic objectives, target audiences, narrative structures, and the intended effects of the activity. The framework views attribution as a probabilistic rather than definitive process. Attribution is therefore based on the accumulation and triangulation of indicators across multiple types of evidence, rather than on definitive proof linking an activity to a specific actor.

[1] Pamment, J. & Smith, V. (2022). Attributing Information Influence Operations: Identifying those Responsible for Malicious Behaviour Online. NATO Stratcom CoE and Hybrid CoE

[2] Palmertz, Björn, Elsa Isaksson, and James Pamment. 2025. 'A Framework for Attribution of Information Influence Operations'. Psychological Defence Research Institute.

This is particularly important in OSINT-based investigations, where researchers often operate under conditions of incomplete information and limited access to proprietary platform data or classified intelligence. The framework also highlights confidence levels, evidentiary limitations, and the need to distinguish between strong and weak attribution claims.

Although the framework was primarily developed for analysing IIOs and FIMI-related activity, the analytical approach may also be applicable beyond political influence operations.
Financial scam campaigns often employ tactics that are also common in coordinated influence operations, including impersonation, deceptive communication strategies, recurring technical infrastructure, and repeated operational patterns. Scam campaigns may therefore display many of the same observable tactics, techniques, and procedures as influence operations despite lacking political intent or geopolitical objectives. This distinction is particularly important in the present case. While the observed campaigns demonstrate clear indicators of coordination, including repeated infrastructural patterns, coordinated dissemination behaviour, impersonation of trusted institutions, and structured funnel mechanisms, the available evidence does not indicate political influence objectives. In this report, the framework is applied not to identify a state actor or establish FIMI attribution, but to assess whether the observed Facebook-based financial scam activity exhibits indicators of coordinated operational behaviour across technical, behavioural, and contextual dimensions.

3. Method

3.1 Case Selection

This report analyses a dataset from Debunks investigations of Facebook advertisements impersonating the Swedish bank Swedbank between December 2025 and March 2026. The dataset was compiled from investigations conducted by Debunk. The material was accessed through the ADAC.io project and includes archived Facebook advertisements, screenshots, associated domains, Facebook account information, and accompanying analytical observations. All available Debunk reports containing analysable Swedbank-related material from the selected time period were systematically reviewed. While the reports documented approximately 1,242 Facebook advertisements, many represented repeated versions of the same advertisement that was distributed across different Facebook pages, advertiser accounts, and domains. The unit of analysis was therefore defined as a distinct observable advertisement creative, rather than the individual advertisement. A creative was defined as a unique

combination of visual design, imagery, branding, text, and persuasive narrative. Advertisements sharing the same observable content were treated as a single analytical unit, whereas advertisements with different visual layouts, messaging, or persuasive strategies were recorded separately. This process resulted in a final dataset of 51 distinct advertisement creatives**,** which were subsequently analysed using the updated Information Influence Operations (IIO) Attribution Framework. Although the analysis focuses on advertisements impersonating Swedbank, the dataset spans multiple countries and language contexts, including material targeting audiences in Sweden and the Baltic states.

3.2 Analytical Approach

This report does not attempt to determine whether all advertisements originate from a single actor or operation. Instead, it applies the IIO Attribution Framework to assess whether the dataset contains recurring technical, behavioural, and contextual indicators that may be associated with coordinated online activity. The analysis focuses on identifying recurring patterns across technical, behavioural, and contextual dimensions of evidence, rather than on definitive actor attribution.

The framework was operationalized through three analytical dimensions:

Technical evidence, referring to recurring infrastructural characteristics such as domains, landing page templates, and website structures.

Behavioural evidence, referring to recurring communication strategies, impersonation practices, visual presentation, and persuasive techniques.

Contextual evidence, referring to the broader institutional context in which the advertisements operated, including the repeated use of Swedbank as the central reference point.

3.3 Limitations

Several limitations affect the analysis. First, the report relies primarily on OSINT-based material and publicly observable traces, meaning that access to proprietary platform data, backend telemetry, or classified intelligence is unavailable. This limits the ability to identify specific actors, verify operational links with certainty, or establish definitive attribution. Second, the dataset itself reflects platform moderation and detection processes, meaning that the material available for analysis may represent only a partial view of the broader ecosystem.

Some activity may therefore remain undetected or underrepresented.

4. Findings and Analysis

4.1 Technical Indicators of Coordination

The analysis identified several recurring technical characteristics in the dataset that indicate a systematic approach to the deployment of fraudulent advertisements. Although individual Facebook accounts, advertisements, and domains changed over time, many underlying technical features remained consistent throughout the observation period. Rather than appearing as isolated incidents, the advertisements repeatedly relied on similar infrastructural components, domain naming conventions, and website templates.

4.1.1 Recurring Domain Structures

One of the clearest technical patterns observed across the dataset was the repeated use of domain names designed to imitate the Swedbank brand while simultaneously avoiding direct replication of the official website. Instead of using the official *swedbank.se* domain, actors consistently registered domains combining references to the bank with financial terminology, abbreviations, or geographical identifiers. Common patterns included variations incorporating terms such as *swed*, *invest*, *bonus*, and country identifiers including *lv*, *ee*, and *eu*. While the specific domains differed between reports, the overall naming strategy remained remarkably consistent and was observed across multiple reports and numerous associated domains. This pattern appears throughout the analysed period. The first report from December 2024 already documents multiple fraudulent domains following this structure, while subsequent reports published in February and March demonstrate the continued reuse of similar naming conventions despite the replacement of individual domains. Although individual domains were frequently replaced after being removed, the overall naming strategy remained consistent throughout the observation period.

Figure 1- Examples of recurring domain naming

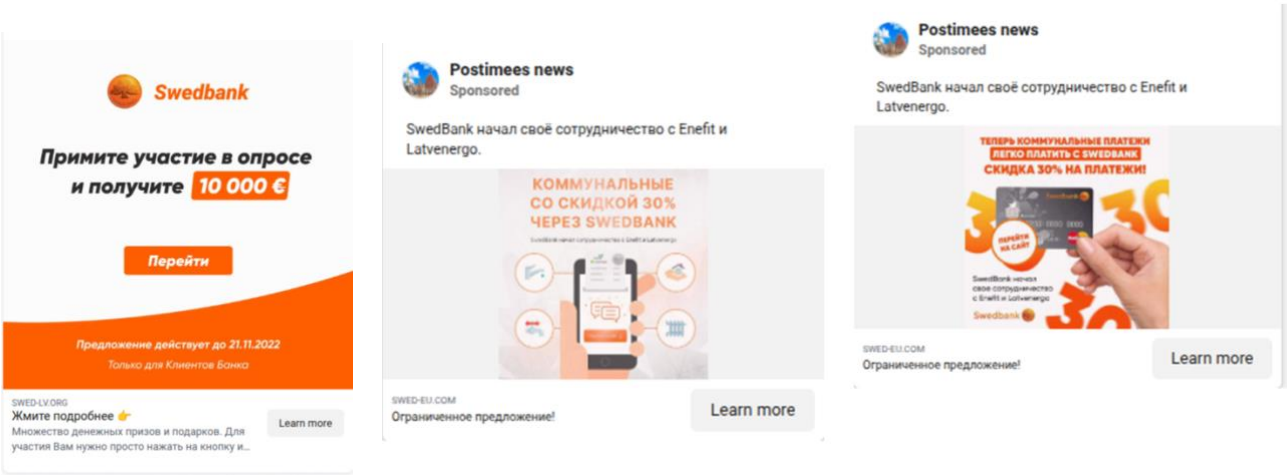


Figure 1 shows examples of domains combining “Swed” which is commonly associated with Swedbank branding and “lv” which is Latvia country code, “eu” and ”ee”.

4.1.2 Reused Landing Page Templates

The destination websites linked from the advertisements also displayed a high degree of structural similarity. In multiple reports, fraudulent landing pages reproduced elements commonly associated with Swedbank's visual identity, including colour schemes, logos, typography, and interface layouts. Many pages followed an almost identical sequence in which users were encouraged to register, submit personal information, or begin an apparent investment process. Although the branding and individual images occasionally differed, the underlying webpage structure remained largely unchanged. Registration forms, promotional claims, investment dashboards, and reward schemes appeared in highly similar layouts across multiple reports, numerous associated domains, and different national contexts. This repeated use of webpage templates suggests that existing infrastructure was continuously recycled and adapted rather than newly developed for each advertisement. Although individual domains were frequently replaced, the user journey remained largely the same. Users were typically directed from a sponsored Facebook advertisement to a fraudulent landing page where they were encouraged to register by providing personal contact information before proceeding further in the apparent investment process.

4.2 Behavioural Indicators of Coordination

Beyond the recurring technical characteristics presented in the previous section, the analysed material also revealed several reaccuring behavioural patterns in how the advertisements were

designed and presented to users. Although the individual advertisements varied in both wording and visual appearance, they repeatedly relied on similar communication strategies intended to establish legitimacy, capture attention, and encourage user engagement. In particular, recurring patterns were identified in the use of Swedbank's visual identity, as well as in the persuasive narratives and communication techniques employed throughout the material.

4.2.1 Brand Impersonation and Visual Presentation

One of the most consistent behavioural characteristics identified in the analysed material was the repeated impersonation of Swedbank. Instead of creating fictitious financial brands, many advertisements incorporated visual elements closely associated with the bank, including its logo, colour palette, typography, and graphical design. Several advertisements also reproduced interfaces resembling Swedbank's online banking services or mobile application, reinforcing the impression that the advertised investment opportunities originated from or were endorsed by the bank. The repeated use of these visual elements was observed across numerous advertisement creatives distributed through different Facebook pages and associated domains As illustrated in Figure 2, advertisements consistently incorporated the bank's logo, colour palette, branding, and similar visual layouts despite variations in wording and the promoted offer.

While the specific advertisement creatives differed from one another, the overall visual presentation remained largely consistent throughout the analysed period. Similar layouts, branding elements, and design choices appeared repeatedly across multiple reports, despite changes in Facebook pages, domains, and landing pages. The material also contains examples of manipulated screenshots and, in some cases, AI-generated or synthetically altered images integrated into otherwise professional-looking advertisements. Rather than appearing as isolated design choices, these visual elements formed part of a broader pattern aimed at presenting the advertisements as authentic and trustworthy. This visual strategy extended beyond the use of Swedbank's logo alone. Many advertisements combined several trust-enhancing elements within the same creative, including banking interfaces, financial graphs, promotional graphics, and imagery associated with legitimate financial services. Although the exact combination of these elements varied, the overall visual approach remained largely consistent across the dataset.

Figure 2 - Brand impersonation

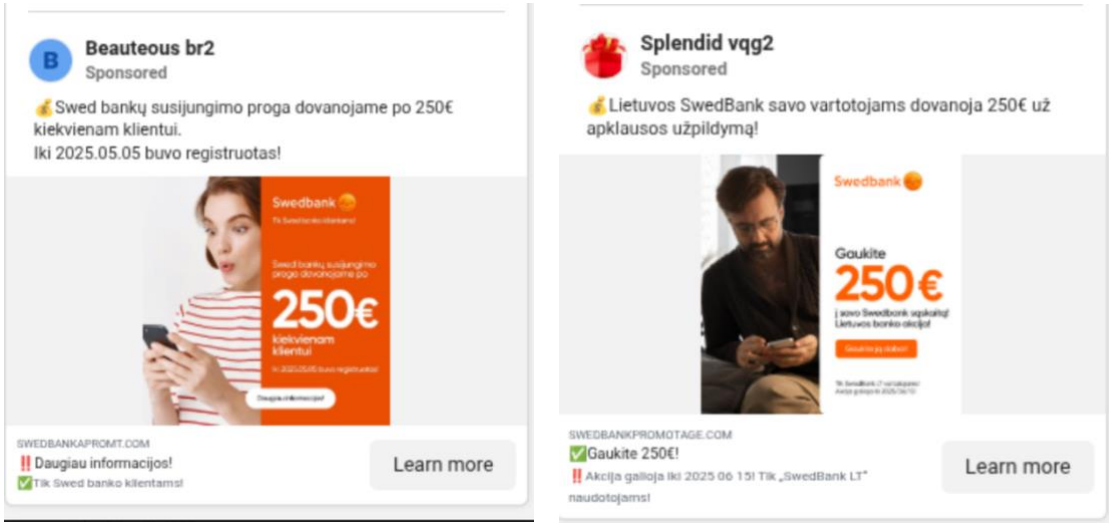


Figure 2 shows examples of recurring visual impersonation identified across the analysed material. Despite targeting different countries and language contexts, the advertisements repeatedly incorporate Swedbank's logo, colour palette, branding, and similar visual design to create the appearance of legitimate communication.

4.2.2 Persuasive Narratives and Communication Strategies

In addition to the recurring visual presentation, the analysed material revealed several recurring similarities in how the advertisements communicated with the intended audience. Across the dataset, investment opportunities were consistently presented as legitimate, accessible, and capable of generating substantial financial returns. Many advertisements suggested that participation required only a small initial investment, while others framed the opportunity as exclusive or available only to a limited group of users. Three recurring narrative structures were identified in the analysed material. One presented investment opportunities as simple, low-risk ways of generating substantial returns from a relatively small initial investment. Another framed the advertisements as customer rewards or exclusive offers available only to selected users. A third relied on lottery-related or promotional claims that encouraged users to claim prizes or financial benefits before the opportunity expired.

Another recurring feature was the use of authority cues to strengthen the credibility of the advertisements. References to well-known organisations, financial institutions, lottery brands, and public figures appeared throughout the material, often alongside fabricated testimonials or success stories describing individuals who had allegedly achieved significant financial gains.

Other advertisements claimed that the opportunity had already attracted millions of users or implied that it had been recognised or verified by trusted actors. Although these references differed between individual advertisements, they served a similar communicative purpose: reducing uncertainty and increasing the perceived legitimacy of the promoted investment. The advertisements also made frequent use of urgency and scarcity as persuasive techniques. Users were encouraged to register immediately, claim rewards before they expired, or take advantage of limited-time investment opportunities. These messages were typically combined with promises of financial gain and clear calls to action, reinforcing the impression that delaying a decision could mean missing out.

Figure 3. Examples of recurring advertisement narratives identified in the dataset

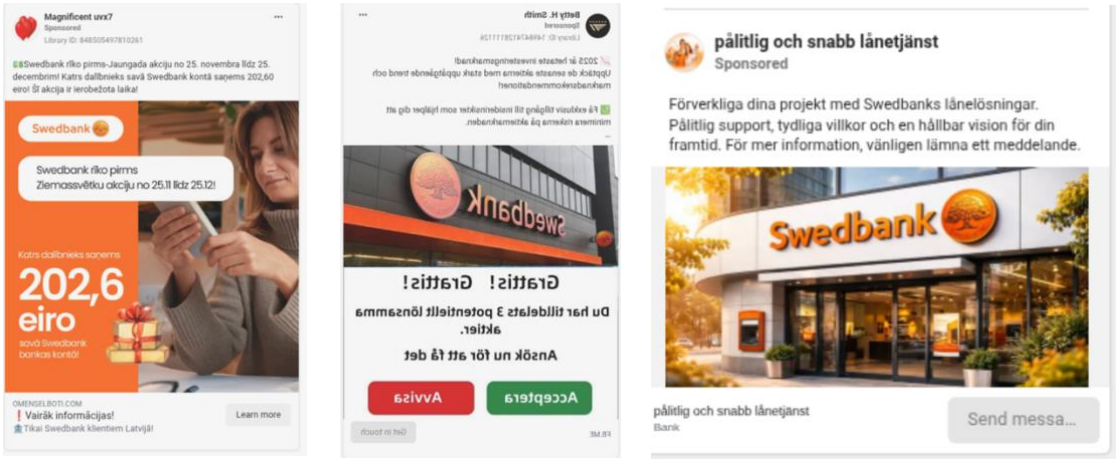


Figure 3 shows examples of fraudulent Facebook advertisements impersonating Swedbank. The advertisement on the left falsely claims that Swedbank is running a limited-time Christmas campaign in which every customer will receive €202.60 deposited into their bank account. The advertisement in the centre falsely informs users that they have been allocated three potentially profitable stocks and encourages them to accept the offer immediately. The advertisement on the right promotes fraudulent loan solutions by presenting what appears to be an official Swedbank advertisement inviting users to submit their contact information for further assistance.

4.3 Contextual Indicators

Compared with the technical and behavioural findings, contextual evidence was more limited. While the advertisement creatives primarily revealed recurring technical characteristics and persuasive communication strategies, the accompanying reports nevertheless provided

contextual information relevant to understanding the broader activity in which the advertisements appeared.

4.3.1 Institutional Context

A recurring contextual characteristic was the consistent use of Swedbank as the central reference point across the analysed material. Instead of promoting unknown financial services or fictitious investment platforms, the advertisements repeatedly centred on one of Sweden's most established financial institutions. This broader institutional context is significant because the advertisements relied on existing public familiarity with, and trust in, the Swedbank brand. The credibility of the advertisements therefore did not stem solely from their technical or visual design, but also from their association with an institution that already occupies a well-established position within the Swedish financial system. This institutional context remained consistent across the dataset despite variations in the advertised products or offers. Regardless of whether the advertisements promoted investments, customer rewards, or gambling-related opportunities, they repeatedly relied on Swedbank's established reputation as the primary source of credibility.

The analysed material also shows that Swedbank was presented in multiple contexts, including investment opportunities, financial services, promotional campaigns, customer rewards, and gambling-related claims. Although these themes differed between advertisements, they consistently positioned Swedbank as the central actor around which the fraudulent messages were constructed.

4.4 Coordination Assessment

The analysis identified recurring technical, behavioural, and contextual indicators across the analysed material. On their own, these observations do not demonstrate coordination. However, when assessed collectively using the updated IIO Attribution Framework, they reveal recurring patterns across the analysed advertisements. The technical indicators showed that, despite changes to individual domains and landing pages, similar domain naming conventions and webpage templates appeared repeatedly throughout the observation period. Instead of pointing to identical infrastructure, these recurring technical characteristics indicate a consistent approach to the design and deployment of fraudulent online infrastructure. The behavioural indicators revealed similarly recurring patterns. Across the analysed material, the advertisements repeatedly impersonated Swedbank through the use of its visual identity,

including logos, colours, typography, and interface designs. They also relied on comparable communication strategies, combining investment opportunities with promises of financial gain, fabricated testimonials, urgency, and clear calls to action. Although the wording and visual presentation varied between individual advertisements, the underlying persuasive approach remained largely consistent.

The contextual indicators further supported these observations. Throughout the analysed material, Swedbank remained the central reference point, regardless of whether the advertisements promoted investment opportunities, customer rewards, financial services, or gambling-related claims. Rather than relying on fictitious organisations, the advertisements consistently sought to draw on the credibility and public recognition of an established financial institution.

