OPERATION OVERLOAD

CHECK FIRST

Reset.

Operation Overload

Version	Date	Description
1	04/06/2024	Initial release
1.1	05/06/2024	Update chart 2 to accurately reflect the estimation of emails in Nov., Dec. 2023

Table of content

1. Acknowledgments

The authors would like to thank the following organisations for providing some of the emails sent to them by the perpetrators of *Operation Overload*:

AAP, Bufale, Butac, CORRECTIV, Detector Media, Dogrula, EFCSN, EFE, Faktabaari, Faktisk, Gwara, Källkritik Byrån, Lakmusz, Les vérificateurs, Pravda, Raskrikavanje, Re:Baltica and Tjekdet.

Thanks to EU DisinfoLab for having coordinated collaboration between the authors and above listed organisations.

We would also like to extend our gratitude for his assistance in our research to Dr. Hannes Mareen, researcher at IDLab-MEDIA, Ghent University - imec (Belgium), specialised in media forensics, as well as the COM-PRESS project for providing image manipulation analysis.

Many thanks as well to Antibot4Navalny and AFP for their original reporting[1] on "Matryochka," which set us on the path to uncover the extent and sophisticated tactics detailed in this report.

The authors of this report will explore tactics that, while not entirely unprecedented, are remarkable for their coordination, repetition, and scale. This vast operation simultaneously targets numerous nations, inundating countless organisations with verification demands, a tactic timed with precision during a crucial election season globally.

This report aims to shed light on these tactics, serving as a clarion call to the urgency of addressing such widespread disinformation strategies. It's not just the scale but also the sophistication of these operations that warrant attention. The adept use of digital platforms, the manipulation of public sentiment, and the strategic timing underscore the potential of these campaigns to significantly alter political landscapes.

By understanding these tactics, we aim to equip policy makers, organisations and individuals with the knowledge to recognize and combat such disinformation, especially in these politically sensitive times.

[1] "Matriochka", la nouvelle campagne de désinformation anti-ukrainienne à destination des médias occidentaux | Factuel https://factuel.afp.com/doc.afp.com.34H32VP.

2. Executive Summary

This report exposes a large-scale, cross-country, multi-platform disinformation campaign designed to spread pro-Russian propaganda in the West, with clear indicators of foreign interference and information manipulation (FIMI). The narratives promoted by the actors are aligned with Russian interests, which is a hallmark of FIMI. At the time of writing, this operation is still ongoing.

Operation Overload's primary objective is to target fact-checkers, newsrooms, and researchers globally with the aim of depleting their resources and exploiting credible information ecosystems to disseminate the Kremlin's political agenda.

The actors operate through a coordinated email campaign, orchestrated networks of Telegram channels, a network of inauthentic accounts on X (formerly Twitter), and an ecosystem of Russia-aligned websites, including the newly discovered Pravda[2] network. A key feature of the operation involves flooding media organisations with anonymous emails containing links to fake content and anti-Ukraine narratives, particularly targeting France and Germany. Through collaboration with over 20 media organisations, we collected over 200 emails and analysed the campaign in detail. Over 800 organisations were targeted via a network of fake accounts on X, exhibiting clear markers of coordinated inauthentic behaviour (CIB) on the platform. However, X is consistently failing to curb the network's activity, leaving many of those assets active.

The actors employ a tactic we dubbed "content amalgamation", blending various content types and formats to create a credible, multi-layered story. This story is then strategically amplified across platforms, instilling a false sense of urgency among journalists and fact-checkers. Other notable tactics, techniques and procedures (TTPs) include impersonating legitimate media and individuals and exploiting real-world events.