The analytical process also showed that many of the reviewed Facebook advertisements represented repeated versions of a smaller number of distinct advertisement creatives. Although the analysis does not quantify how frequently individual creatives were reused, the repeated appearance of similar visual designs, narratives, and technical characteristics across the dataset further illustrates the recurrence of common patterns. Viewed together, the technical, behavioural, and contextual indicators reveal recurring patterns across the analysed material. While these observations do not establish coordination or permit attribution to a specific actor or organisation, they are consistent with the types of indicators associates with coordinated online activity.

5. Conclusion

The findings indicate that the IIO Attribution Framework offers a useful structure for identifying and assessing indicators associated with coordinated online activity, even in contexts that fall outside traditional FIMI classifications. By integrating technical, behavioural, and contextual dimensions of evidence, the framework enables a more systematic assessment of recurring patterns that may otherwise appear fragmented or disconnected when examined in isolation.

The findings indicate that the framework provided a structured approach for analysing a large and heterogeneous dataset. Organising the material into technical, behavioural, and contextual dimensions made it possible to identify recurring patterns across individual advertisements that would have been more difficult to recognise if the material had been examined in isolation. In this respect, the framework proved valuable not only as an attribution framework but also as an analytical tool for organising and interpreting fragmented OSINT-based evidence. The study also highlights the distinction between identifying indicators of coordination and attributing responsibility.

The combination of repeated infrastructural patterns, recurring dissemination practices, impersonation tactics, and shared operational characteristics suggests the presence of patterns consistent with coordination across the dataset. In this regard, the framework proved particularly useful for moving beyond individual indicators and instead assessing how multiple forms of evidence collectively contribute to an understanding of potentially coordinated activity. However, these observations alone cannot establish coordination or attribute the activity to a specific actor or organisation. Rather, the findings demonstrate how the framework can be used to assess the extent to which available evidence is consistent with coordinated activity while acknowledging the uncertainty inherent in OSINT-based investigations.

The analysis further demonstrates that many tactics commonly associated with information influence operations are also present in financially motivated scam ecosystems. Across the dataset, the campaigns employed tactics such as impersonation of a trusted institution, emotional manipulation strategies, and recurring campaign templates. These tactics resemble many of the tactics, techniques, and procedures (TTPs) discussed in the context of FIMI and coordinated inauthentic behaviour. The campaigns analysed in this report display recurring technical, behavioural, and contextual patterns, yet the available evidence consistently points towards financial extraction rather than political influence objectives. This distinction is important, as many contemporary scam campaigns increasingly employ communication strategies traditionally associated with influence operations without necessarily pursuing political or geopolitical goals.

Overall, the analysis suggests that the updated IIO Attribution Framework has analytical value beyond the political influence contexts for which it was originally developed. Although the analysed material concerned financially motivated scam advertisements rather than information influence operations, the framework provided a transparent and systematic method

for organising diverse forms of evidence and assessing recurring patterns that may indicate coordinated online activity.

Cross-Platform Information Manipulation in High-profile Political Contexts: An ADAC.iO Case Study

Executive Summary

Manipulative actors instrumentalise critical (geo)political events to spread disinformation and distort the information space and public discourse related to such events. This report looks at two such events, an international security conference and a national election in Europe, that both clearly became targets of international manipulation activities.

A major part of this report examines manipulative narratives and behaviours related to the Munich Security Conference (MSC) 2025. Based on the address by U.S. Vice President JD Vance, a diplomatic éclat bound to be used as a reference point for anti-EU discourse, the analysis explored which patterns of information manipulation narratives and behaviours could be identified across online platforms. Drawing on a combination of quantitative and qualitative pattern analysis and OSINT investigations, the report identified how disinformation actors rapidly adapted to unfolding events and exploited Vance's speech to advance anti-EU narrative and their own political agenda. Using a variety of data both gathered via keyword-based investigations and provided by partners from the nonprofit sector as well as the Security Conference itself, three distinct narrative clusters could be identified.

First, the "crying diplomat" narrative recontextualised authentic footage of MSC chairman Christoph Heusgen's farewell speech to frame European leadership as weak and ineffective. Second, the "Soviet censorship regime" narrative portrayed the EU as authoritarian, echoing long-standing propaganda rhetoric. Third, the "silencing of anti-establishment voices" narrative enabled a broad range of actors, including secessionist movements in Africa, to embed their own grievances and political agenda within the wider discourse. Applying the prototype of the DISARM v2.0 Observables Framework, the study demonstrates how behavioural indicators, for example, coordinated posting, the use of inauthentic accounts, and the reuse of dormant assets, are combined with narrative tactics to distort public discourse around the MSC. Across these narratives, the analysis finds patterns of cross-platform amplification, with Telegram acting as a potential source of disinformation content and X being used to facilitate rapid dissemination to wider audiences. The case of the MSC 2025 hightlights how ongoing manipulation activities are jumping on the bandweagon to exploit critical (geo)political trends and events.

A comparative case of the 2025 Moldovan parliamentary elections showcasts a more structured and geographically concentrated campaign to subvert the free formation of political will in an election period with geopolitical significance. As a prime example of a FIMI campaign with the goal to interfere in an election, this case provided an ideal basis for subjecting the prototype of the DISARM v2.0 Observables Framework to a systematic inter-coder reliability test and reflect on the status quo of research on disinformation effects. Overall, the report shows the complexity and context-dependence of international manipulation activities and emphasizes the need for further methodological reflection.

Autor's note

The author wants to thank Andreas Block, Director of Communications at the Munich Security Conference (MSC), and his team for providing anonymized social media data for research purposes.

The author also thanks Veronika Solopova (TU Berlin), Aleksandra Atanasova (Reset Tech), and Guillaume Kuster (Check First) from Alliance4Europe's (A4E) Counter Disinformation Network (CDN) for their valuable input to this analysis.

Special thanks go to Saman Nazari from the ADAC.iO consortium partner A4E for providing access to the Meltwater app via the CDN and for facilitating contact with the community of analysts and OSINT investigators.

Furthermore, the author gratefully received a dataset from Saman Nazari (A4E) that underpins the additional case study on the 2025 Moldovan parliamentary elections included in this report; the dataset was collected by OSINT investigators from A4E, GLOBSEC, and Polisphere.

A heartfelt thank-you also goes to Klara Loser, student assistant at TU Dortmund University, who provided dedicated and energetic support for the research that led to this report.

Overview and approach

The aim of this report is to test the developments of work packages 1-3 of the Horizon Europe ADAC.iO project via a case study of cross-platform information manipulation. It reflects on the methodology and practical analysis conducted from a social science perspective.

This report covers two incidences of information manipulation in the context of high-profile political events. The largest part of the analysis focusses on manipulative narratives and inauthentic activities across social media platforms during the Munich Security Conference 2025 (MSC 2025). Additionally, the report features a case of coordinated foreign interference targeting the 2025 Moldovan parliamentary elections.

While the MSC 2025 case is based on a process that involved both original data gathering, cross-platform investigation, and the reduction of a large dataset kindly provided by the MSC Communications department, the additional minor part on the Moldovan election case is based on an already processed dataset provided by A4E. The inclusion of this second case lends itself particularly well to an assessment of the inter-coder reliability of the DISARM v2.0 Observables Framework prototype in the context of an exemplary case of Foreign Information Manipulation and Interference (FIMI). It also allows for a comparison between two different forms of information manipulation during two very different high-profile political events: federal elections and an international security conference. The analysis applies the current (early 2026) prototype of the updated DISARM v2.0 Observable Framework to categorize the findings and base their interpretation. Proceeding in the following steps, the report

- gives a short overview of the tools used in and the general analytical logic underlying this research,
- documents data gathering and reduction, highlighting the use of LLMs in data preparation and processing,

- analyses key narrative themes and suspicious online activities across platforms related to the MSC 2025,
- applies the DISARM v2.0 Observables Framework to the Moldovan election dataset to assess inter-coder reliability and reflect on the potential effects of such campaigns,
- concludes by reflecting on both cases and providing further research recommendations.

Tools and the analytical logic underlying this research

The *DISARM Framework*[42] is an open-source framework for documenting and analysing influence operations. It is operationalized in the *DISARM Navigator*, a web-based application to navigate, annotate and visualise manipulative behaviors. The prototype of the updated version of the Navigator (v2.0) distinguishes between directly observable and inferred aspects of an influence campaign, focusing on observable techniques to enhance analytical rigour.

With reference to the ADAC.iO report, "A Framework for Attribution of Information Influence Operations"[43], the investigation documented in this report and conducted in a university setting draws on *behavioural evidence*, based on aggregated posting activities and account metadata, and *contextual evidence*, including media content, narratives, and political contexts, from open sources, to describe patterns of cross-platform information manipulation.

Grounded in an ethics approval by the Ethics Committee of TU Dortmund University, this research mandate requires the careful handling of data and allows a *cui bono assessment* of coordinated influence activities, as well as the motives and actors inferred from the analysed material.

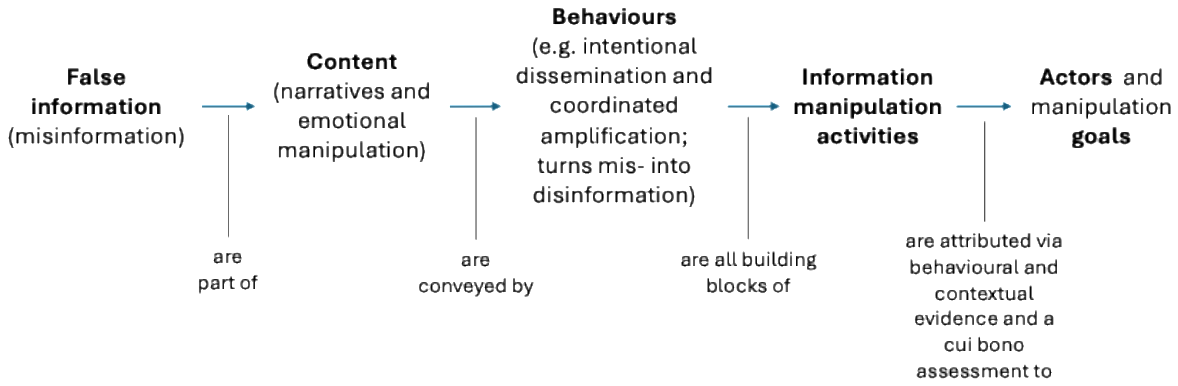


Figure 1: Conceptualization of the analytical process and scope of this report. The analysis takes into account both content and behaviours to identify information manipulation attempts. Behavioural and contextual evidence and a cui bono assessment are used to assess the involvement of certain actors and manipulation goals. Source: Own illustration.

Figure 1 highlights content and behaviours as building blocks of information manipulation, that is, the deliberate attempt to shift and shape public discourse by spreading false, biased, and emotionally manipulative content in a coordinated way. To discern the legitimate expression of political will by genuine individuals from illegitimate influence, content analysis must be accompanied by an analysis of behaviours and contextual aspects. Available signs of irregularities in online behaviour, including a clustering of account creation dates, temporal posting clusters, and other observable patterns such as similar account names or recurring

visual elements, can be read as observable indicators that a deliberate manipulation attempt might be observed. However, from an academic research perspective, these indicators must be interpreted with the utmost caution. To meet this requirement, the analysed data, where practically useful, are presented in aggregate form, highlighting overarching narrative and behavioural patterns. As this type of analysis requires OSINT research methods to identify communication and metadata patterns across networks, it necessarily draws on qualitative data, which may in certain cases allow inferences about individual accounts. To address this risk, all relevant material is reported in an anonymized form and in full compliance with the applicable ethics approval. This applies in particular to visual evidence and illustrative representations as well.

Main case: cross-platform manipulative in the context of the MSC 2025

Abstract

This analysis examines coordinated information manipulation targeting the Munich Security Conference 2025 (MSC 2025) through propaganda channels, social media posts, and email campaigns. It is based on a qualitative-quantitative cross-platform content analysis and an analysis of dissemination behaviours. The results demonstrate how ongoing information influence activities rapidly connect to current events, such as U.S. Vice President JD Vance's speech at the MSC 2025, to exploit critical diplomatic situations in pursuit of narrative dominance in online discourse, and how actors piggyback on broader geopolitical trends.

Case selection and objectives

While most investigations of information influence activities focus on high-profile (geo)political events, particularly national elections and contexts of warfare, this analysis focuses on an annual security event of global importance, that is, however, not among the most critical democratic events, such as Parliamentary or Presidential elections. The annual Munich Security Conference is widely recognized as the world's leading independent forum for international security policy. Its February meetings in Munich brings together heads of state and government, foreign and defence ministers, and heads of international organizations. In recent years, overall attendance has exceeded 700 participants, including heads of state and government from around the globe engaging in public debates and private meetings to discuss transatlantic strategies and international responses to emerging security crises[44]. The 61st MSC took place from February 14 to 16, 2025.

With this focus, this case study is able to demonstrate how an ecosystem of disinformation actors reacts to a security event that is closely followed by political observers and attentive public, and how disinformation narratives are contextually tailored to susceptible audiences across multiple platforms as the event is shaken by a political éclat. By showing how disinformation actors opportunistically exploited an evolving diplomatic crisis, this analysis addresses an important gap in practice-oriented information manipulation research.

Starting point for the case selection and data acquisition was the premise that the speech of U.S. Vice President Vance at the MSC 2025 would be exploited in information manipulation efforts. Vance's speech can be seen as the announcement and beginning of a broader

reorientation of U.S. foreign policy under the second Trump administration. This reorientation frames Europe as being in decline and European institutions as oppressive[45], thereby echoing familiar themes from Russian propaganda[46]. These positions have since been articulated more explicitly in the new U.S. National Security Strategy[47]. Against this background, the research question was as follows:

RQ: Which patterns of information manipulation narratives and behaviours exploiting the diplomatic éclat overshadowing the MSC 2025 can be identified across online platforms?

Goal: The objective of this case study is to identify narrative and behavioural patterns related to the MSC 2025 that target international audiences across social media platforms. Particular emphasis is placed on narratives directed against the EU. The sample comprises content and behavioural evidence drawn from online propaganda outlets, email campaigns, and various social media platforms, including X, Telegram, and Facebook. The dataset consists exclusively of publicly accessible posts.

Techniques from the DISARM v2.0 Observables Framework were used to tag key passages in this section of the report. An overview of the techniques applied is included in the appendix to this report (Appendix 1).

Data gathering, data reduction, and the use of LLMs in data preparation and processing

The data sources of this analysis are versatile. A search for themes and narratives across social media platforms was conducted via queries using the Meltwater app for social media monitoring, access to which was provided by ADAC.iO partner A4E via the CDN. As the conference took place from February 14 to 16, 2025, data gathering focused on but was not limited to the second half of February 2025. Starting with a very rudimentary query including the terms (“Munich” OR “Security Conference” OR “MSC*”) AND (“NATO” OR “EU*” OR “Ukrain*”) AND “Vance” in English, German, and Russian language, the first search attempt retrieved nearly 400k results for the relevant time period. In an iterative process, the search query was refined by incorporating additional keywords identified through the Debunk app, provided by ADAC.iO partner Debunk.org, as well as terms drawn from a supplementary list of recurring propaganda keywords developed by Solopova et al.[48]. This additional search focused on channels that are partly sanctioned by the EU, including rt.com, tass.com, eng.globalaffairs.ru, and others, as well as radical nationalist assets from international geographical contexts such as presstv.ir (an Iranian state-owned news media organisation) and Infowars.com (a U.S. far-right fake news website created by Alex Jones), publishing articles with headlines such as “Europe: a Spectre of Irrelevance” (eng.globalaffairs.ru), “Munich Security Conference chairman weeps over deepening division in NATO” (presstv.ir), “Vance blasts ‘Orwellian’ German laws” (rt.com), and “Musk calls Heusgen ‘pathetic’ for crying during closing speech at Munich Conference” (tass.com). This iterative procedure progressively narrowed the search output to approximately 1k substantively relevant results. The process of refining the final query structure was supported by ChatGPT 5.1. The final query used in the Meltwater app is attached in the appendix to this report (Appendix 2).

An additional dataset comprising 20,000 social media posts and associated metadata, primarily from X, which had been collected independently as part of monitoring activities accompanying

the event, was made available by the MSC communications department for the purposes of this research. This dataset was reduced to a workable subsample of 500 posts, including relevant account metadata in successive stages. The first step focused on content, applying predefined content-related criteria, such as recurring patterns of specific phrases, keyword clusters, and indicators of negative sentiment. Keywords from Solopova et al. and the Debunk app were incorporated at this stage as well. To manage the large volume of material in the 20,000 posts, this initial content-level screening was supported by ChatGPT 5.2. The second step focused on irregular patterns in the account metadata, including a suspicious clustering of account creation dates, arbitrary account names that may be interpreted as indicators of the creation of disposable accounts, and recurring visual elements such as generic profile and cover pictures, as well as potential signs of coordinated posting behaviour, such as temporal posting clusters. Furthermore, a collection of emails from the known Russian campaign Opera*tion Overload* was provided by *CheckFirst*, a Finnish software and methodologies company.

The integration of the different data sources and the subsequent data reduction process resulted in an initial dataset comprising 1,500 social media posts, by far the majority from X. To gain an initial overview of key narrative patterns in the remaining data, Google's Gemini 3 was used as an assisting tool to identify content patterns. Building on these results, the researcher conducted a qualitative analysis, assessing potential narrative clusters while also taking into account the accounts involved in disseminating the content and the associated posting behaviour (behavioural evidence). This was complemented by a qualitative OSINT investigation aimed at identifying related content on additional platforms that could be assigned to specific narrative clusters in order to expand and diversify the platforms included in the cross-platform analysis.

Throughout the entire process, data gathering and analysis went hand in hand, following an inductive-deductive approach and combining quantitative and qualitative elements. From a social science research perspective, this procedure is similar to *Grounded Theory* approaches[49].

Ethics statement

The Ethics Committee of TU Dortmund University has reviewed and approved this research project. From a methodological perspective, the data retrieval process does not constitute a separate data collection, but rather a gathering of publicly accessible posts based on a list of keywords derived from previous research findings on disinformation on the internet. The data collection through web scraping on the aforementioned platforms is supported by project partners A4E and Debunk.org who provided research infrastructure. For evaluation purposes, the collected posts were temporarily stored in the *Synology Cloud* of the Institute of Journalism at TU Dortmund University. Since this is an in-house cloud with encrypted partitions within the protected TU domain, the data was particularly secure against unauthorized access and other threats. It is important to emphasize that the analysis did not focus on individual political expressions by authentic users, but rather on identifying indicators of inauthentic accounts and coordinated behavior aimed at disseminating false or distorted information. In cases where the report includes content from individual accounts, which occurs only when there is reason to suspect that the accounts are inauthentic, the data are reported in anonymized form in order to protect the personal rights of the individuals concerned in the event of a misclassification. The

conclusion of the research project is followed by the deletion of the datasets.

Results

Quantitative assessment and dataset characteristics

U.S. Vice President JD Vance delivered his speech on the first day of the conference on 14 February, in which he claimed that it is not foreign threats but an internal erosion of democratic norms, such as the restriction of free speech, political censorship, and religious freedom, as well as "mass migration" that pose the greatest dangers to Europe[50,51]. Immediately following his speech, the posting activity on social media connected to the keyword "MSC 2025" spiked expectedly (Figures 2 and 3). An analysis of account metadata and other behavioural evidence from the datasets reveals that a noticeable share of the accounts active in the communication environment around the spike of online activity shows indicators of inauthenticity.

Figure 2: Global mentions trend across the overall population of social media posts related to MSC 2025, based on the query "Munich Security Conference" OR "MSC*" OR "Sicherheit*" OR "Мюнхенск* безопасн*" in English, German, and Russian on the platforms X, Reddit, and Facebook. Telegram data were not available. The data show a sharp spike in posts referring to MSC 2025 following Vance's speech on 14 February 2025. Source: Meltwater.

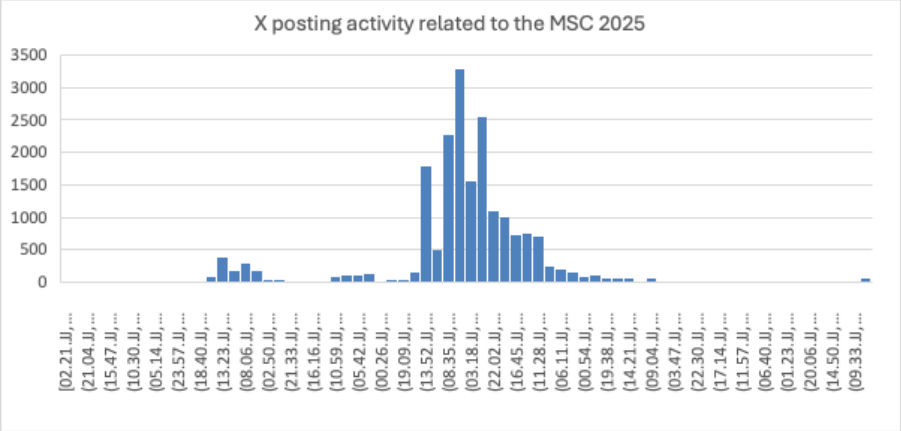


Figure 3: A quantitative assessment of the dataset of 20k social media posts with negative sentiment provided by the MSC Communications department reflects this spike in social media attention following Vance's speech.

The initial dataset includes several account creation date clusters in which 50 or more accounts that were active during the spike had been created within 48-hour time windows surrounding major political events in the past. The formation of three distinct clusters dates back to 2022, indicating a potential reactivation or reuse of existing structures of inauthentic account assets (Techniques as specified in the DISARM framework: T0146.000: Account Asset; T0149.000: Online Infrastructure; T0160.004: Asset Activated after Period of Dormancy; T0150.002: Dormant Asset). Example accounts from the three clusters from 2022 and explanations of the (geo-)political contexts of their formation are shown in Figure 3. These accounts in many instances have no or only very generic profile and cover pictures, generic profile names and handles, and solely engage in reposting. Many of these accounts amplified content from high-reach accounts such as *Fox News*, far-right activist Laura Loomer, Charlie Kirk, and *Libs of TikTok*, a username used by various anti-LGBTQ and far-right accounts across social media platforms[52] (T0157.000: Amplify Content; T0157.001: Repost Post). These accounts framed JD Vance's speech and other conference speeches, for example by Ursula von der Leyen, within right-wing narratives, depicting European political elites as "behaving like tyrants and control freaks"[53] and "a bunch of HYPOCRITES"[54]. These accounts also amplified quotes from Vance's speech, for example that "[T]he biggest threat to Europe isn't external – it's internal. A retreat from its own fundamental values, values shared with the U.S."[55]

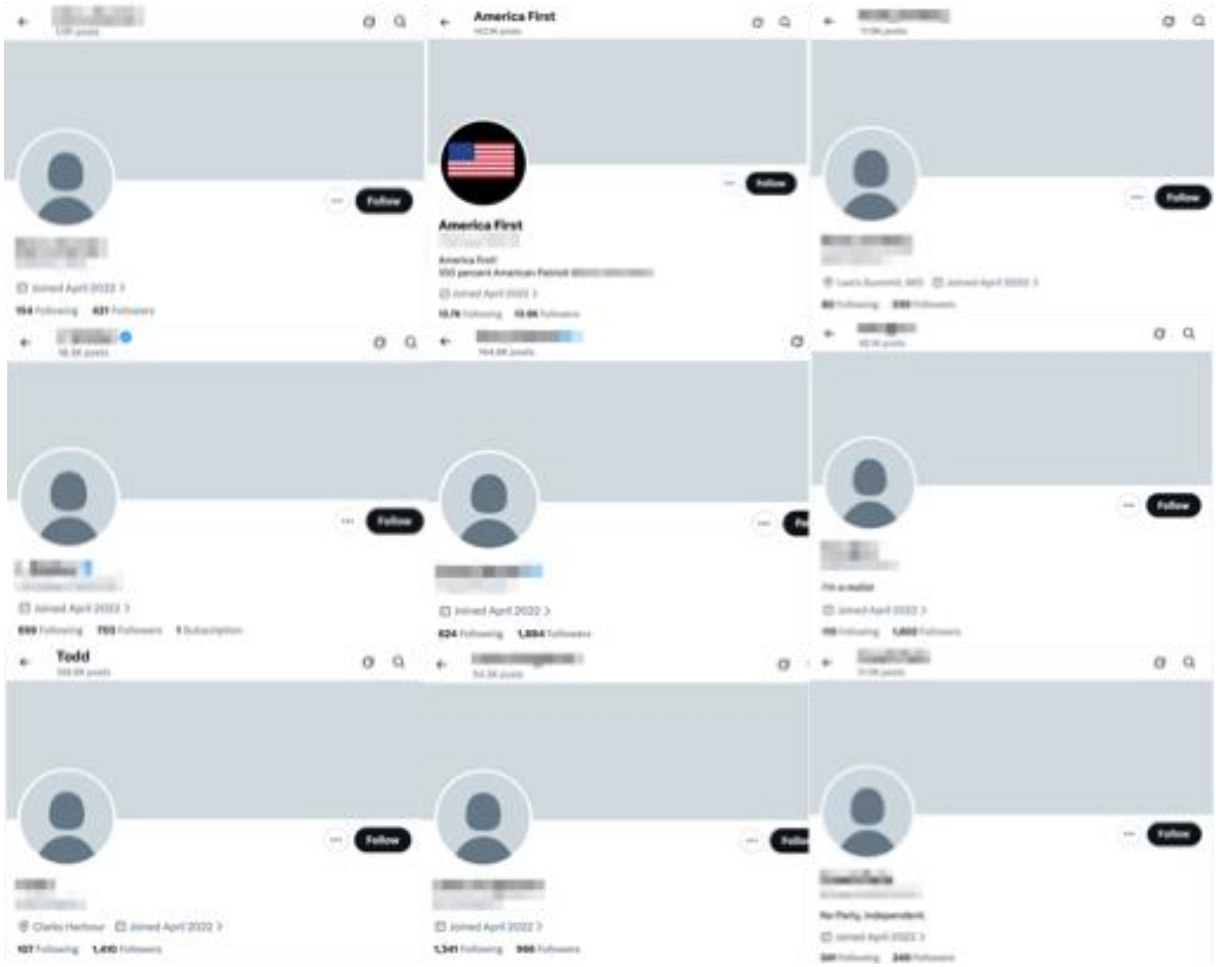
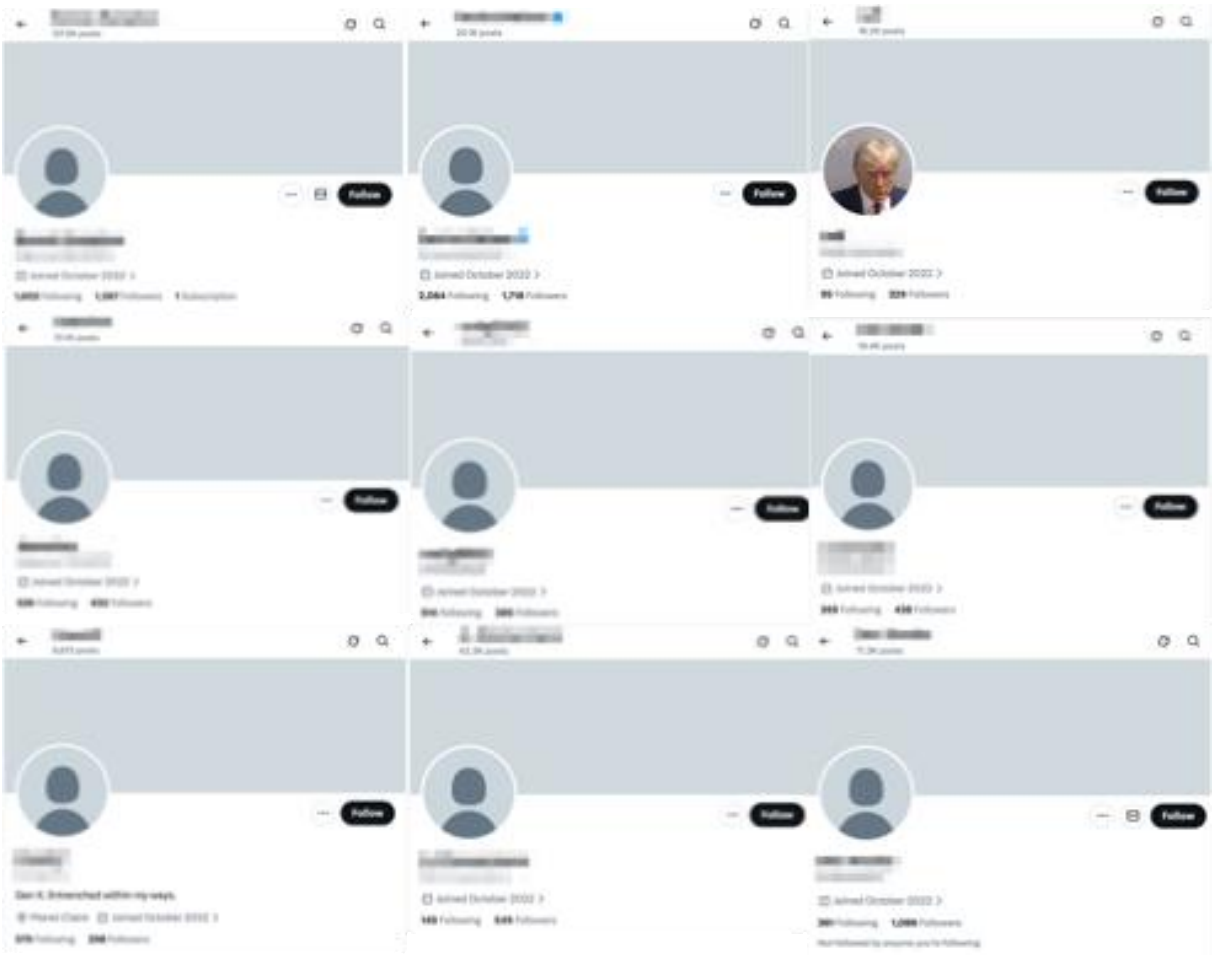


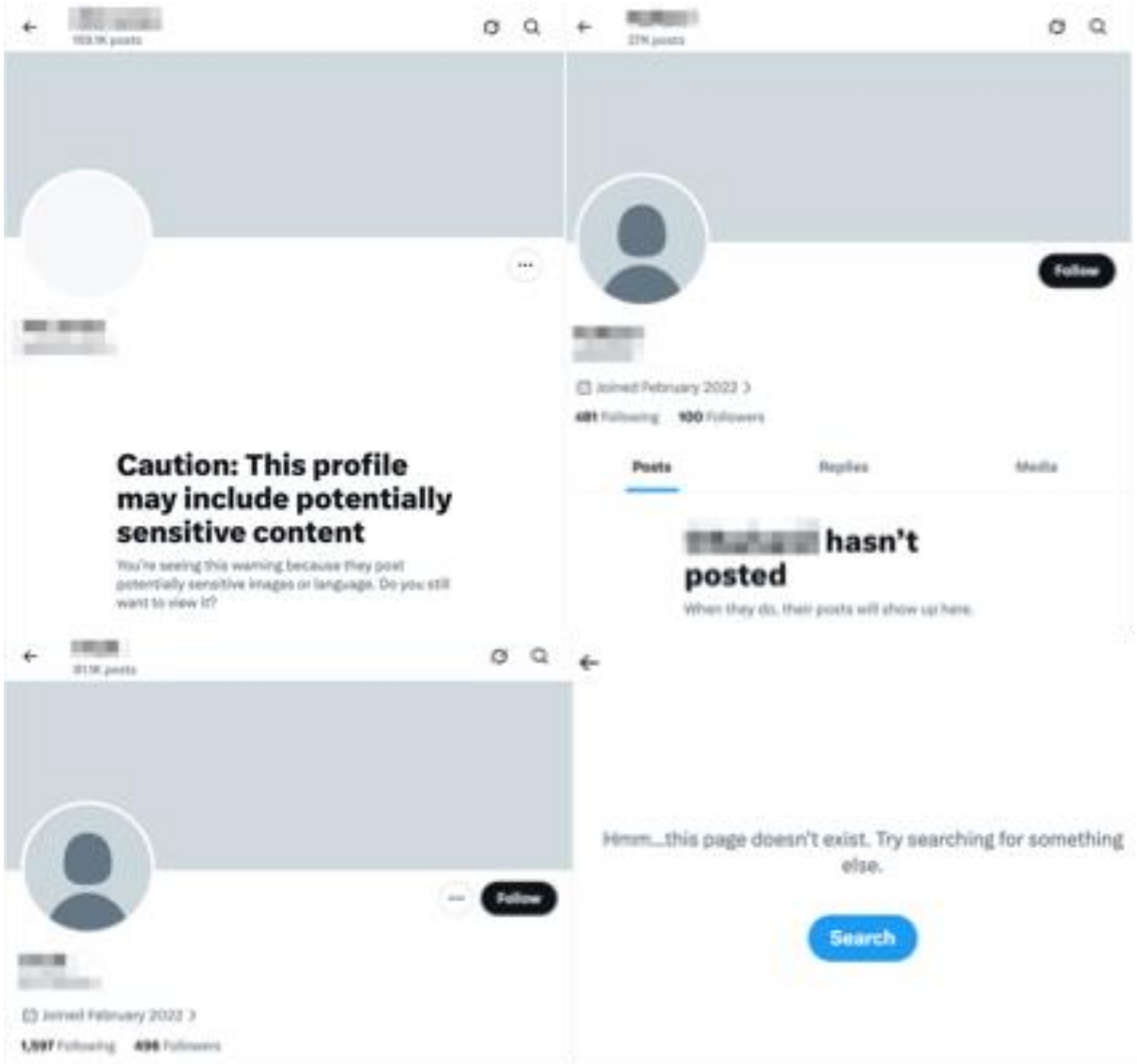
Figure 4: Example accounts from three account creation burst clusters from 2022. **4.1 – First cluster:** April 25-28, 2022. This account creation date cluster temporarily aligns with the second round of the French presidential election on April 24, 2022. The accounts in question often lack profile images and have generic alphanumeric handles with random strings of numbers (e.g. "Co***Pe34574243"[3]). Together with the creation date clustering and the spread of divisive content, the combination of these observables indicate that the accounts in question might be inauthentic accounts or even "bots"[56].

[3] "***" are inserted to protect online users in case the assessment that the accounts in question are inauthentic is unsubstantiated.



Oct 27–28, 2022

4.2 – Second cluster: October 27-30, 2022. A cluster of accounts with generic handles and no profile or cover pictures that were all created within 48 hours in 2022, accusing the EU of censorship and oppression (e.g. referring to EU political elites as „being petty tyrants and criminalizing freedom of speech“). This account creation date cluster coincides with the U.S. 2022 midterm election campaign (election day Nov 8, 2022). Again, many of these accounts have random alphanumeric handles (e.g. “Patr***56091091”, “Mus***371959931”) as an indicator of inauthentic creation ahead of the vote.



Feb 26–27, 2022

4.3 – Third cluster: February 26-27, 2022. These dates immediately follow Russia's full-scale invasion of Ukraine on Feb 24, 2022. The suspicious accounts from this period all have no profile photo and often include names with numbers or random strings (e.g. "sv***7"). A particular characteristic of this cluster is that at the time of this analysis, a significant proportion of the accounts that shared these messages had already been deactivated at the time of the analysis, which suggests that they might have been used as disposable or so-called "burner accounts", which are known to be set up for a specific manipulation purpose and oftentimes deleted afterwards to hinder analysis[57]. The creation dates could be traced based on the available metadata in the dataset.

Key narrative themes and inauthentic amplification activities across platforms

During the qualitative analysis of the data, three main narrative clusters emerged, which are labelled as (1) the "crying diplomat" narrative, (2) the "Soviet censorship regime" narrative, and (3) the "silencing of anti-establishment voices" narrative. These three narratives, together with the associated behavioural and contextual evidence, are examined in greater depth in the following sections.

(1) The "crying diplomat" narrative: "emasculation" and weak leadership framing

Many accounts from the creation date clusters amplified a decontextualized representation of former MSC chairman Christoph Heusgen's emotional reaction at the end of his farewell speech, which was wilfully misinterpreted as a direct response to Vance's speech. Although Heusgen did indeed shed tears during the conference's closing ceremony on Sunday, February 16, 2025, this occurred two days after Vance's speech on Friday, February 14. Thus, this narrative illustrates the contextual manipulation technique that is commonly found Foreign Information Manipulation and Interference (FIMI) operations, where real footage is recontextualized to support a false narrative[58] (T0168.007: Context Removed from Content; T0068.000: Respond to Breaking News Event or Active Crisis).

A noteworthy recurring framing in this regard is the "disgrace" of the so-called "castration" or "emasculation" of the EU or "the West", which is a recurring theme not only in far-right rhetoric but also in Russian propaganda[59]. The amplified posts linked this narrative to the alleged "weakness" of elites and political instability within the European Union. Heavily amplified posts on X also insinuate a connection between Heusgen's alleged breakdown and the car attack in the Munich city center in the run-up to the conference[60].

This false connection between alleged unsafety in Europe's public spaces and weak political leadership was further reinforced at the narrative level through a compiled video that incorporated footage from police operations and other security forces responding to unrelated security situations (Figure. 5) (T0178.005: Content Presented with False Context; T0170.003: Historic Content; T0178.006: Content Falsely Presented as Depicting Location). The video montage was shared art least 149 times on X, creating the misleading impression of ongoing terrorist attacks in Europe.