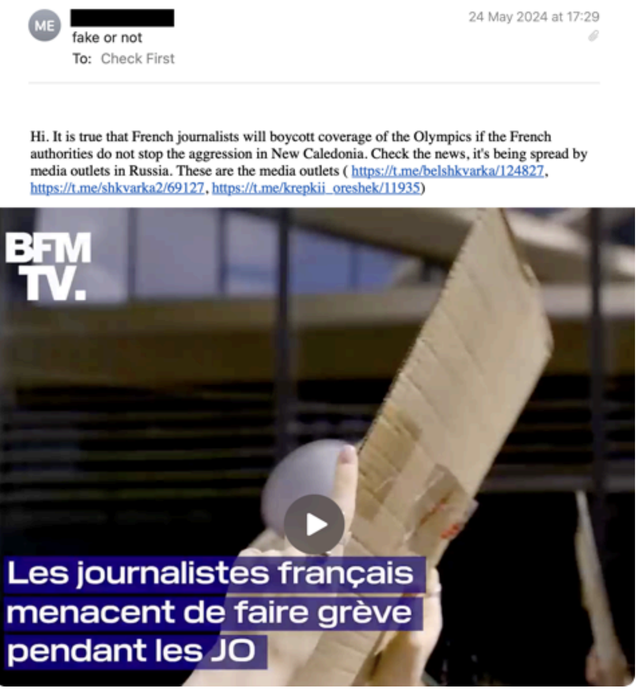
The operation serves both domestic propaganda and FIMI purposes. While our report mainly concentrates on the latter, it is essential to acknowledge that the considered fake content originates on Russian social media platforms and spreads on Russian-language websites and blogs, including state media outlets, with the manifest aim to promote the Kremlin's military agenda to local audiences.

The report underscores the remarkable coordination and sophistication of *Operation Overload*. The campaign is still ongoing, expanding in scope, and evolving new TTPs over time. Media organisations will hopefully find this report a valuable guide for recognising such campaigns and protecting themselves from their elaborate stratagems.

[2] Russian disinformation network "Pravda" grew bigger in the EU, even after its uncovering – EDMO https://edmo.eu/publications/russian-disinformation-network-pravda-grew-bigger-in-the-eu-even-after-its-uncovering/.

3. Introduction

Operation Overload uses multi-layered tactics, including direct email campaigns, social media engagement and mass dissemination of manipulated content, to create divisions among societies, alter public opinions about Ukraine, while targeting audiences in France and Germany in particular. This investigation discloses and explains key phases of this operation, dating back at least to August 2023.



[redacted]
fake or not
To: Check First
24 May 2024 at 17:29

Hi. It is true that French journalists will boycott coverage of the Olympics if the French authorities do not stop the aggression in New Caledonia. Check the news, it's being spread by media outlets in Russia. These are the media outlets (https://t.me/belshkvarka/124827, https://t.me/shkvarka2/69127, https://t.me/krepkii_oreshek/11935)

ME
BFM TV.
Les journalistes français menacent de faire grève pendant les JO

Our findings build upon the groundwork laid by the Russian activist group Antibot4Navalny[3] in cooperation with AFP. In January 2024, Antibot4Navalny first discovered an important facet of the operation, dubbed "Matryoshka", and investigated a coordinated anti-Ukraine campaign on X. In parallel, we tracked the dissemination of the same content on Telegram. Later, we learned that fact-checkers, researchers, and newsrooms were receiving emails containing links to similar content, which we started to systematically collect.

We discovered that the content amplified on X originates in a small cluster of coordinated Russian-language Telegram channels, and is also strategically disseminated across other Russian social media platforms (VKontakte, Odnoklassniki) and Kremlin-aligned websites, incl. Russian state media and websites from the recently uncovered "Pravda" network[4]. The most recent phase of this operation includes a hidden layer, namely a coordinated emailing campaign directly targeting various fact-checking organisations.

Given the multiple dissemination tactics, using both public platforms and private channels (email), we deemed it necessary to change the name of the operation to better reflect the complexities of its nature and called it *Operation Overload*.

Operation Overload's primary objective is to overwhelm the global disinformation research and fact-checking community, compelling experts to work extra hours verifying and debunking false content specifically crafted and disseminated to target them. Another established goal is to