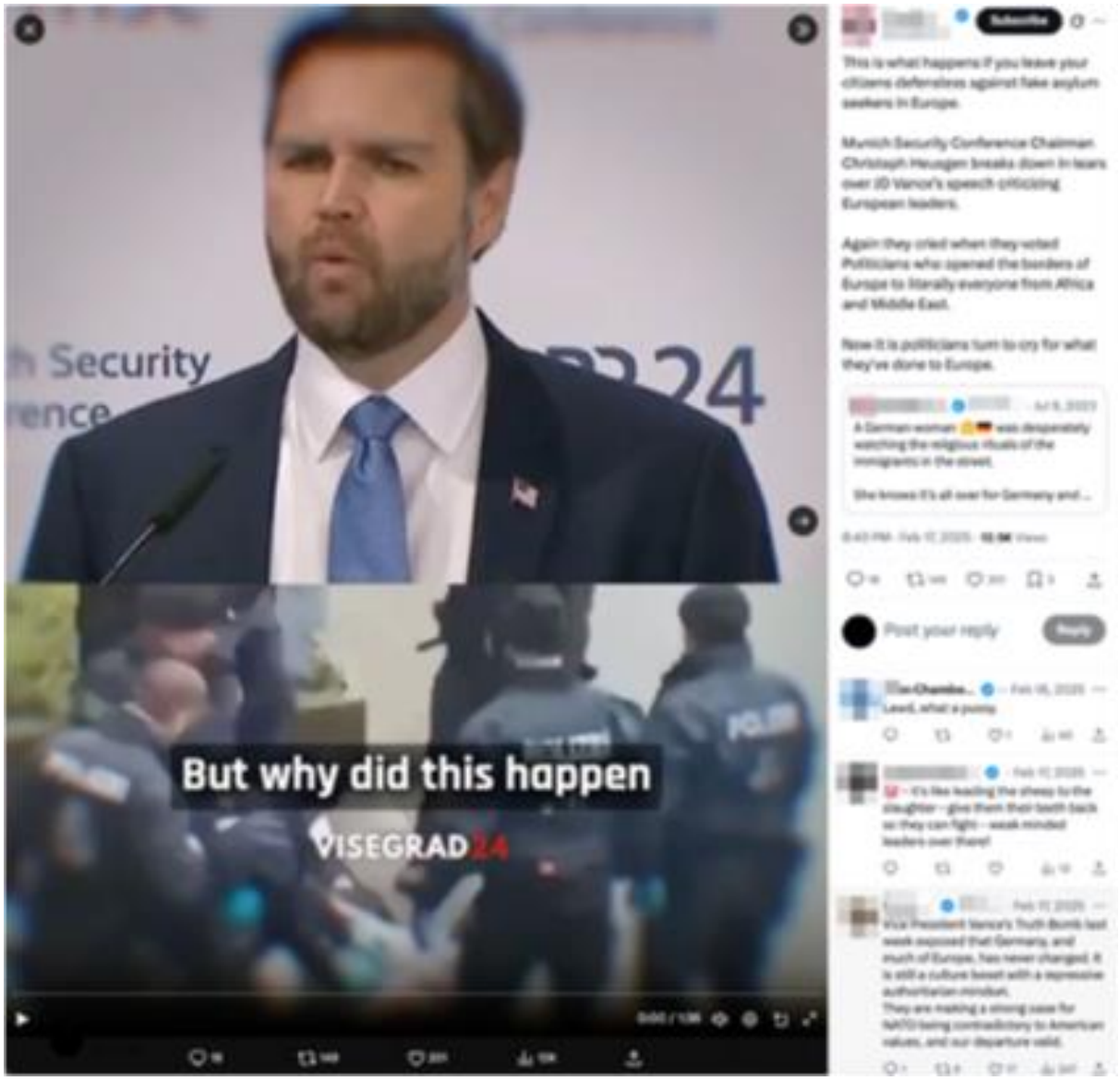


Figure 5: Heavily amplified video montage that fabricates a connection between the car attack in the run-up to the security conference and other terrorist attacks, Vance's speech, and Heusgen's emotional closing speech.

While identifying inauthentic accounts and activity is a balancing act as mentioned in the methodological part, account metadata and posting activities provides useful indicators for inauthentic activities going on in relation to the spread of the "Heusgen breakdown" narrative: On *X*, numerous accounts with arbitrary account names and random alphanumeric account handles reposted the same posts, in many cases uncommented, within minutes of each other between 23:40 and 23:56 on February 17, which might be read as a sign of a simulated grassroot reaction (T0159.003: Network Amplifies Post). Furthermore, a significant proportion of the accounts that shared these messages had already been deactivated at the time of the analysis, which suggests that they may have been used as disposable accounts. This is especially true for the February 2022 cluster that formed immediately after Russia's full-scale invasion of Ukraine, which was described above.

Numerous accounts engaged in the generic and uncommented reposting of a post by *The*

Gateway Pundit, an influential American far-right fake news website[61], linking to an online article framing the emotional reaction of Heusgen as "Munich Security Conference Chairman Goes on Stage and Cries Like a Baby After J. D. Vance Rocks His World" (Figure 6).

Interestingly, many of the accounts involved in this amplification display AI-generated profile and cover images that can be found repeatedly online. These images share a strong American nationalist iconography, featuring combinations of flags, bald eagles, and various stylized portraits of Donald Trump. Some of these images, particularly bald eagles, could be traced to stock photo websites via *Google Image Search*, where they are explicitly labelled as stock photos (T0145.002: AI-Generated Account Imagery; T0145.007: Stock Image Account Imagery). Some particularly striking examples are shown in Figure 7.

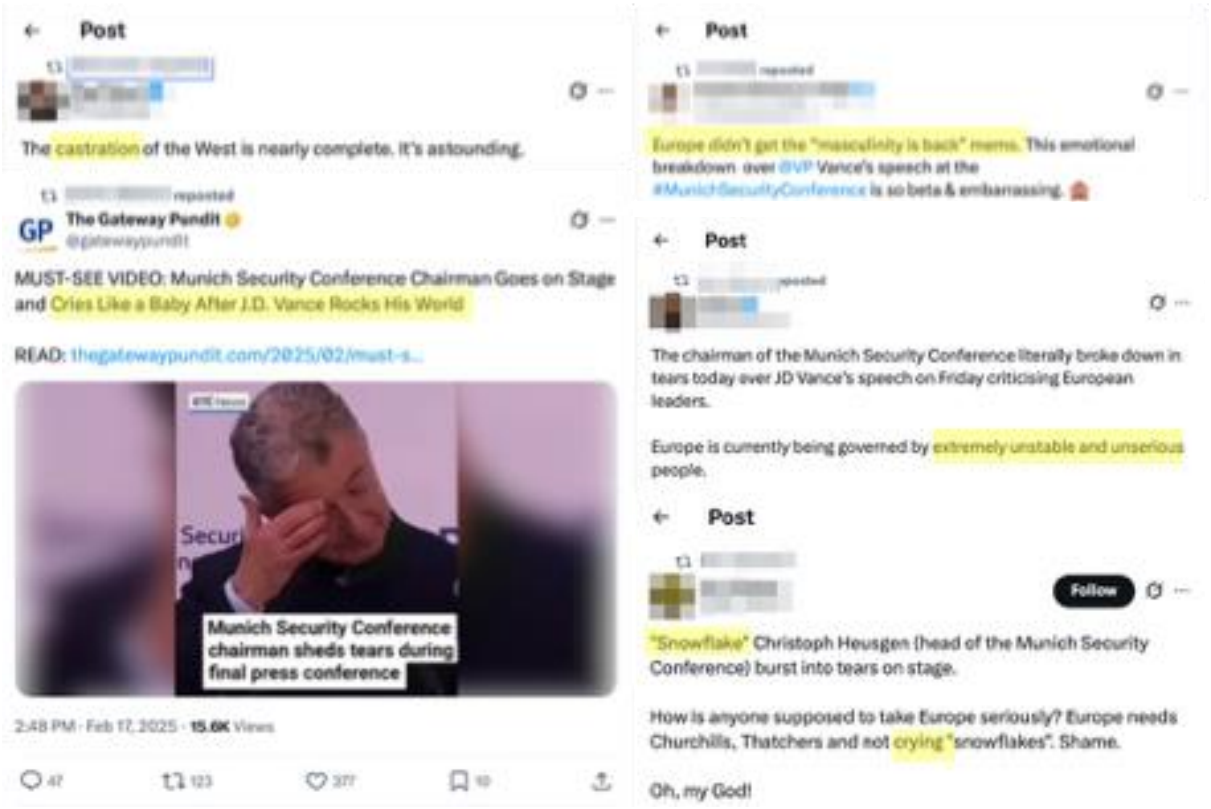


Figure 6: The decontextualization of Christoph Heusgen's speech and the exploitation of his emotional farewell on X. The posts draw on the "emasculation" rhetoric, which is a strong characteristic of far right and nationalist ideology[62] and authoritarian propaganda[63].

Figure 7: Profiles with stylized flags, eagles, and portraits of Donald Trump involved in the dissemination of the "crying chairman" narrative on X.

This narrative gained traction across several social media platforms. Heusgen's speech took place on the afternoon of February 16. With the rapid dissemination described above and the possible involvement of inauthentic accounts, X functioned both as a seeding ground and dissemination platform for the narrative. According to narrative similarities and a temporal assessment, Russian Telegram channels might have acted as repositories for the raw disinformation material: While the spike in activity on X happened after 23:40 CET on February 17, this was preceded by activity on Telegram. Russian Telegram disinformation accounts referenced in the Overload campaign, which are contained in the Overload emails dataset, spread the narrative of Heusgen's speech being a direct reaction to Vance's address and as an act of emasculation and weakness from early morning on February 17, for example at 08:03, 08:51, 08:54, 09:23, 16:44, and 22:12 CET. The similarity in narrative structure and the temporal sequence indicates that Telegram channels might have been used as a source for the narrative material that was later spread on X.

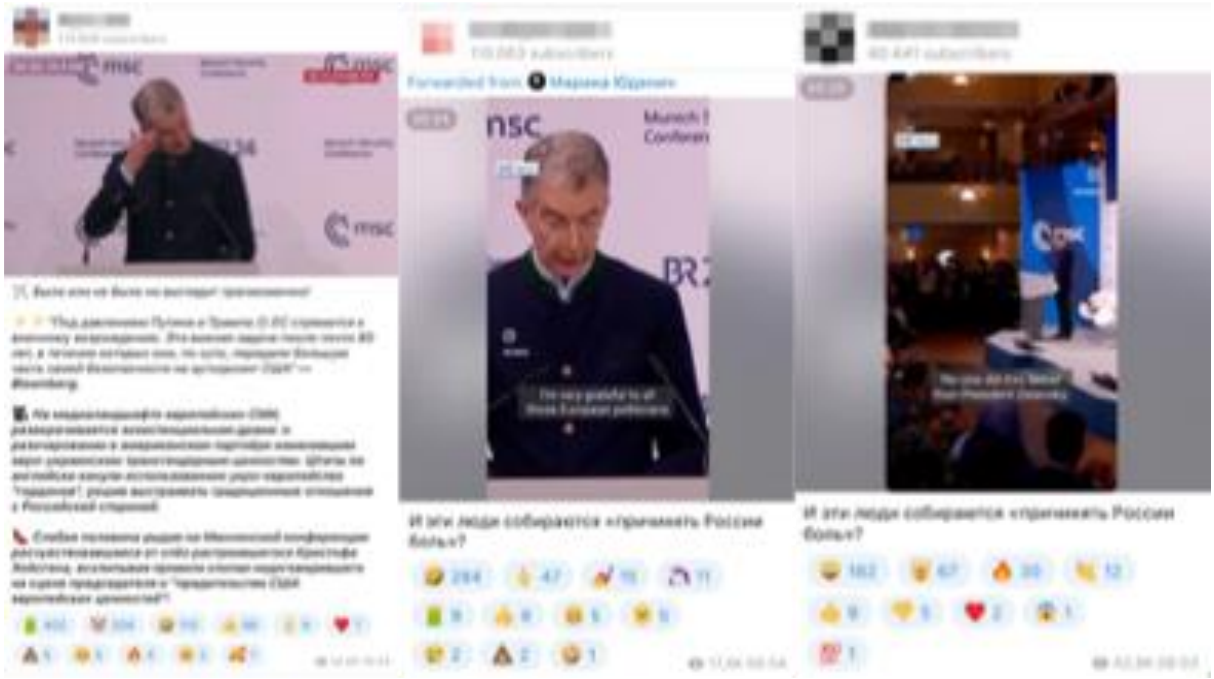


Figure 8: Posts on Russian disinformation channels on Telegram propagating the false narrative of Heusgen's emotional speech as a "breakdown" directly following U.S. Vice President Vance's address. These posts were posted right before the massive dissemination of similar narratives on X. **Translations**: left: *It may or may not have happened, but it looks tragicomic! / 'Under pressure from Putin and Trump (!), the EU is striving for a military revival. This important task comes after nearly 80 years during which they essentially outsourced most of their security to the United States.' Bloomberg. / Across the media landscape of European outlets, an existential drama is unfolding: disappointment in the American partner who has betrayed Euro-Ukrainian transgender values. The States, in plain English, dumped the used-up Ukro-Europeanism of the 'Gordons,' deciding instead to build traditional relations with the Russian side. / The weaker sex, weeping at the Munich Conference and moved to tears by the sobbing, upset Christoph Heusgen, sniffled and applauded as the chairman, cut off mid-speech on stage, spoke of the 'betrayal by the United States of European values'!"* Center and right: *"And these people are going to >>cause pain to Russia<<?"*(Translation assisted with Google translation plugin and ChatGPT 5.1.)

While it is inherently difficult to assess the degree and effects (the "D" and "E" in Pamment's ABCDE-Framework[64]) of such manipulation activities, the downstream effect of these activities could be observed in different Reddit threads, where genuine users fell into a discussion about the incident and its geopolitical implications. This shows that the distorted narrative that was spread about a direct connection between Vance's speech and Heusgen's farewell address led to organic replication across platform boundaries. Although the narrative was contextualized, it at least attracted attention and distorted the discourse. For example, threads in "r/europe"[65] and "r/de"[66] show users actively debating Vance's speech. While disinformation was reproduced in these contexts, the community structure often led to their debunking. However, the discussion often circled around geopolitics and subjective interpretations that are not easy to fact-check. Overall, this shows that the effects of disinformation narratives do not necessarily have to be persuasive in nature but may also consist in shifting the terms of the debate and concentrating discursive attention.

(2) The "Soviet censorship regime" narrative: instrumentalising the online debate

The findings further reveal a convergence of narratives between U.S.-linked activities in the information sphere, European nationalists, and state-sponsored Russian propaganda networks exploiting the "threat from within" narrative from Vance's speech[50]. As Vance's speech shifted the debate from military and security threats to a discussion about values, this provided ammunition for disinformation actors and fuelled narratives that cast doubt on the European Union as a legitimate actor. Allegations of censorship as proof of the EU's alleged double standards have since been echoed by official Russian channels[67].

Vance's comparison of the alleged suppression of freedom of expression in the EU with that in the Soviet Union[68] has triggered both organic and inauthentic amplification across platforms. One centrepiece was a Fox News article titled "Vance eviscerates 'Soviet'-style European censorship in address to Munich Security Conference", which was rapidly spread on X by a noticeable number of accounts from the dataset, several of which exhibit characteristics of inauthentic accounts (T0159.003: Network Amplifies Post; T0170.005: Content Produced by Third Party). In the wider ecosystem, channels amplified similar narratives from *The Gateway Pundit* (Figure 9).

This characterisation of the EU as a dictatorship and its equation with the Soviet Union is a well-known trope in both Russian state-aligned propaganda[69] and far-right conspiracy channels. The same trope drawing parallels between the Soviet Union and the EU was also invoked by European nationalists Marine Le Pen, who characterized the EU with its regulatory framework as the "European Soviet Union"[70], Viktor Orbán, who compared Hungary's EU membership to Soviet occupation and refers to Brussels as a "bad contemporary parody" of Moscow[71], and a regional AfD account using the acronym "EUSSR", a combination of EU and UDSSR, to frame the Digital Services Act as a tool to silence EU-critical voices[72] in the course of 2025.

Interestingly, the clusters of potentially inauthentic accounts also amplified content from accounts that disparaged political voices who criticised Vance for his speech. One post called out former Prime Minister of Sweden and now chairman of the *Middle East Investment Initiative*, Carl Bildt, for criticising Vance's speech as an interference in the upcoming German

elections in favour of the far-right AfD. The disparaging post referring to this statement directly addressed Elon Musk, then chairman of the so-called *DOGE* commission, stating that the Middle East Investment Initiative was receiving money from USAID and that it would be appropriate to cancel this funding[73] (T0179.001: Content Threatens Action). The post was amplified around 100 times within a few hours, with accounts from the creation-date clusters reported above among those contributing to its dissemination (T0159.003: Network Amplifies Post).

Along the same lines, posts on X and particularly Telegram highlighted that there were "reasonable" political voices in Europe supportive (or at least not dismissive) of Vance's speech, such as Nigel Farage, leader of Reform UK, who "has applauded JD Vance's remarks"[74], or Karin Keller-Sutter, President of the Swiss Confederation, who, referring to one of her speeches, allegedly claimed that "J. D. Vance spoke of nothing more than freedom of speech and direct democracy" (Google-translation of the originally Russian post)[75], were amplified. This suggests attempts to distort the perception of the discourse in favour of Eurosceptic voices.