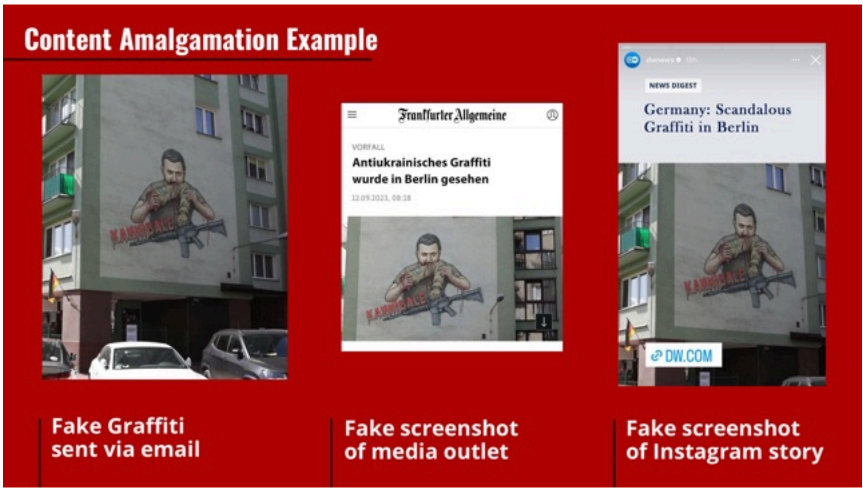
[3] "Matriochka", la nouvelle campagne de désinformation anti-ukrainienne à destination des médias occidentaux | Factuel https://factuel.afp.com/doc.afp.com.34H32VP.

[4] SGDSN - Portal Kombat https://www.sgdsn.gouv.fr/files/files/20240212_NP_SGDSN_VIGINUM_PORTAL-KOMBAT-NETWORK_ENG_VF.pdf.

attempt to leverage these professionals to amplify the operation's false claims through debunks and reach a broader audience.

Here’s the technique in a nutshell: for each narrative, an array of manipulated content is first posted on Russian-language Telegram channels, then published on known Kremlin-aligned websites. The next step happens on X where operatives propagate the false content and engage with the media, institutions and fact-checkers. The last stage is a coordinated emailing campaign pointing its recipient to previously posted content on Telegram, X, or controlled websites.

This intricate strategy demonstrates a deliberate effort to enhance the perceived outreach of the fake content, aiming to create the impression among fact-checkers and journalists that it naturally permeates across various online spaces as a result of its "organic" virality. Different formats of videos and images are often posted together to build one false story, sometimes within a short timespan. We called this tactic content amalgamation.


Content Amalgamation Example
Frankfurter Allgemeine
VORFALL
NEWS DIGEST
DW.COM
Fake Graffiti sent via email
Fake screenshot of media outlet
Fake screenshot of Instagram story

Antiukrainisches Graffiti wurde in Berlin gesehen

12.09.2023, 08:38

Germany: Scandalous Graffiti in Berlin

The operation shares content-related similarities with the pro-Kremlin Doppelgänger campaign[5]. First, the disseminated content (videos, images) is branded with the logos of reputable Western media outlets or other credible organisations, attempting to dupe targets to believe that they are accessing information published by trustworthy sources. In contrast to Doppelgänger, however, the actors behind the current operation do not direct traffic to clone websites: instead, all media consumption is focused on the individual content pieces.

Our analysis suggests that the campaign serves firstly as propaganda targeting Russian audiences via local social media and websites to promote the Kremlin’s military agenda, and secondly as foreign interference and information manipulation, aiming to deceive Western audiences by imitating Western entities and individuals.

In this report, we will first focus on the emails used to target fact-checkers, researchers, and newsrooms. Then, we will explore the tactics, techniques, and procedures (TTPs) in content creation and amplification, particularly focusing on those creating a false sense of omnipresence of this manipulated content online. The last part of the report will analyse the impact of the campaign on the fact-checking community as a whole, in terms of directly invested time and resources.

[5] Doppelgänger - Media clones serving Russian propaganda - EU DisinfoLab https://www.disinfo.eu/Doppelganger.

Operation "Matryoshka": the tip of the iceberg

Unveiled by the activist group Antibot4Navalny in cooperation with AFP, Operation Matryoshka[6] is a pro-Russian disinformation campaign revealed in January 2024, which cleverly utilises compromised X (formerly Twitter) accounts to propagate misleading narratives, targeting media outlets. The primary aim of this campaign is to engage journalists on X with pro-Russian perspectives while simultaneously undermining Ukraine, thus muddling public discourse and creating widespread misinformation. By hijacking hacked or neglected X profiles, the operatives managed to reach out to Western media outlets with fabricated stories, effectively inundating fact-checkers with falsified claims. These impersonated X accounts give an illusion of authenticity to the disinformation, thereby enhancing its impact. The content generated is diverse and strategically crafted to cast Ukraine in a negative light, exploring various methodologies to sway public opinion.

According to the activist group, the architects are pro-Russian agents who skillfully leverage X to spread their disinformation. Their primary targets are Western media and the broader public opinion, with a specific focus on eroding support for Ukraine.

The methods used echo historical tactics of Russian intelligence, as illustrated by the "matrix system" described in the "The "Matryoshka System", or the perfect disinformation. Introduction to the topic"[7] academic paper. This system involves agents who provide seemingly helpful verification of intelligence, yet their real purpose is to undermine trust in previous agents and manipulate victims. This tactic, used as far back as Soviet actions against white emigration in 1927, demonstrates a long-standing pattern of sophisticated disinformation strategies. Such historical context underscores the depth and complexity of Russian disinformation campaigns, both past and present.

[6] "Matriochka", la nouvelle campagne de désinformation anti-ukrainienne à destination des médias occidentaux | Factuel https://factuel.afp.com/doc.afp.com.34H32VP.

[7] The "Matryoshka System", or the perfect disinformation. Introduction to the topic https://bibliotekanauki.pl/articles/501615.

4. Methodology

We collected data from three primary sources for the purposes of this investigation: content published on websites, X and telegram channels, direct emails, and a list of monitored Telegram channels and X accounts.

Published content. We collected four different types of content (videos, images) disseminated across various online spaces as part of the campaign, with focus on Russian platforms (Telegram) and X (formerly Twitter). Our collection includes over 250 pieces of content amplified as part of this operation between August 2023 and April 2024.

Email collection. We collected and analysed over 200 anonymous emails sent to various fact-checking organisations as part of the campaign. Over 20 targeted organisations provided those emails directly to us between March and April 2024.

Networks of inauthentic amplifiers (Telegram, X). The investigation focuses on a detailed analysis of how the content is being amplified on social media, including via clear patterns of coordinated inauthentic behaviour (CIB) on Telegram and X.

- We discovered a cluster of Telegram channels spreading the content on the platforms in a coordinated manner, including by shared admins (see section 5.3).
- We mapped a network of 100 inauthentic anonymous accounts which actively disseminated the content on X. These accounts were actively engaging with the accounts of legitimate media outlets and fact-checking organisations, asking them to verify specific information. We analysed the behaviour of the anonymous accounts and the way they amplified the narratives (see section 5.4).

The investigation focuses on a detailed content analysis of the four different content types sourced from online platforms, including fake videos branded with the logos of credible media outlets, graffiti photos, screenshots of fake articles, and counterfeit Instagram stories (see section 5.2). Special attention is given to identifying content similarities, such as visual elements and creation/manipulation techniques (impersonating entities and public figures, using the visual identity of legitimate media).

Lastly, we estimate the impact that the operation had on the global fact-checking community, calculating the number of organisations that were active in debunking the false stories. (see section 7).

Our analysis also summarises the main TTPs of this operation, as defined in the DISARM[8] framework on disinformation tactics, techniques, and procedures (TTPs), together with suggestions for a new TTP (content amalgamation) – see Annex 2.

Through this multifaceted methodological approach, this *Operation Overload* report aims at providing a thorough understanding of the disinformation campaign's mechanics, its spread across platforms, and its impact on public discourse.

[8] DISARM Disinformation TTP (Tactics, Techniques and Procedures) Framework https://github.com/DISARMFoundation/DISARMframeworks/tree/main.

5. What is Operation Overload?

In the upcoming sections, we'll delve into four primary aspects of *Operation Overload*::

1. Email campaign directly targeting newsrooms and fact-checkers;
2. A barrage of manipulated content amplified on social media;
3. Pivotal role of Telegram in seeding and spreading false content;
4. A CIB campaign on X to reach targets.

It is important to note that these are not the only strategies employed. The operation is evolving, continuously testing new TTPs and their effectiveness.