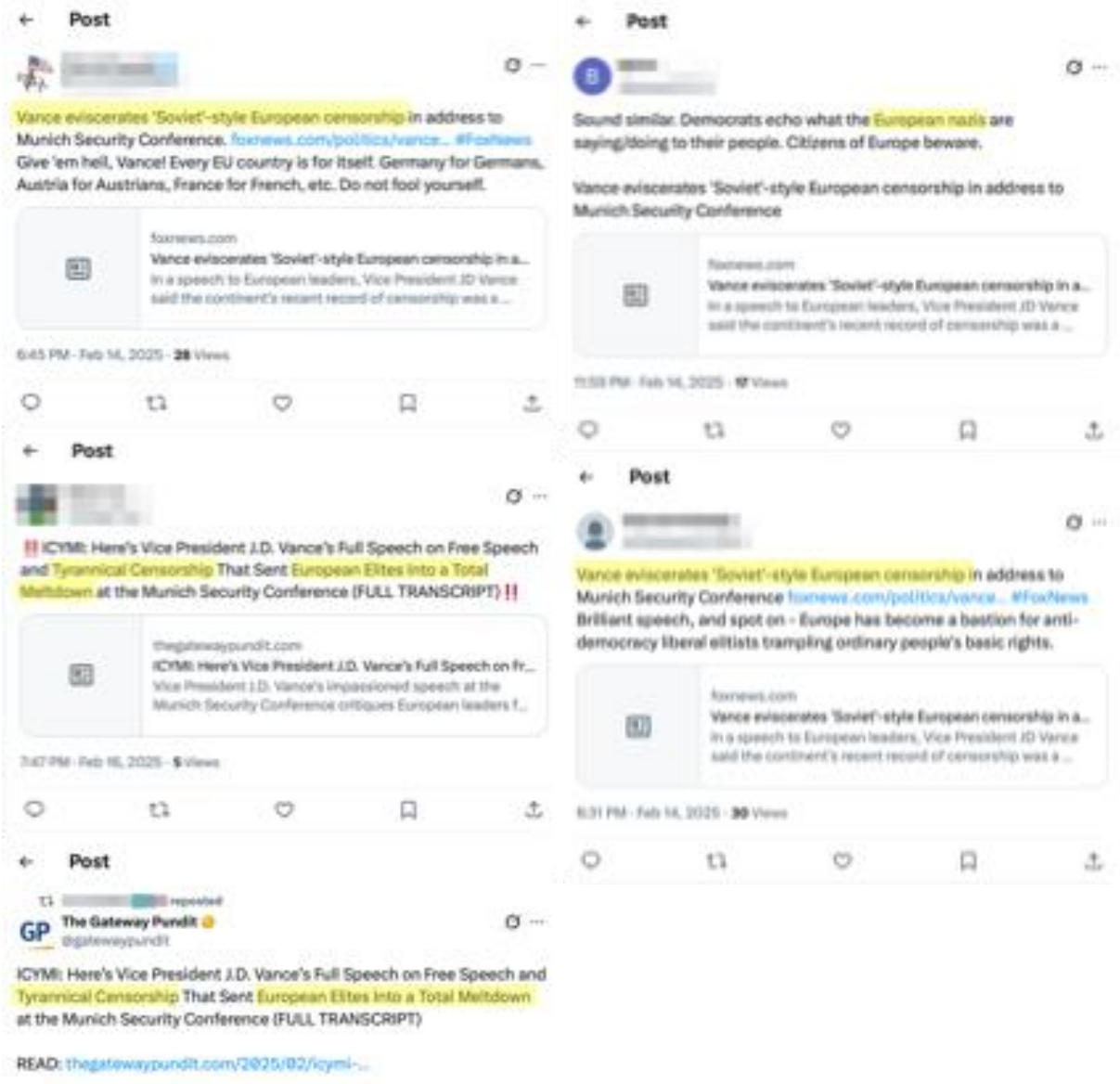


Figure 9: Example posts from the spread of Fox New's "Soviet-style censorship" narrative on X and a similar framing from other amplified far-right channels. Behavioural evidence suggests that the amplification on X was partly organic and partly coordinated.

An additional investigation showed that the very same rhetoric of "dictatorial" censorship in the EU was used to spread a variety of related narratives. Notable *Telegram* posts, including from Oleg Tsaryov and Alexander Dugin, who are both on EU sanctions list, proclaimed the collapse of the collective West and to portray the crackdown on Russian propaganda as a pretext for the suppression of freedom of speech in the European Union (Figure 10).

Further posts spread by Russian disinformation channels on Telegram picked up on Vance's false claim that the annulment of the presidential election process in Romania was a move by established elites to suppress political opposition, rather than a measure taken against sophisticated foreign interference and influence operations, as was actually the case[76] (Figure 9).

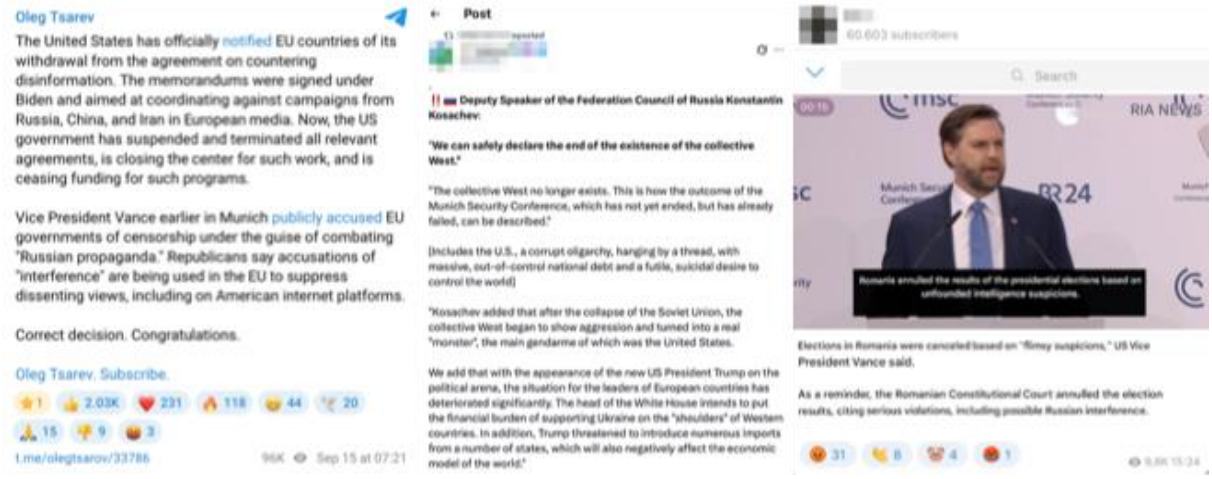


Figure 10: Various disinformation narratives that tie in with aspects from Vance's speech across Telegram: The EU is using its measures against Russian propaganda as a pretext to suppress freedom of expression, the outcome of MSC 2025 marks the clear end of the Western alliance, and Romanian/EU elites annulled the Romanian presidential elections to suppress the opposition. (Original Russian translated to English via the Google translator extension.)

(3) The "silencing of anti-establishment voices" narrative: Global exploitation

Vance's framing of the EU as a censorship regime created a convenient hook for disparate political groups to hang their specific grievances upon. The data shows a convergence of unrelated actors utilizing the #MSC2025 hashtag to amplify their own causes under the umbrella of "free speech." Similar phenomena are discussed as following "hijacking logics" in the literature, describing how actors piggyback on global trends and events to advance their own (local) agenda[77]. In this regard, an unexpected finding in the data is the significant activity of accounts supporting secessionist movements in Africa. Two central accounts were "Amba News Line" (@amba_newsline) and "Biafra Liaison Malaysia" (@BiafraLiaisonMY).

A 2025 report by African Digital Democracy Observatory (ADDO) identifies "Amba News Line" as one of the X accounts "flagged for promoting the activities of Ambazonia separatists"[78]. "Ambazonia" refers to a secessionist movement in Cameroon with the aim to transform the Englich-speaking regions in Cameroon into an independent nation of the same

name, Ambazonia, due to an alleged marginalisation by the Francophone-dominated government[79]. "Biafra" refers to an historic attempt to secede an independent Biafra republic from Nigeria. Both areas in question lie along the Cameroon-Nigeria border and share a common boundary. Secessionist efforts continue to this day and include acts of violence[80]. Leaders of both separatist movements face legal consequences. In the case of Biafra, Simon Ekpa was convicted of terrorism and sentenced to six years in prison by a Finnish court in September 2025, and his predecessor, Nnamdi Kanu, was arrested by Interpol in Kenya and extradited to Nigeria[81]. In the case of Ambazonia, Cho Ayaba, a separatist leader operating from Europe, was arrested by Norwegian authorities in September 2024 on the suspicion of the incitement to crimes against humanity[82].

Both accounts, "Amba News Line" and "Biafra Liaison Malaysia" retweeted the exact same wording of: "President Trump Says 'Free Speech in Retreat' Across Europe" in posts immediately responding Vance's speech, followed by narratives tailoring Vance's talking points to their specific local conflicts. Both condemn the prosecution of the leaders of both movements, Simon Ekpa and Cho Ayaba, in their respective posts and frame these cases as oppression of freedom of expression in Europe. "Biafra Liaison Malaysia" also refers to the case of Nnamdi Kanu and condemns the British government for not intervening (Figure 11). Based on the known facts about the cases mentioned above, these are clearly disinformation narratives. Such efforts by Africa-based secessionist movements, particularly Ambazonia and Biafra, to deploy propaganda aimed at global audiences in order to mobilize international support are not new; indeed, social media has become an increasingly central tool for disseminating disinformation narratives in pursuit of these local causes[83] (T0169.002: Produce Localised Content).

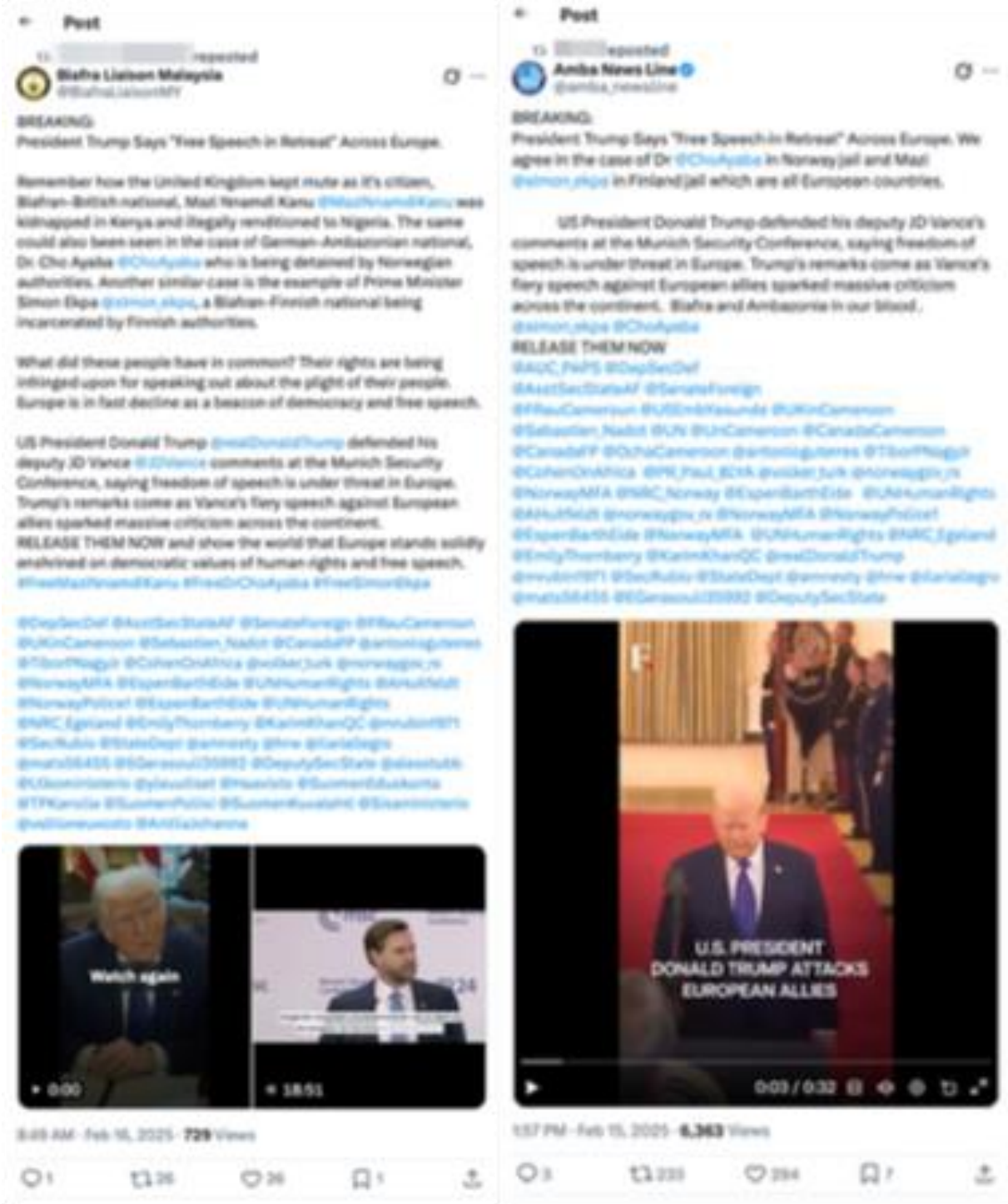


Figure 11 shows the two original posts of "Amba News Line" and "Biafra Liaison Malaysia" as posted and amplified on **X**.

Among the manipulation techniques employed by "Amba News Line" are the production of localised content to disseminate their narratives, as well as the replication of narratives fragments ("copypasta") of narratives, accompanied by clear indicators of inauthentic amplification[78] (T0157: Amplify Content). @amba_newsline posted at around 13:58 CET in the early afternoon of Feb 15, 2025. The post's content was "BREAKING: President Trump Says 'Free Speech in Retreat' Across Europe…". @BiafraLiaisonMY posted at around 08:50 CET in the morning of Feb 16, 2025. This post carried a similar headline about "Free Speech

in Retreat Across Europe,". The posting times were derived from the posts' IDs included in the dataset. The @amba_newsline post was reposted 228 times, the @BiafraLiaisonMY post 26 times. The first repost of both posts appeared almost immediately, within minutes on Feb 15. There are several indications of coordinated amplification in the reposting activity. First, there are several periods where multiple accounts reposted in quick succession, with 5 to 6 accounts reposting the original posts within 5-minute time windows, in some cases at the exact same minute or even at the exact same second, per timestamp, which is rather unlikely for coincidental behaviour.

Second, there is an overlap in the accounts promoting both posts of at least 9 accounts, which could hint at a common operator behind a network of accounts. Third, a closer look at other metadata shows that a large proportion of accounts is very new (some being only a few weeks old) and have minimal follower numbers. Combined with generic account handles, and the inclusion of politicised labels such as "ambafree", "ambaknights" in account handles, and combinations of "biafra" and random letter-number combinations, this is a relatively strong sign of inauthentic accounts**Error! Bookmark not defined.** created for the purpose of amplifying social media posts related to the Ambazonia and Biafra cause (T0159.003: Network Amplifies Post). This assessment is also supported by the fact that a significant proportion of the amplifier accounts had already been deleted at the time of this analysis. Whether these presumably inauthentic accounts were bots or human controlled accounts is not clear.

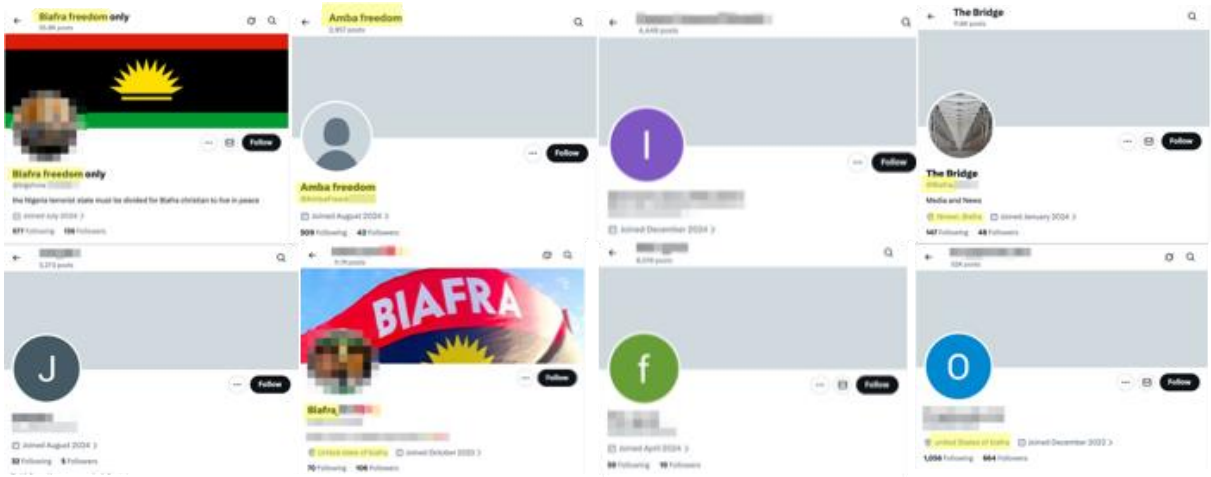


Figure 12: A sample of suspicious accounts that amplified the two original posts of@amba_newsline and @BiafraLiaisonMY on X. Account imagery, account names, and locations (marked yellow) as well as creation dates (almost all from 2024) strongly indicate the purposeful creation of accounts for coordinated amplification activities.

Coinciding with these activities, multiple instances of Russian propaganda and Russia-related disinformation narratives were observed specifically targeting relations between the EU and African nations between 14 and 28 February 2025, falling in the exact time of social media firestorm in the aftermath of Vance's MSC 2025 speech. A common tactic of Russian propaganda in Africa is to invoke Europe's colonial past and its continuing exploitation of African nations, and to present Russia as a moral counterweight to the EU, effectively camouflaging its own neo-imperial agenda[84]. Technically, Russia often launders its disinformation through African intermediaries to make its propaganda more organic[85].

Russian propaganda also intersected with the separatist movements Ambazonia in Cameroon and Biafra in Nigeria. In this regard, pro-secessionist and pro-Russian narratives, for instance, that European countries continue to oppress the African people while Russia promotes freedom in Africa and therefore supports Biafra and Ambazonia, are part of a larger and ongoing campaign targeting African and global audiences: The portal "BaretaNews", a pro-separatist website active on several platforms[86], praises Vladimir Putin and the Russian Federation for their "support" and "their push against neocolonial influence" of Europe[87]. The same narratives are spread by pro-separatist sites on Facebook, which functions as a central platform leveraged for the massive distribution of inflammatory and pro-Russian content via fake news sites in Africa[88,89]. The Facebook channel "Africa News Line 700," a social media–based outlet with more than 700,000 followers on Facebook, consistently promotes the separatist movements of Biafra and Ambazonia and portrays Russia as a moral supporter.