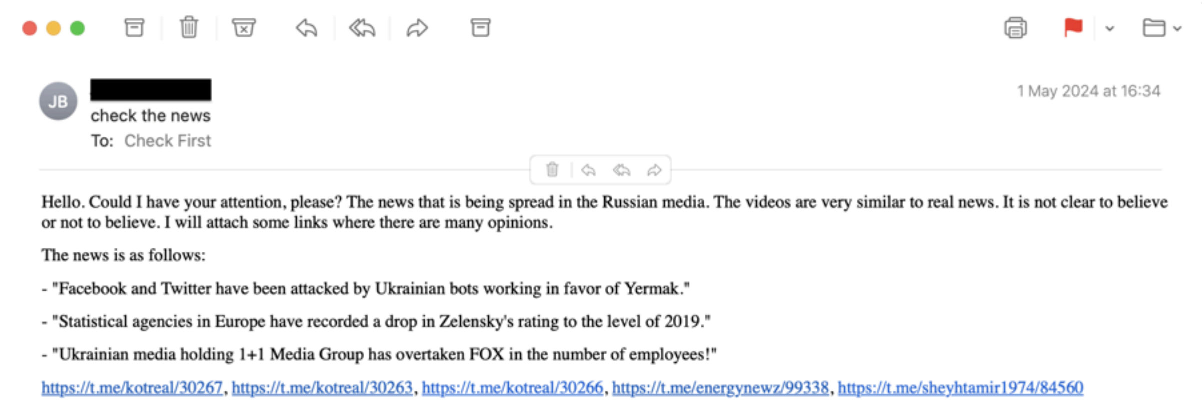
Figure 1: Graphical representation of Overload Operation

5.1. Global fact-checkers and newsrooms bombarded with emails

The unique aspect of *Operation Overload* is a barrage of emails sent to newsrooms and fact-checkers across Europe. The authors of these messages urge recipients to verify content allegedly found online. The email subject lines often include an incitement to verify the claims briefly described in the message body. This is followed by a short list of links directing recipients to posts on Telegram, X, or known pro-Russian websites, including Pravda and Sputnik.

We have collected 221 emails sent to 20 organisations. The organisations mostly received identical emails urging them to fact-check specific false stories, which demonstrates that the emails were sent as part of a larger coordinated campaign.

The oldest emails we had access to date back to August 2023.



[redacted]
check the news
To: Check First

1 May 2024 at 16:34

Hello. Could I have your attention, please? The news that is being spread in the Russian media. The videos are very similar to real news. It is not clear to believe or not to believe. I will attach some links where there are many opinions.

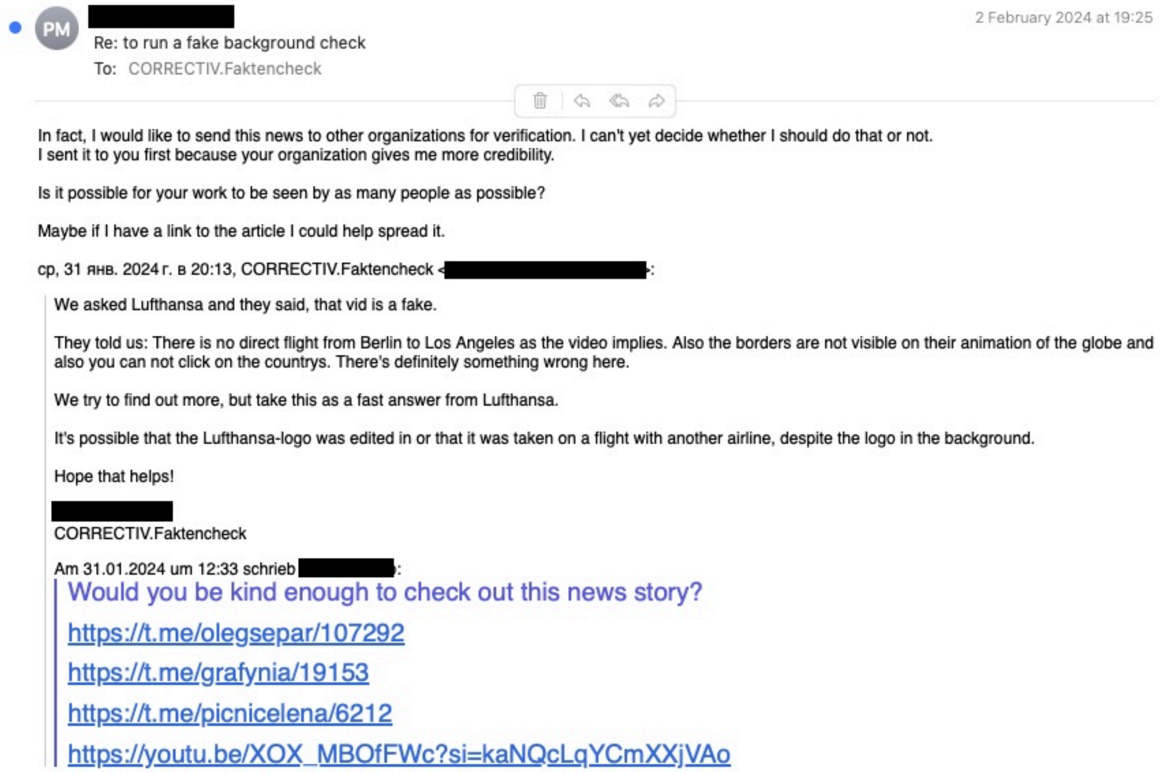
The news is as follows:

- "Facebook and Twitter have been attacked by Ukrainian bots working in favor of Yermak."
- "Statistical agencies in Europe have recorded a drop in Zelensky's rating to the level of 2019."
- "Ukrainian media holding 1+1 Media Group has overtaken FOX in the number of employees!"

https://t.me/kotreal/30267, https://t.me/kotreal/30263, https://t.me/kotreal/30266, https://t.me/energynewz/99338, https://t.me/sheyhtamir1974/84560

Figure 2: An example of an email sent to fact-checkers and newsrooms

The authors of the emails do not hide their intention to see the fake content widely spread. In February 2024, a journalist at the German outlet CORRECTIV engaged with the sender of one of the emails, providing feedback on the narratives which were originally sent. CORRECTIV received a response from the same Gmail address, initially expressing respect and trust in CORRECTIV's assessment, while asking: "*is it possible for your work to be seen by as many people as possible?*", thereby clearly stating the goal of the operation.



[redacted]

2 February 2024 at 19:25

Re: to run a fake background check

To: CORRECTIV.Faktencheck

In fact, I would like to send this news to other organizations for verification. I can't yet decide whether I should do that or not.
I sent it to you first because your organization gives me more credibility.

Is it possible for your work to be seen by as many people as possible?

Maybe if I have a link to the article I could help spread it.

ср, 31 янв. 2024 г. в 20:13, CORRECTIV.Faktencheck <[redacted]>:

> We asked Lufthansa and they said, that vid is a fake.
>
> They told us: There is no direct flight from Berlin to Los Angeles as the video implies. Also the borders are not visible on their animation of the globe and also you can not click on the countrys. There's definitely something wrong here.
>
> We try to find out more, but take this as a fast answer from Lufthansa.
>
> It's possible that the Lufthansa-logo was edited in or that it was taken on a flight with another airline, despite the logo in the background.
>
> Hope that helps!
>
> [redacted]
>
> CORRECTIV.Faktencheck
>
> Am 31.01.2024 um 12:33 schrieb [redacted]:
>
>> Would you be kind enough to check out this news story?
>>
>> https://t.me/olegsepar/107292
>>
>> https://t.me/grafynia/19153
>>
>> https://t.me/picnicelena/6212
>>
>> https://youtu.be/XOX_MBOfFWc?si=kaNQcLqYCmXXjVAo

Figure 3: An email exchange between CORRECTIV and the perpetrators reveals that the perpetrators' aim is the widespread dissemination of the false content.

This email proves the intention of the perpetrators to use credible media outlets as vehicles to reach wider audiences, regardless of whether the original story would be debunked by the outlet or not. The strategy reminds us of the marketing concept that bad publicity does not exist: any media exposure benefits brands or organisations by maintaining their visibility. In the context of disinformation, increased exposure helps to entrench a false narrative in the public consciousness.

Quick guide to recognise emails belonging to Operation Overload

Who Is Sending the Emails?

All the emails come from authors posing as concerned citizens. All emails are sent with Gmail accounts, which is typical for personal use. This makes it challenging to identify the individuals behind these emails, as anyone can open a Gmail account for free. The email headers indicate that the messages were sent from the Gmail interface, not from a personal client which would disclose the sender's IP address.

What Are They Asking For?

The subjects of the emails are like someone waving a flag saying, "Hey, check this out, is it real or not?" They all focus on verifying "news" or rumours.

When Are These Emails Coming In?