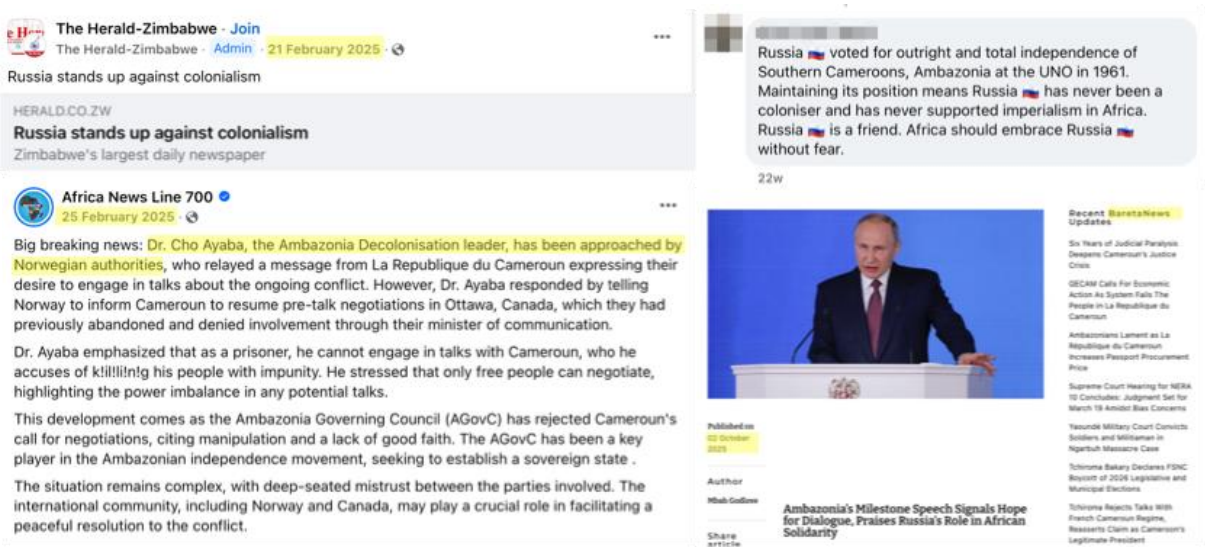


Figure 13: Continued amplification of Biafra and Ambazonia narratives around the 2025 MSC and throughout 2025 (and still continuing). A Google search using the "site:" and "before:" and "after:" parameters reveals a recurring condemnation of European activities and praise for Russia across time, Facebook pages, and websites: (The following search string was used for research: "*African nations must now rise to protect their shared interests by supporting the decolonisation of Ambazonia and the liberation of biafra". site:facebook.com before:2025-03-1 after:2025-02-14*)

A final noticeable pattern is the alignment between Biafra-related accounts and MAGA movement communications in a time-synchronised way during to the MSC 2025. The posting behaviour of Biafra-related accounts suggests that the movement is seeking to position itself narratively closer to the MAGA movement. This becomes visible through frequent reposts of prominent MAGA figures, including Donald Trump, Elon Musk, and Charlie Kirk. Several accounts promote narratives that resonate with the MAGA agenda, most notably the allegation that the militant jihadist group Boko Haram was funded through USAID under the Obama and Biden administrations (Figure 14). In the context of this case study, however, these dynamics are of limited relevance, as they display no concrete reference to the MSC 2025.

Figure 14: Biafra-related accounts (bottom row pictures) reposting MAGA-related content (top row pictures) on X. The cover image of the account in the bottom-left shows Biafra leader Simon Ekpa, convicted of terrorism and sentenced to six years in prison by a Finnish court in September 2025. The cover image of the account in the bottom-right shows the flag of Biafra, a symbol for the Biafran people and the separatist movement seeking an independent state from Nigeria.

Comparative case: the 2025 Moldovan parliamentary elections

Author's note on the additional case

This section of the analysis is based on a dataset kindly provided by Saman Nazari from A4E. The dataset was collected by OSINT investigators from the A4E, GLOBSEC, and Polisphere. Their report is available at alliance4europe.eu[90].

This additional case represents a strong case of a cross-platform campaign interfering with the 2025 Moldovan parliamentary elections. The case was reanalysed with the prototype of the DISARM v2.0 Observables Framework for this report. This allows a qualitative assessment of the usability of the prototype. Such assessments are crucial to advance the interoperability of the FIMI defender community. More generally, replication studies testing new or advanced tools add great value to the assessment of results and research methods[91].

Moreover, the inclusion of this second case allows for a comparison between different phenotypes of information manipulation during two very different types of high-profile political events, international security conferences and national elections. As it is already known that manipulation activities targeting similar types of events such as elections often follow similar patterns, selecting and comparing cases with greater variation adds valuable from the perspective of social science case study methodology[92].

Brief case introduction

This case summary and the subsequent short report for tagging purposes is based on the provided dataset and additional information from the original report referenced above[90]. This was complemented by a recent verification of whether the campaign infrastructure that had been flagged to the respective platforms shortly after the election still remains accessible.

Even though Moldova is a small country in territory and population with around 2,4 million inhabitants, it constitutes a key case for studying Foreign Information Manipulation and Interference (FIMI) in electoral contexts from a European perspective, given its position between pro-European and pro-Russian political orientations. In the past, Moldova has repeatedly served as a testing ground for Russian information manipulation activities[93].

The 2025 Moldovan parliamentary elections witnessed sophisticated multi-platform information manipulation[94]. The particular activity reported here aimed at mobilizing paid street demonstrations against Moldova's pro-European government during the election period to destabilize pro-European governance. Even though the turnout was small compared to the resources invested, the campaign presents a valuable case of how online information manipulation is employed to incite offline activities.

The following analysis applies the prototype of the DISARM Observables Framework v2.0 for categorizing manipulation behaviours. The report was written in a condensed form based on the dataset provided by A4E. The following table (Table 1) present the identical report tagged by two independent coders to assess the inter-coder-reliability of the framework. In ambiguous cases, coders were allowed to assign multiple techniques from the DISARM framework to the same text passages. In these cases, the presence of any overlap was counted as agreement, even if the other assigned techniques did not match, which increased the potential for coder

agreement slightly. The pale numbers in brackets are nominal representations of the techniques that were used to calculate Cohen's Kappa. The table is accompanied by a list of techniques from the prototype of the DISARM Observables Framework used by the coders in their coding processes to assign the techniques' alphanumeric codes in the Coders' columns to the corresponding technique labels.

The tagged summaries are followed by a contextualisation of the value of Cohen's Kappa and a brief tagging assessment. The section concludes with a brief assessment of the influence operations' effectiveness in manipulating election outcomes from a communication research perspective.

DISARM v2.0 Observables Framework prototype two-coder tagging

Text	Coder 1	Coder 2	Agreement
The 2025 parliamentary elections in Moldova were targeted by a campaign designed to incite people, through coordinated activities, to participate in an organized anti-government protest (1). The main campaign activity took place between August 11-16, 2025, and can be linked with high confidence to sanctioned oligarch Ilan Shor, exiled in Russia. Central to the operation was a Telegram bot, "MD Live Check 897," (2) used to register protest participants (3). Shor disseminated explicit video calls (4) on VK, Telegram, and Odnoklassniki, directing supporters to the bot (5). The operation relied on coordinated inauthentic behavior across six platforms: Telegram, Instagram, TikTok, Facebook, YouTube, and Odnoklassniki. Inauthentic accounts (6) spammed identical messages into 64 largely apolitical Odnoklassniki groups (7) and 23 inauthentic Telegram channels (8) named after Moldovan municipalities. These channels posed as local news outlets (9) to enable geographic micro-targeting. The sanctioned Gagauznews network, controlled by Shor associates[95], played a key role in amplifying of the video material and the Telegram bot. Videos promoted financial inducements of $3,000 per month, framed as compensation for lost wages rather than direct payment, obscuring the transactional intent (10). The bot collected sensitive data, including passport images, facial photos, phone numbers, and live geolocation (11), and assigned registrants tasks such as coordinated social media posting (12),			NO
	1 – T0057.000/T0057.003 (11)	1 – T0179.002 (20)	NO
	2 – T0146.007 (2)	2 – T0150.003/T0151.004 (3)	NO
			YES
	3 – 10T0057.004 (10)	3 – T0179.007 (19)	YES
	4 – 16T0173.000 (16)	4 – T0173.000 (16)	
	5 – 8T0119.002/T0179.002 (8)	5 – T0119.002 (8)	
	6 – T0143.002/T0150.008 (4)	6 – T0143.002 (4)	YES
	7 – T0119.001 (7)	7 – T0159.003 (9)	NO
	8 – T0157.000/T0119.002 (6)	8 – T0143.002/ T0159.003 (4)	NO
	9 - T0097.101/ T0097.202 (5)	9 – T0097.101 (5)	YES
	10 – T12T0057.001/T0162.002 (12)	10 – T0148 (1)	NO
	11 – T0167.001 (14)	11 – T0167.001 (14)	YES
	12 – T0179.004 (18)	12 – T0179.004 (18)	YES
	13 – T0169.002 (15)	13 – T0178.005 (17)	NO

effectively converting them into active influence agents. Narratives portrayed the pro-European government as repressing the population and blamed economic decline on European integration, while presenting Russia as a preferable partner. These narratives were injected into non-political online communities in Romanian and Russian, targeting older, rural users and the diaspora (13). Immediate platform responses were minimal, with no action taken by Telegram[90]. As of January 2026, despite having been flagged, some assets from the inauthentic network and the disseminated video remain available across social media, particularly on Telegram[4] (14).	14 – T0165.001 (13)	14 – T0165.001 (13)	YES

Table 1: Inter-coder reliability assessment of the DISARM v2.0 Observables Framework prototype. **Techniques coded by the coders**: T0057.000: Organise Events; T0057.003: Physical Gathering; T0146.007: Automated Account Asset; T0057.004: Facilitate Attendance; T0173.000: Video Content; T0119.002: Post across Platform; T0143.002: Fabricated Persona; T0119.001: Post across Groups; T0157.000: Amplify Content; T0119.002: Post across Platform; T0159.001: Concurrent Networked Action; T0097.101: Local Persona; T0057.001: Pay for Physical Action; T0162.002: Initiate Subscription Payment; T0167.001: Personally Identifiable Information; T0179.004: Content Contains Instructions for Action; T0169.002: Produce Localised Content; T0165.001: Asset Remains Active after Reporting Breach of Platform Policy to Platform; T0179.002: Content Encourages Action; T0150.003: Pre-Existing Asset; T0151.004: Chat Platform; T0151.001: Social Media Platform; 19T0179.007: Content Directs Off Platform; T0159.003: Network Amplifies Post; 4T0143.002: Fabricated Persona; T0159.003: Network Amplifies Post; T0148: Financial Instrument; T0178.005: Content Presented with False Context.

[4] In greater detail: As of January 2026, the video is no longer available on YouTube, Instagram, and TikTok. One instance of the video remains on Facebook, and all links to the video on Telegram are still functional. While banned from YouTube, Gagauznews and some other flagged channels remain accessible on Instagram. The same holds for some of the accounts on Facebook. All reported accounts are banned from TikTok.

Tagging assessment

Conducting an inter-coder reliability test provides a scientifically grounded assessment of the reliability of the DISARM Observables Framework by examining the extent to which different analysts assign the same codes when coding identical material. Assessing interoperability is crucial in this context, as an above-chance level of inter-coder agreement in the application of the framework is essential, given its role as a central tool for influence operations analysts.

The case summary was tagged by two coders independently to assess coder agreement. In preparation, the first coder identified and marked 14 text passages in the document, which were then coded by both coders independently. The coders were allowed to assign multiple techniques (codes) from the Framework to one text passage, which is common practice in many analyses that apply the DISARM Framework. If at least one code from each of the coding procedure matched, that overlap was counted as agreement.

The first coder, the author of this report, is moderately experienced in using the DISARM Framework and participated in a DISARM Certificate course in the past. The second coder had no prior experience in using the Framework. She was given a brief introduction to the logic and functionality of the Framework prior to coding. This means that this test is based on the premise that the Framework is designed to enable new groups of analysts to learn how to apply the taxonomy relatively quickly. Inter-coder reliability was measured with Cohen's Kappa, a standard measure in qualitative social science research. Cohen's Kappa was calculated manually using Microsoft Excel. The corresponding Excel sheet is included in the appendix to this report (Appendix 3).

Cohen's Kappa was K=0.48, which indicated moderate coder agreement (for reference: <0 (poor), 0.01–0.20 (slight), 0.21–0.40 (fair), 0.41–0.60 (moderate), 0.61–0.80 (substantial), and 0.81–1.00 (almost perfect)[xcvi]). Since the revision of the DISARM framework is still a work in progress, this result must be interpreted with caution. At the same time, it provides useful insights for the further development process. The revision process of the DISARM Framework is shaped by the need to accommodate different user groups. On the one hand, the framework must be sufficiently comprehensive to cover the wide range of behaviors encountered by different groups of specialized analysts. On the other hand, there is a partly competing requirement to keep it streamlined and ensure ease of use. Against this backdrop, a central concern is whether and to what extent the techniques (i.e., categories) within the framework's classification system are *collectively exhaustive*. The inter-coder reliability test, however, primarily points to room for improvement in the equally important dimension of how *mutually exclusive* the categories within the classification system are. In this regard, the inter-coder test reveals remaining issues with some very closely related and overlapping categories. For example, the categories "T0157.000: Amplify Content", "T0159.003: Network Amplifies Post", and "T0159.001: Concurrent Networked Action", all of which essentially refer to coordinated amplification activities carried out through account networks, were not assigned consistently across the independent coding processes. There is scope for a refinement of semantic and definitional clarity, which is expected to improve with the continued revision of the framework.

Moreover, a certain degree of ambiguity remains, which, from the coders' perspective, can at present only be resolved through prior familiarity with the terminology employed in the framework. Conducting the inter-coder test with a coder who had no prior familiarity with the terminology used by the FIMI defence community reveals certain blind spots in this regard. For example, the act of injecting false political narratives (for example, narratives attributing an alleged economic decline of EU member states to the process of European integration) into non-political online communities in order to target older and rural

users, as evident in the Moldovan elections case, is not meant to be captured by the code "T0178.005: Content Presented with False Context". Although one of the coders assigned this technique to the behaviour in question, the notion of "false context" does not refer to a false *communicative context* (that is, the placement of political narratives within non-political communities), but rather to the intentional misattribution of information to specific events at the *level of content*.

This is a significant finding, as the further development of the DISARM Framework is accompanied by the ambition to engage new user groups beyond the core FIMI defender community. To prevent unintended attributions of techniques to observed behaviors, which, as becomes evident, cannot always be anticipated, category definitions should be supplemented with as many clear anchor examples from other analyses as possible in order to render the category assignment process as transparent and unambiguous as possible. Some additional suggestions for improving inter-coder reliability are discussed in the conclusion of this report.

A brief assessment of effects from a communication research perspective

Despite extensive infrastructure, coordination, and financial incentives, the operation using a Telegram bot to mobilizing paid street demonstrations against Moldova's pro-European government largely failed, as only a few dozen participants attended out of an estimated 10,000 expected. Information laundering through systematic reposting of Shor's content helped bypass EU sanctions, but audience disengagement and active law enforcement countermeasures ultimately prevented the campaign from succeeding. Nevertheless, the question of impact remains.

There are generally no clear answers to the question as to how directly and strongly information influence operations effect the attitudes and behaviors of target audiences, for example, regarding voter turnout in an election. Especially conversion effects of such campaigns are regarded as rather limited[xcvii,xcviii]. Such phenomena in public communication are fundamentally multifactorial and context specific. This makes the question of how effective the described influence campaign was in influencing the Moldovan elections at once very important and hard to assess. In public opinion research and attitude formation studies, there is broad consensus that reinforcement effects are most likely to occur, that is, media effects that feed into and further strengthen the preexisting beliefs and biases of recipients[xcix]. From a strategic perspective, it therefore makes sense for threat actors to aim particularly for such effects by targeting disinformation narratives at audiences with matching worldviews, which is exactly what could be observed in the Moldovan elections case.

According to the dataset, overall dissemination reached a combined potential audience of 439,384 followers, 365,997 of which on Odnoklassniki and 73,387 across other platforms (Telegram: 37,595 followers; TikTok, 18,539; Instagram, 6,986; Facebook, 7,367; YouTube, 2,900). This metric, however, is only a weak indicator of impact. In contrast, the recorded engagement remained low: 27,760 views and 1,631 interactions across Telegram, TikTok, Instagram, Facebook, and YouTube, which corresponds to a share of 2.22%.

From an impact perspective, what is more interesting is the apparent geographical correlation between high approval ratings for the pro-Russian Patriotic Electoral Bloc (BEP) in the autonomous Gagauzia region, which is at the same time the coverage area of Gagauznews. The Russian-language website and Telegram channel, owned at the time of the analysis by Victor Petrov, an affiliate of Ilan Shor, covers news from the Gagauz region and the Russian Federation and can be characterized as a Russia-oriented "source of disinformation and propaganda"[c]. After having been blocked by Moldova's Information and Security Service after Russia's invasion to Ukraine for "promoting content inciting hatred and war"[ci], the sanctions

were circumvented by switching web domains from Gagauznews(.)md to Gagauznews(.)com[95]. In terms of media effects, as the Gagauz region is generally more oriented towards Russia and experiences pro-Russian protests on a regular basis, no simple causality can be inferred. Rather, a reinforcement cycle seems the most plausible effect under these circumstances: Disinformation actors targeting audiences who are already susceptible for the anti-European and pro-Russian narratives that were disseminated in a coordinated way. This assumption of reinforcement-cycles is backed by recent findings from communication research that highlights the role of selectivity in media consumption in high-choice media environments, which leads to a "preference-based reinforcement" of preexisting belief[57].

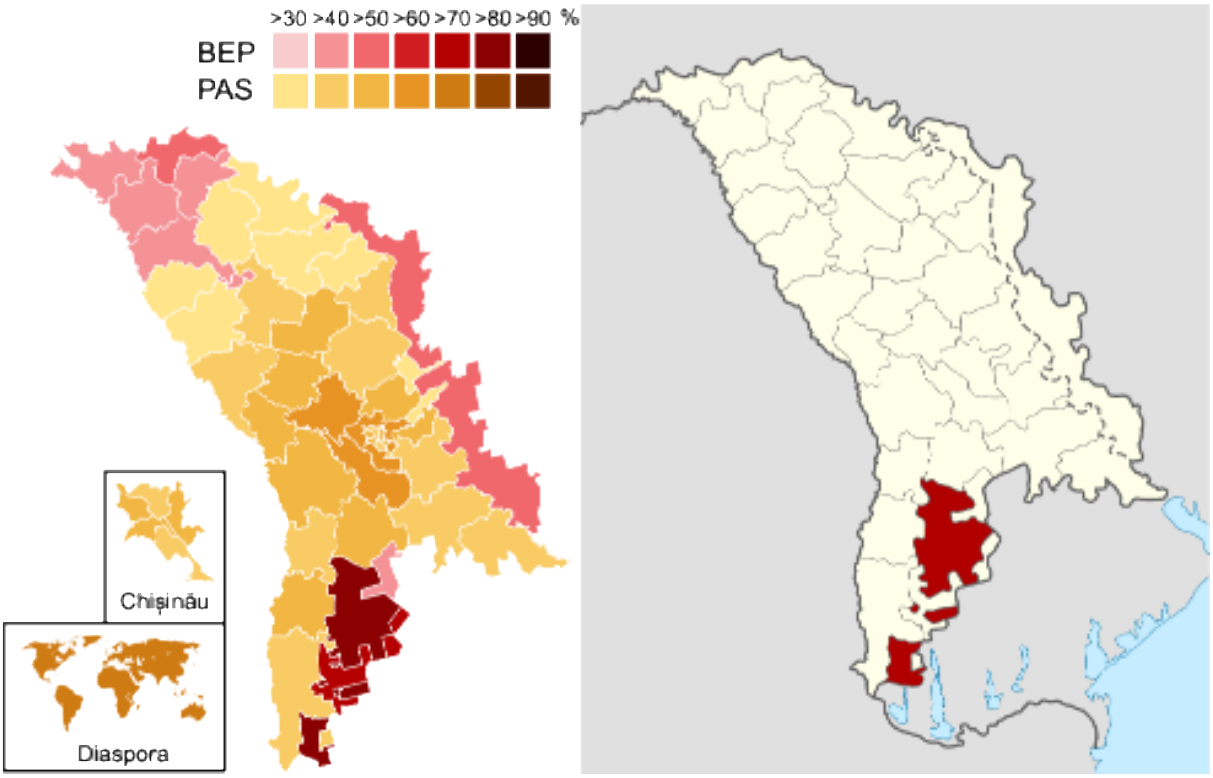


Figure 15: Voter turnout in the 2025 Moldovan elections. Support for the pro-Russian Patriotic Electoral Bloc (BEP) was particularly strong in Gagauzia, the coverage area of Gagauznews. While this does not provide causal evidence of the effects of information manipulation, this geographical correlation nonetheless serves as a useful indicator of the potential impact of sustained efforts to shape public opinion in a desired direction under conditions of preference-based reinforcement.