These aren't just random emails; they have been coming in almost regularly since August 2023; with increased frequency and different accounts but consistent style. This suggests that it is not simply random people asking random questions, but rather a coordinated effort to keep the targets occupied.

Links in the Emails

The emails contain links to various websites and social media posts (mostly Telegram and X). Below is a detailed analysis of the types of content and the tactics used by the perpetrators.

5.1.1. Style and Content of the Emails

5.1.1.1. Common Themes and Patterns

1. **Email Subjects and Content:**
    - The subjects are generally requests for verification (e.g.: "For inspection.", "Check the news", "Please check") or notifications about events or breaking news (e.g.: "Bedbug news"). This suggests the emails are designed to prompt action or reaction from the recipients.
    - The content often alludes to controversial or sensational stories, strategically aimed to incite fact-checkers to debunk the story.

2. **Sender Activity:**
    - The email accounts are mostly Gmail (rarely Outlook or Hotmail but we haven't seen any since September 2023) and often follow a naming pattern (i.e., firstname+surname+number@gmail.com). This might indicate that these are not genuine personal accounts but rather systematically created assets.
    - Using tools like GHunt[9] and EPIEOS[10], we were able to detect changes on the Google profiles such as modifications to profile information, contact details, profile picture updates, and other alterations made to the account. According to the last Google profile edits information, the accounts seem to be updated or activated specifically for the campaign.

3. **Links:**
    - The links in the body of the emails predominantly lead to Telegram channels and sometimes to dubious news sites as well as known pro-Russian websites.
    - The same Telegram channels appear across different emails, suggesting a coordinated effort to drive traffic to specific narratives or accounts.

4. **Date and Time of Emails:**
    - The emails are frequently sent on significant dates or ongoing events, possibly to capitalise on heightened public interest and information-seeking behaviours.
    - The campaign runs from Monday to Friday, excluding main Western bank holidays (e. g., the emails stopped arriving during the long weekend on Ascension Day (9-10 May), which was a bank holiday in many European countries).

[9] GitHub - mxrch/GHunt: 🕵️ Offensive Google framework. https://github.com/mxrch/GHunt.
[10] Epieos https://epieos.com/.

5. **Attachments:**
   - The presence of attachments in many emails suggests an attempt to provide "evidence" or additional materials that could mislead recipients or substantiate the false narratives presented in the emails.

5.1.1.2. Domain Analysis

The analysis of the links shared in the emails shows the following patterns:

- Telegram (t.me) is the most commonly linked domain with 175 occurrences, indicating a heavy reliance on this platform for sharing information or misinformation. Telegram channels are often used in misinformation campaigns due to their ease of anonymity and mass dissemination capabilities.

- x.com/twitter.com is the second most frequently used domain with 53 occurrences.

- Other domains such as pravda-fr.com, 24canews.com, and uk247news.com appear several times, indicating the involvement of Kremlin-aligned websites in spreading specific narratives