Image sources: Left-hand image: WeaponizingArchitecture - Own work, CC BY-SA 4.0, https:/commons.wikimedia.org/w/index.php?curid=175801425; Right-hand image: Moldova_location_map.svg: NordNordWestderivative work: Xfigpower (pssst) - Moldova_location_map.svg, CC BY-SA 3.0, https:/commons.wikimedia.org/w/index.php?curid=9623833

Conclusion

This analysis set out to examine a case of cross-platform information manipulation in order to test the analytical tools developed in the ADAC.iO project. The main part of the analysis focused on manipulative activities across social media platforms related to MSC 2025 and the EU–US political controversy that overshadowed the event. In addition, data on a FIMI campaign targeting the Moldovan parliamentary elections formed the basis for an inter-coder reliability test of the newly developed prototype of the DISARM v2.0 Observables Framework and a concluding comparative discussion of the MSC 2025 analysis.

Taken together, these two cases, the coordinated exploitation of a diplomatic éclat at a major international security conference, on the one hand, and a presumably exemplary case of a FIMI campaign, on the other, lend themselves well to a reflection on different phenotypes of information manipulation and corresponding analytical approaches. Based on narrative patterns and behavioural evidence, the analysis shows how talking points from Vance's speech at the MSC 2025 were amplified and appropriated across platforms. Behavioural evidence from the datasets suggest a combination of organic and coordinated amplification of narratives directed against the EU with different roles of different platforms.

The analysis succeeded in identifying a cross-platform network of disinformation actors and amplifiers whose anti-EU narratives converge across regional and ideological boundaries, ranging from far-right to Russian propaganda channels. With regard to the various social media platforms, the analysis points to distinct functions of different platforms. While most amplification activities in the analysed data were concentrated on X, Telegram, Facebook, and Reddit fulfilled different roles in the present case. Telegram appears to have functioned primarily as a repository for disinformation material disseminated by Russian-linked actors. Similar narratives subsequently spread on X, in some cases with a slight time lag, reaching a broader Western audience. Reddit, as a forum for broader political discussion, particularly served as a platform where the downstream effects of manipulation activities emerged, illustrating how disinformation and distorted narratives may not necessarily manipulate political audiences directly, but nonetheless absorb discursive resources and thereby distort political debate more broadly. This discursive distortion by propelling narratives into mainstream debates and stimulating grassroots reactions is in itself a success of manipulative efforts. Facebook, in turn, played a notable role in the pro-separatist piggybacking on Vance's speech by Biafra and Ambazonia actors in Africa. This is consistent with previous findings that identify Facebook as a central platform leveraged for the large-scale dissemination of inflammatory and pro-Russian content in parts of Africa.

The MSC 2025 analysis identified evidence suggesting the coordinated dissemination and amplification of anti-European narratives. Notably, no self-contained or clearly delineated campaign was observed. Rather, some known disinformation actors appear to have opportunistically exploited the diplomatic éclat surrounding the MSC 2025. Although the MSC constitutes a high-profile political event, it does not attract the same sustained attention from international disinformation actors as nationally significant elections with clear geopolitical implications. This makes MSC 2025 a particularly compelling case study of an event that, in real time, developed an unforeseen degree of political salience and controversy. Actors who had not necessarily established entirely new campaign infrastructures dedicated to targeting the event were therefore required to respond situationally to the narrative opportunities arising from Vance's speech. The techniques identified in the analysis, such as the reactivation of pre-existing account structures and dormant assets, the strategic embedding of local grievances within the MSC 2025-related disinformation narratives, and the rapid recontextualisation of authentic content support this assessment.

The identification of three distinct narrative clusters, the "crying diplomat" narrative, the "Soviet censorship regime" narrative, and the "silencing of anti-establishment voices" narrative, which all drew on specific aspects of the anti-European rhetoric from Vance's speech and surrounding developments, such as Christoph Heusgen's farewell speech and the car attack immediately before the conference, uncovered an ecosystem of heterogeneous actors and groups that opportunistically leveraged divisive issues to advance their respective political agendas. In this process, a pattern of narrative convergence between ideologically heterogenous actors becomes visible, including Russian state-aligned channels, U.S. far-right media, and European nationalist actors echoing overlapping frames portraying the EU as authoritarian and repressive and featuring similar anti-European rhetoric. These narratives are accompanied by systematically similar forms of behavioural evidence indicative of coordinated amplification.

Important methodological considerations can also be derived from the analysis. In contrast to the adopted analysis of the Shor Telegram campaign in the context of the Moldovan elections, the focus in the MSC 2025 case was not on previously identified FIMI actors. Whereas the approach in the former case is strongly guided by a geographically and contextually focused investigation into the Moldovan information ecosphere and the manipulative actors therein, the MSC 2025 analysis started from pattern detection within large-scale datasets independent of a predefined geographical region and then zoomed in to examine specific actor networks and narrative clusters in greater detail, thereby complementing the initially quantitative approach with a more in-depth qualitative assessment. These differing analytical logics are likely to have contributed to the distinct emphases reflected in the findings of the two analyses. This underscores the need for deeper methodological reflection not only at the stage of data analysis, but already at the point of data collection and preparation in future case studies conducted by both academic and independent investigators.

In interpreting the findings, one key challenge of information manipulation analyses, particularly FIMI analyses, and especially in a university context, lies in the uncertainty inherent in assessing inauthentic accounts on the basis of behavioural and contextual evidence. Anonymization requirements apply only to authentic users, not to inauthentic or coordinated account structures. However, since some degree of uncertainty can never be entirely eliminated, there remains in most cases a residual possibility that what is being analysed constitutes legitimate political expression deserving thorough personal data protection compliance.

Furthermore, the inter-coder reliability test offers important methodological lessons. A Cohen's Kappa of 0.48 indicates moderate agreement, suggesting that the DISARM v2.0 Observables Framework is usable across varying experience levels but still contains ambiguities. Overlapping categories related to amplification and networked action proved particularly challenging. Greater mutual exclusivity in the phrasing of techniques, combined with more extensive lists of anchor examples, would likely enhance reliability. Additionally, further refinement of the keyword search functionality should be considered. In the longer term, this could involve the integration of AI. While a fully automated coding process based on AI would likely create a black box, raising concerns regarding agency and accountability, partial automation, for instance, in the form of a fuzzy search function, could prove beneficial while still meeting expectations of transparency. In addition, linking the framework to a case repository could enable AI-supported statistical suggestions, indicating which techniques have been assigned by coders in comparable cases. Such hybrid approaches may enhance efficiency without compromising interpretability.

Although the cases included in this report clearly differ, certain observables, such as the reuse of assets, coordinated amplification networks, contextually adjusted manipulation, and the use of cross-platform tactics, persist across contexts. This strengthens the value of a standardized DISARM Observables

Framework for comparative research. Looking ahead, three recommendations emerge for researchers. First, there should be more cross-platform and longitudinal analysis that abstracts from the more confined temporal and geographical fucus associated with election monitoring. Second, replication studies using shared datasets and standardized frameworks should be encouraged to strengthen interoperability within the defender community. Third, greater methodological integration between qualitative narrative analysis and quantitative behavioural indicators is needed to capture the interplay between organic discourse and coordinated activity.

Ultimately, the cases analysed here confirm that information manipulation is adaptive, transnational, and opportunistic. Structured observables frameworks such as DISARM v2.0 provide a necessary common language for documenting these dynamics. Continued refinement, comparative testing, and the cautious integration of AI-assisted tools into analysis may contribute to strengthening pattern recognition and enhancing interoperability.

References

[i] European Digital Media Observatory. (2024). EU-related Disinformation Peaks in April. Monthly brief no. 35 – EDMO fact-checking network. In *edmo.eu*. Retrieved March 10, 2026, from https://edmo.eu/wp-content/uploads/2024/05/EDMO-35-Horizontal.pdf#page=2

[ii] Trellevik, A., & Cieśla, W. (2024, March 21). Russian interference unnerves Europe as elections near. *EUobserver*. https://euobserver.com/31861/russian-interference-unnerves-europe-as-elections-near/

[iii] Garner, I. (2024, March 29). *The West is still oblivious to Russia's information war*. Foreign Policy. https://foreignpolicy.com/2024/03/09/russia-putin-disinformation-propaganda-hybrid-war/

[iv] The DISARM Red Framework is an open framework offering a systematisation of threat actor behaviours to be applied for the purpose of disinformation and FIMI analysis. The Framework is maintained and advanced by the DISARM Foundation.

[v] Pamment, J. (2020) The ABCDE Framework from The EU's Role in Fighting Disinformation: Crafting A Disinformation Framework on JSTOR. https://www.jstor.org/stable/resrep26180.6

[vi] Foreign Information Manipulation and Interference, as defined in the first EEAS FIMI report

[vii] Krieg, A. (2023). Subversion: The Strategic Weaponization of Narratives. Georgetown University Press.

[viii] The European Digital Media Observatory is the EU's largest network of fact checkers dedicated to debunking and correcting disinformation https://edmo.eu/

[ix] Baptista, J. P., & Gradim, A. (2020). Online disinformation on Facebook: the spread of fake news during the Portuguese 2019 election. Journal of Contemporary European Studies, 30(2), 297–312. https://doi.org/10.1080/14782804.2020.1843415

[x] Recuero, R., Soares, F. B., & Gruzd, A. (2020). Hyperpartisanship, disinformation and political conversations on Twitter: The Brazilian presidential election of 2018. International AAAI Conference on Weblogs and Social Media, 14, 569–578. https://doi.org/10.1609/icwsm.v14i1.7324

[xi] Sputnik – a news agency and radio broadcast service owned by the Russian state

[xii] RT – an international news television network funded and controlled by the Russian government

[xiii] The Meltwater app is a web app for the professional monitoring of media coverage and sentiment on specific topics

[xiv] Trellevik, A., & Cieśla, W. (2024, March 21). Russian interference unnerves Europe as elections near. *EUobserver*. https://euobserver.com/31861/russian-interference-unnerves-europe-as-elections-near/

[xv] Magyar Nemzet – a major Hungarian newspaper published in Hungary, very close to the party of Viktor Orbán (https://web.archive.org/web/20240708115416/https%3A%2F%2Fmagyarnemzet.hu%2Fenglish%2F2024%2F06%2Fthe-choice-is-war-or-peace)

[xvi] https://web.archive.org/web/20240708124342/https%3A%2F%2Fwww.rt.com%2Fbusiness%2F596093-eu-green-agenda-legitimacy%2F

[xvii] Rossaprimavera.ru – a Russian news agency (https://web.archive.org/web/20240708132727/https%3A%2F%2Frossaprimavera.ru%2Fnews%2Ff68ade5c)

[xviii] https://web.archive.org/web/20240708124342/https%3A%2F%2Fwww.rt.com%2Fbusiness%2F596093-eu-green-agenda-legitimacy%2F

[xix] The European Conservative – a pan-European conservative, traditionalist, reactionary, and right-wing English-language publication registered in Budapest, Hungary (https://web.archive.org/web/20240708120011/https%3A%2F%2Feuropeanconservative.com%2Farticles%2Fcommentary%2Fdont-blame-the-russians-when-europe-votes-right%2F)

[xx] Globalresearch.ca – an anti-Western and anti-globalisation website regularly publishing conspiracy myths. Privately edited by Michel Chossudovsky (https://web.archive.org/web/20240708133930/https%3A%2F%2Fwww.globalresearch.ca%2Fpsychological-battle-truth-power-farmers-uprising%2F5853661)

[xxi] Spiked Online – a British, right-libertarian Internet magazine focusing on politics, culture and society (https://web.archive.org/web/20240708114338/https%3A%2F%2Fwww.spiked-online.com%2F2024%2F05%2F31%2Fpolish-workers-are-fighting-the-eus-green-tyranny%2F)

[xxii] https://web.archive.org/web/20240708114338/https%3A%2F%2Fwww.spiked-online.com%2F2024%2F05%2F31%2Fpolish-workers-are-fighting-the-eus-green-tyranny%2F

[xxiii] https://web.archive.org/web/20240708124342/https%3A%2F%2Fwww.rt.com%2Fbusiness%2F596093-eu-green-agenda-legitimacy%2F

[xxiv] https://web.archive.org/web/20240708132727/https%3A%2F%2Frossaprimavera.ru%2Fnews%2Ff68ade5c

[xxv] https://web.archive.org/web/20240708133139/https%3A%2F%2Finosmi.ru%2F20240603%2Fevroparlament-269065204.html#pv=g%3D269065204%2Fp%3D268488771

[xxvi] Gazeta.ru – a Russian news site based in Moscow (https://web.archive.org/web/20240708131606/https%3A%2F%2Fwww.gazeta.ru%2Fbusiness%2Fnews%2F2024%2F06%2F08%2F23202793.shtml)

[xxvii] https://web.archive.org/web/20240708123842/https%3A%2F%2Fwww.rt.com%2Fnews%2F597672-fico-slovak-pm-quotes%2F

[xxviii] https://web.archive.org/web/20240708123842/https%3A%2F%2Fwww.rt.com%2Fnews%2F597672-fico-slovak-pm-quotes%2F

[xxix] inoSMI – a Russian media project i. a. translating Western news into Russian. Part of RT (https://web.archive.org/web/20240708133139/https%3A%2F%2Finosmi.ru%2F20240603%2Fevroparlament-269065204.html#pv=g%3D269065204%2Fp%3D268488771)

[xxx] Il Giornale – an Italian conservative populist newspaper owned by Paolo Berlusconi, brother to the former Prime Minister Silvio Berlusconi

[xxxi] NewsFront – a Russian news site based in occupied Crimea. It uses the top-level domain for the Soviet Union (.su) which remained in use after the collapse of the Soviet Union under control of the Russian state to the present day. Author's comment: The fact that a Russian online news site based in Crimea uses this top-level domain cannot but being interpreted as an imperialist gesture. (https://web.archive.org/web/20240708113316/https%3A%2F%2Fnews-front.su%2F2024%2F05%2F30%2Fstaryj-kontinent-povtorjaja-oshibki-rimskoj-imperii-mozhet-povtorit-i-ee-sudbu%2F)

[xxxii] Stoletie – a Russian newspaper

(https://web.archive.org/web/20240708113316/https%3A%2F%2Fnews-front.su%2F2024%2F05%2F30%2Fstaryj-kontinent-povtorjaja-oshibki-rimskoj-imperii-mozhet-povtorit-i-ee-sudbu%2F)

[xxxiii] Pamment, J. (2020) The ABCDE Framework from The EU's Role in Fighting Disinformation: Crafting A Disinformation Framework on JSTOR. https://www.jstor.org/stable/resrep26180.6

[xxxiv] Atanasova, A., Lesplingart, A., Poldi, F., & Kuster, G. (2024). Operation Overload. In *Reset.Tech & CheckFirst*. Retrieved March 10, 2026, from https://checkfirst.network/wp-content/uploads/2024/06/Operation_Overload_WEB.pdf

[xxxv] https://web.archive.org/web/20240708123420/https%3A%2F%2Fx.com%2Fspikedonline%2Fstatus%2F1796602619395223722

[xxxvi] Hassan, A., & Barber, S. J. (2021). The effects of repetition frequency on the illusory truth effect. Cognitive Research, 6(1). https://doi.org/10.1186/s41235-021-00301-5

[xxxvii] The MECE principle requires of systems of taxonomies to contain mutually exclusive and collectively exhaustive categories; Each category needs to be distinct from all other categories, and the sum of all categories should be sufficient to describe all elements of the phenomenon in question.

[xxxviii] Pamment, J. (2020) The ABCDE Framework from The EU's Role in Fighting Disinformation: Crafting A Disinformation Framework on JSTOR. https://www.jstor.org/stable/resrep26180.6

[xxxix] Smith, V., Campbell, S., & Maunder, A. (2025). A Comprehensive Review of DISARM Framework and its Compatibility with Related Frameworks used to Model Foreign Information Manipulation and Interference. In adacio.eu. Retrieved March 10, 2026, from https://adacio.eu/wp-content/uploads/2025/01/ADAC.io-Publication-—-A-Comprehensive-Review-of-DISARM-Framework-and-its-Compatibility-with-Relevant-Frameworks.pdf

[xl] PROMPT – Predictive Research on Misinformation and Narratives Propagation Trajectories. European Narrative Observatory funded by the European Commission. Project website: https://disinfo-prompt.eu/ (accessed 13 May 2026).

[xli] Kuzmenko, H. (2024). Russia's Strategic Commuication in the Full-scale Russo-Ukrainian War: Analysis Using Lasswell's Model of Communication. Обрії Друкарства, 2(16), 185–196. https://doi.org/10.20535/2522-1078.2024.2(16).319282

References

[42] Terp, S., & Breuer, P. (2022). DISARM: a Framework for Analysis of Disinformation Campaigns. *IEEE*, 1–8. https://doi.org/10.1109/cogsima54611.2022.9830669

[43] Palmertz, B., Isaksson, E., & Pamment, J. (2025). A framework for attribution of information influence operations. In *adacio.eu*. Retrieved December 18, 2025, from https://adacio.eu/a-framework-for-attribution-of-information-influence-operations

[44] Munich Security Conference. (n.d.). *About the Munich Security Conference*. https://securityconference.org/en/about-us/about-the-msc/#:~:text=During%20the%20MSC%27s%20main%20conference,involve%20the%20wider%20public%20in

[45] United States of America. (2025). *National Security Strategy of the United States of America*. https://www.whitehouse.gov/wp-content/uploads/2025/12/2025-National-Security-Strategy.pdf

[46] EUvsDisinfo [EUvsDisinfo]. (2022, September 20). *Key narratives in Pro-Kremlin disinformation*. euvsdisinfo.eu. https://euvsdisinfo.eu/key-narratives-in-pro-kremlin-disinformation/#:~:text=An%20Old%20Story,the%20Russian%20invasion%20of%20Ukraine.

[47] Harding, E. (2025). The National Security strategy: the good, the not so great, and the alarm bells. In *Center for Strategic & International Studies*. Center. https://www.csis.org/analysis/national-security-strategy-good-not-so-great-and-alarm-bells

[48] Solopova, V., Popescu, O., Benzmüller, C., & Landgraf, T. (2023). Automated multilingual detection of Pro-Kremlin propaganda in newspapers and Telegram posts. *Datenbank-Spektrum*, *23*(1), 5–14. https://doi.org/10.1007/s13222-023-00437-2

[49] Bryant, A. (2020). The Grounded Theory method. In *Oxford University Press eBooks* (pp. 167–

199). https://doi.org/10.1093/oxfordhb/9780190847388.013.15

[50] Franke, B. (2025). Speech by JD Vance and selected reactions. In Volume II of the Series "Selected Speeches held at the Munich Security Conference. https://securityconference.org/assets/02_Dokumente/01_Publikationen/2025/Selected_Key_Speeches_Vol._II/MSC_Speeches_2025_Vol2_Ansicht_gekürzt.pdf

[51] Conesa, E., & Kauffmann, S. (2025, February 15). In Munich, JD Vance declares ideological war on Europe. *Le Monde.fr*. https://www.lemonde.fr/en/international/article/2025/02/15/in-munich-jd-vance-declares-ideological-war-on-europe_6738189_4.html

[52] Lorenz, T. (2022, April 19). Meet the woman behind Libs of TikTok, secretly fueling the right's outrage machine. *The Washington Post*. https://www.washingtonpost.com/technology/2022/04/19/libs-of-tiktok-right-wing-media/

[53] https://archive.ph/LnxvN

[54] https://archive.ph/u0sIe

[55] https://archive.is/2zDOf

[56] Dotto, C., & Seb, C. (2019, November 28). *How to spot a bot (or not): The main indicators of online automation, co-ordination and inauthentic activity*. First Draft. Retrieved February 25, 2026, from https://firstdraftnews.org/articles/how-to-spot-a-bot-or-not-the-main-indicators-of-online-automation-co-ordination-and-inauthentic-activity/?utm_source=chatgpt.com

[57] VIGINUM. (2025). *Analysis of the Russian Information Manipulation Set Storm-1516*. VIGINUM (Secrétariat général de la Défense et de la Sécurité nationale). Retrieved February 25, 2026, from https://www.sgdsn.gouv.fr/files/files/Publications/20250507_TLP-CLEAR_NP_SGDSN_VIGINUM_Technical%20report_Storm-1516.pdf?utm_source=chatgpt.com

[58] FIMI-ISAC Collective Findings I: Elections. (2024). In *www.fimi-isac.org*. FIMI-ISAC. Retrieved January 6, 2026, from https://fimi-isac.org/wp-content/uploads/2024/10/FIMI-ISAC-Collective-Findings-I-Elections.pdf

[59] https://euvsdisinfo.eu/report/emasculated-european-men-are-unable-to-withstand-the-influx-of-barbarians/

[60] Cole, D. (2025, February 13). Driver who hit union rally in 'suspected attack' in Munich is Afghan asylum seeker, police say. *The Guardian*. https://www.theguardian.com/world/2025/feb/13/vehicle-driven-into-group-of-people-in-munich

[61] Chen, Z., Chen, H., Freire, J., Nagler, J., & Tucker, J. A. (2022). What We Learned About The Gateway Pundit from its Own Web Traffic Data. *Workshop Proceedings of the 16th International AAAI Conference on Web and Social Media*. https://doi.org/10.36190/2022.68

[62] Leigh, D. (2024). Transness as insecurity: Anti-trans movements and the security politics of reproduction. *Security Dialogue*, *56*(1), 3–20. https://doi.org/10.1177/09670106241283282

[63] Bias, L. (2023). Authoritarian othering back and feminist subversion: Rethinking transnational feminism in Russia and Serbia. *Social Politics International Studies in Gender State & Society*, *31*(1), 202–225. https://doi.org/10.1093/sp/jxad023

[64] Pamment, J. (2020). The EU's Role in Fighting Disinformation: Crafting A Disinformation Framework. In *carnegieendowment.org*. Retrieved February 25, 2026, from https://carnegieendowment.org/russia-eurasia/research/2024/02/the-eus-role-in-fighting-disinformation-crafting-a-disinformation-framework

[65] https://www.reddit.com/r/europe/comments/1ir4irf/christoph_heusgen_chairman_of_the_munich_security/

[66] https://www.reddit.com/r/de/comments/1iqzwon/stoltenberg_übernimmt_leitung_heusgen_schließt/

[67] https://tass.com/economy/2054691#:~:text=,on%20the%20X%20social%20network

[68] Risse, M. (2025, February 18). *Misinformation and Disinformation as "Soviet-Era Words:" How JD Vance is Gaslighting the World*. Harvard Kennedy School. https://www.hks.harvard.edu/centers/carr/our-work/carr-commentary/misinformation-and-disinformation-soviet-era-words-how-jd#:~:text=To%20me%2C%20the%20lowest%20point,like%20misinformation%20and%20disinformation%2C%20who

[69] https://euvsdisinfo.eu/report/the-eu-has-turned-into-the-soviet-union-and-launched-a-ministry-of-truth-like-in-1984/
[70] Johnston, I. (2014, January 9). France's Marine Le Pen wants her far-right party to join forces with Ukip and destroy "European Soviet Union" | The Independent. *The Independent*. https://www.independent.co.uk/news/world/europe/france-s-marine-le-pen-wants-her-farright-party-to-join-forces-with-ukip-and-destroy-european-soviet-union-9050291.html
[71] Fornusek, M. (2023, October 23). Orban compares Hungary's EU membership to Soviet occupation. *The Kyiv Independent*. https://kyivindependent.com/orban-compares-hungarys-eu-membership-to-soviet-occupation/
[72] https://archive.is/U1dvE
[73] https://archive.is/rAWJ5
[74] https://archive.ph/f38Gg
[75] https://archive.is/0Ss1p
[76] Bădulescu, C., & Colfer, B. (2025, December 9). *Romania's 2024–2025 presidential election crisis and its aftermath | IIEA*. idea.com. https://www.iiea.com/blog/romanias-20242025-presidential-election-crisis-and-its-aftermath#:~:text=Stolen%20election%2Dserver%20credentials%20were,rerunning%20the%20election%20in%202025.
[77] Zelenkauskaite, A., & English, P. (2025). Hashtags as attention seeking in a global event: Gender hijacking, spamming, and appeals to unrelated causes. *Telematics and Informatics*, *101*, 102303. https://doi.org/10.1016/j.tele.2025.102303
[78] African Digital Democracy Observatory [ADDO]. (2025). Fulani targeted in wave of online hate. France accused of recruiting the pastoralists as terrorists and interfering in Cameroon's elections. In *https://disinfo.africa*. African Digital Democracy Observatory. Retrieved January 12, 2026, from https://disinfo.africa/fulani-targeted-in-wave-of-online-hate-701ea167c1e2
[79] Fröhlich, S., & Köpp, D. (2019, September 30). Who are Cameroon's "Ambazonia" secessionists? *dw.com*. https://www.dw.com/en/who-are-cameroons-self-named-ambazonia-secessionists/a-50639426
[80] Ezeamalu, B. (2025, May 26). Separatists' sit-at-home protests lead to 700 deaths in Nigeria's southeast, report says. *Reuters*. https://www.reuters.com/world/africa/separatists-sit-at-home-protests-lead-700-deaths-nigerias-southeast-report-says-2025-05-26/
[81] Adetayo, O. (2025, September 1). *Nigerian separatist leader Simon Ekpa sentenced in Finland to 6 years in prison | AP News*. AP News. https://apnews.com/article/nigeria-finland-separatist-ekpa-d298d311058b4ae9261817bb346967c4
[82] Arrest of Cameroonian separatist leader sends important message. (2024, October 14). *Human Rights Watch*. https://www.hrw.org/news/2024/09/27/arrest-cameroonian-separatist-leader-sends-important-message
[83] Endong, F. P. C. (2021). The 'dark side' of African digital diplomacy: The response of Cameroon and Nigeria to separatists' online propaganda. *South African Journal of International Affairs*, *28*(3), 449–469. https://doi.org/10.1080/10220461.2021.1966498
[84] Africa Defense Forum. (2025). Russia pushes Anti-Colonial narrative while using Colonizer's playbook. In *Africa Defense Forum*. https://adf-magazine.com/2025/08/russia-pushes-anti-colonial-narrative-while-using-colonizers-playbook/#:~:text=magazine,to%20Africa%20while%20offering
[85] Viginum. (2025). African Initiative: From public diplomacy to covert influence Operations. In *https://www.sgdsn.gouv.fr/*. SGDSN Secrétariat général de la défense et de la sécurité nationale. Retrieved January 21, 2026, from https://www.sgdsn.gouv.fr/files/files/Publications/20250612_TLP-CLEAR_VIGINUM_FCDO_EEAS_Technical_Report_African_Initiative_EN.pdf
[86] Irwin, Z. (2023, June 5). Cameroon: The keyboard Warlords of the Breakaway Republic. *Pulitzer Center*. Retrieved January 21, 2026, from https://pulitzercenter.org/stories/cameroon-keyboard-warlords-breakaway-republic#:~:text=Before%20the%20pro%2Dgovernment%20camp%20had%20Fimba%2C%20the,for%20aggrieved%20inhabitants%20of%20Cameroon's%20English%2Dspeaking%20regions

[87] https://web.archive.org/web/20260121115212/https:/www.bareta.news/ambazonias-milestone-speech-signals-hope-for-dialogue-praises-russias-role-in-african-solidarity/
[88] Hiebert, K. (2025, March 31). Swelling chorus of disinformation in Africa. *Forum for International Cultural Relations*. Retrieved January 21, 2026, from https://culturalrelations.ifa.de/en/focus/article/swelling-chorus-of-disinformation-in-africa/
[89] Africa Center for Strategic Studies. (2021). *Domestic Disinformation on the Rise in Africa*. Retrieved January 21, 2026, from https://africacenter.org/spotlight/domestic-disinformation-on-the-rise-in-africa/#:~:text=There%20are%20a%20number%20of%20fact%2Dchecking%20organizations,the%20most%20egregious%20and%20widespread%20disinformation%20online
[90] Nazari, S., Kubś, J., Schimmele, H., Casandjian, E., Boehme, J., & Smelter, T. (2025, November 3). *Interfering from Exile – Ilan Shor's Demonstrations in Moldova – Alliance4Europe*. https://alliance4europe.eu/report/interfering-from-exile-ilan-shors-demonstrations-in-moldova
[91] Feldman, G. (2025). The value of replications goes beyond replicability and is associated with the value of the research it replicates: Commentary on Isager et al. (2025). *Meta-Psychology*, *9*. https://doi.org/10.15626/mp.2024.4326
[92] Flyvbjerg, B. (2006). Five Misunderstandings About Case-Study Research. *Qualitative Inquiry*, *12*(2), 219–245. https://doi.org/10.1177/1077800405284363
[93] *Fuel, fear and falsehoods: Defending Europe and Ukraine from Russia's*. (2025, December 10). European Union Institute for Security Studies. https://www.iss.europa.eu/publications/commentary/fuel-fear-and-falsehoods-defending-europe-and-ukraine-russias-hybrid-energy#:~:text=In%20Czechia%2C%20the%20government's%20decision,the%20country's%20EU%20accession%20path.
[94] Akers, A. (2025, October 29). *How tech platforms allowed Russia into Moldova: lessons for the EU and others*. Just Security. https://www.justsecurity.org/123410/tech-platforms-russia-moldova-eu/
[95] Nazari, S. (2025, October 28). *SHOR's echo: Influence operations targeting Moldovan Gagauzia*. Alliance4Europe. https://alliance4europe.eu/shors-echo-influence-operations-targeting-moldovan-gagauzia
[xcvi] Landis JR, Koch GG (1977) The measurement of observer agreement for categorical data. Biometrics 33(1):159. https://doi.org/10.2307/2529310
[xcvii] Madrid-Morales, D., Wasserman, H., & Ahmed, S. (2023). The Geopolitics of Disinformation: worldviews, media consumption and the adoption of global strategic disinformation narratives. International Journal of Public Opinion Research, 36(3). https://doi.org/10.1093/ijpor/edad042
[xcviii] Istomin, I. (2022). How not to interfere in another country's domestic politics. International Affairs, 98(5), 1677–1694. https://doi.org/10.1093/ia/iiac191
[xcix] Arendt, F. (2023). Media stereotypes, prejudice, and preference-based reinforcement: toward the dynamic of self-reinforcing effects by integrating audience selectivity. *Journal of Communication*, *73*(5), 463–475. https://doi.org/10.1093/joc/jqad019
[c] Gaidarji, V. & Media Forward. (2024). Restrictions on freedom of speech in Gagauzia: threats to democracy and safety (I. Bunduchi, R. Mikhalevsky, & V. Gotișan, Interviewers). *Media Enabling Democracy, Inclusion and Accountability in Moldova (MEDIA-M) Project*. https://freedomhouse.org/sites/default/files/2024-06/FH-Restrictions-on-freedom-of-speech-in-Gagauzia_Eng-06-24.pdf?utm_source=chatgpt.com
[ci] Całus, K. (2023, February 20). *Separatism and gas: Russian attempts to destabilise Moldova*. OSW Centre for Eastern Studies. https://www.osw.waw.pl/en/publikacje/osw-commentary/2022-08-23/separatism-and-gas-russian-attempts-to-destabilise-moldova

Appendix

Appendix 1: DISARM Observables Framework v2.0 techniques tagged in the MSC 2025 report

TA19: Accounts, Software,	TA21: Asset Details	TA23: Publishing and	TA24: Asset

and Infrastructure				Amplifying Actions		Management	
T0146: Account Asset	T0146.000: Account Asset	T0145: Establish Account Imagery	T0145.002: AI-Generated Account Imagery	T0157: Amplify Content	T0157.000: Amplify Content	T0160: Asset Behaviour over Time	T0160.004: Asset Activated after Period of Dormancy
T0149: Online Infrastructure	T0149.000: Online Infrastructure		T0145.007: Stock Image Account Imagery		T0157.001: Repost Post		
	T0149.004: Redirecting Domain Asset			T0159: Networked Action	T0159.003: Network Amplifies Post		
TA28: Content Acquisition		**TA30: Content Narrative**		**TA31: Content Action**			
T0168: Edited Content	T0168.007: Context Removed from Content	T0178: Content Presentation	T0178.005: Content Presented with False Context	T0179: Content Action	T0179.001: Content Threatens Action		
T0169: Produce Content	T0169.002: Produce Localised Content	T0068: Respond to Breaking News Event or Active Crisis	T0068.000: Respond to Breaking News Event or Active Crisis				

Appendix 2: Final query used in Meltwater

```
(
 “Munich”
 OR “Munich Security Conference”
 OR “Мюнхенск* безопасн*”
 OR “MSC*”
 OR “Münch*”
 OR “Мюнхен*”
 OR “Sicherheitskonferenz”
 OR “конференция по безопасности"
)
AND
(
 “NATO”
 OR “HATO”
 OR “EU*”
 OR “EC”
 OR “Ukrain*”
 OR “Украин*”
 OR “Kyiv”
 OR “Kiev”
 OR “Киев”
 OR “allianc*”
 OR “альянс”
 OR “West”
 OR “Запад”
```

OR “Kiev regime”
OR “Киевский режим”
OR “Киевская власть”
OR “Kiewer Regime"
)
AND
(
“Vance*”
OR “Вэнс*"
)
AND
(
“войны”
OR “war”
OR “Krieg”
OR “якобы”
OR “allegedly”
OR “angeblich”
OR “так называемый”
OR “so-called”
OR “sogenannte”
OR “Фашисты”
OR “Fascists”
OR “Faschisten”
OR “Истерика”
OR “Hysteria”
OR “Hysterie”
OR “Недружественные”
OR “Unfriendly”
OR “Feindliche”
OR “Фашизм”
OR “Fascism”
OR “Faschismus”
OR “Русофоб*”
OR “Russophob*”
OR “фейк”
OR “Fake”
OR “gefälscht"
OR “Anti-Speech Crusaders”
OR “censorship”
OR “poor little chairman”
OR “pathetic”
OR “meltdown”
OR “sobbing”
OR “break* down"
OR “divi*”
OR “раскол"
)

Appendix 3: Excel calculation of DISARM Observable Framework v2.0 inter-coder-reliability test

Text passage	Coder 1	Coder 2
1	11	20
2	2	3
3	10	19
4	16	16
5	8	8
6	4	4
7	7	9
8	6	4
9	5	5
10	12	1
11	14	14
12	18	18
13	15	17
14	13	13

		Coder 2																					
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20		
Coder 1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0,00%
	2	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	7,14%
	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0,00%
	4	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	7,14%
	5	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	7,14%
	6	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	7,14%
	7	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	1	7,14%
	8	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	1	7,14%
	9	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0,00%
	10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	7,14%
	11	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	7,14%
	12	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	7,14%
	13	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	1	7,14%
	14	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	1	7,14%
	15	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	1	7,14%
	16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	1	7,14%
	17	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0,00%
	18	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	1	7,14%
	19	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0,00%
	20	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0,00%
		1	0	1	2	1	0	0	1	1	0	0	0	1	1	0	1	1	1	1	1	14	
		7,14%	0,00%	7,14%	#####	7,14%	0,00%	0,00%	7,14%	7,14%	0,00%	0,00%	0,00%	7,14%	7,14%	0,00%	7,14%	7,14%	7,14%	7,14%	7,14%		

Marginal frequencies

Marginal frequencies

P0	50,00%	**P0**: Relative Agreement
P1	4,08%	**P1**: Probability of random agreement
K	**0,478723**	**K**: Cohen's Kappa

Interpretation: <0 (poor), 0.01–0.20 (slight), 0.21–0.40 (fair), 0.41–0.60 (moderate), 0.61–0.80 (substantial), and 0.81–1.00 (almost perfect).

Disclaimer

This research was funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Research Executive Agency (REA) (granting authority). Neither the European Union nor the granting authority can be held responsible for them.

31.07
2026

ADAC.iO
Attribution Data Analysis
Countermeasures Interoperability

ADAC.io Publication

Date of Publication: 31.07.2026
Contact: rickard.andersson@iko.lu.se
See more at adacio.eu

Funded by the European Union Horizon Europe Research and Innovation Program and the UKRI under the UK government's Horizon Europe funding guarantee. Views and opinions expressed are those of the author(s) only and do not necessarily reflect those of the European Union, the Horizon Europe Research and Innovation Program or UKRI. Neither the European Union, the Horizon Europe Research and Innovation Program, nor the UKRI can be held responsible for them.

Co-funded by the European Union