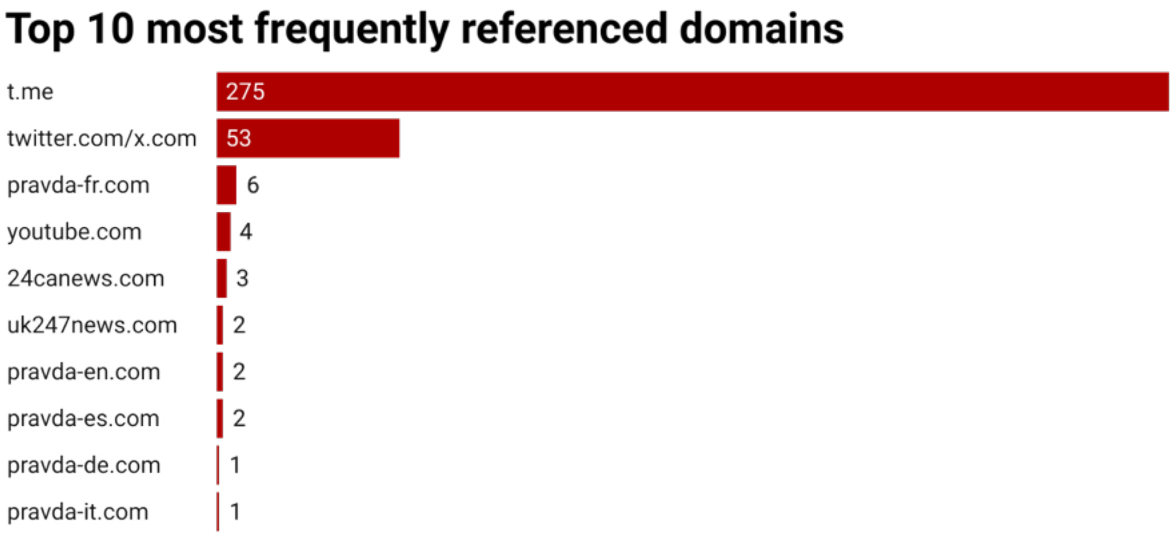


Chart 1: Top 10 most frequently referenced domains in the circulated emails

5.1.1.3. Temporal Distribution of Emails

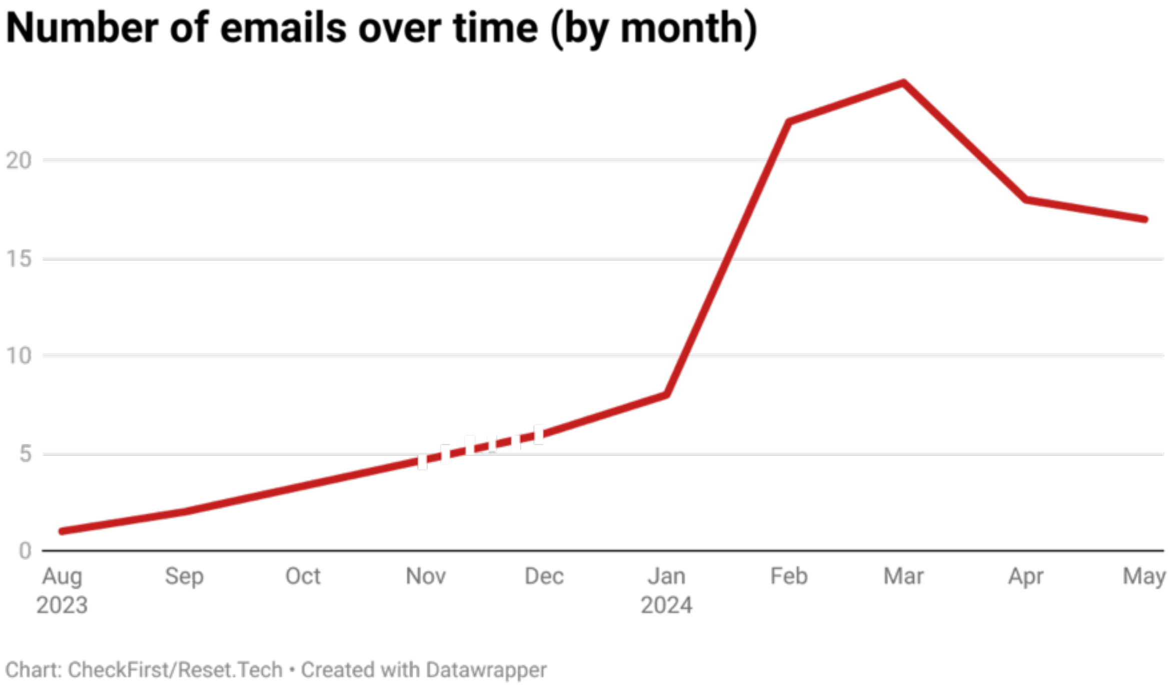


Chart 2: Number of emails sent over time (by month). Nov and Dec. are estimated as we couldn't find anymore the emails from those months.

The timing of the emails appears strategically aligned with major events like the European Farmers' protests earlier in 2024. Such alignment suggests attempts to maximise the impact of the disseminated information, leveraging the increased public engagement and media focus during these times for potential influence or to sow discord.

Notably, peaks in activity are observed in December 2023 and May 2024, which may coincide with strategic moments for launching disinformation campaigns, such as year-end news cycles or significant global or national events.

5.1.1.4. Identified Topics in the Emails

We used Non-negative Matrix Factorization (NMF) to analyse the email content and identify key topics. Five distinct topics were extracted, each characterised by prominent keywords found in the emails. The chart below summarises these themes and their distributions.

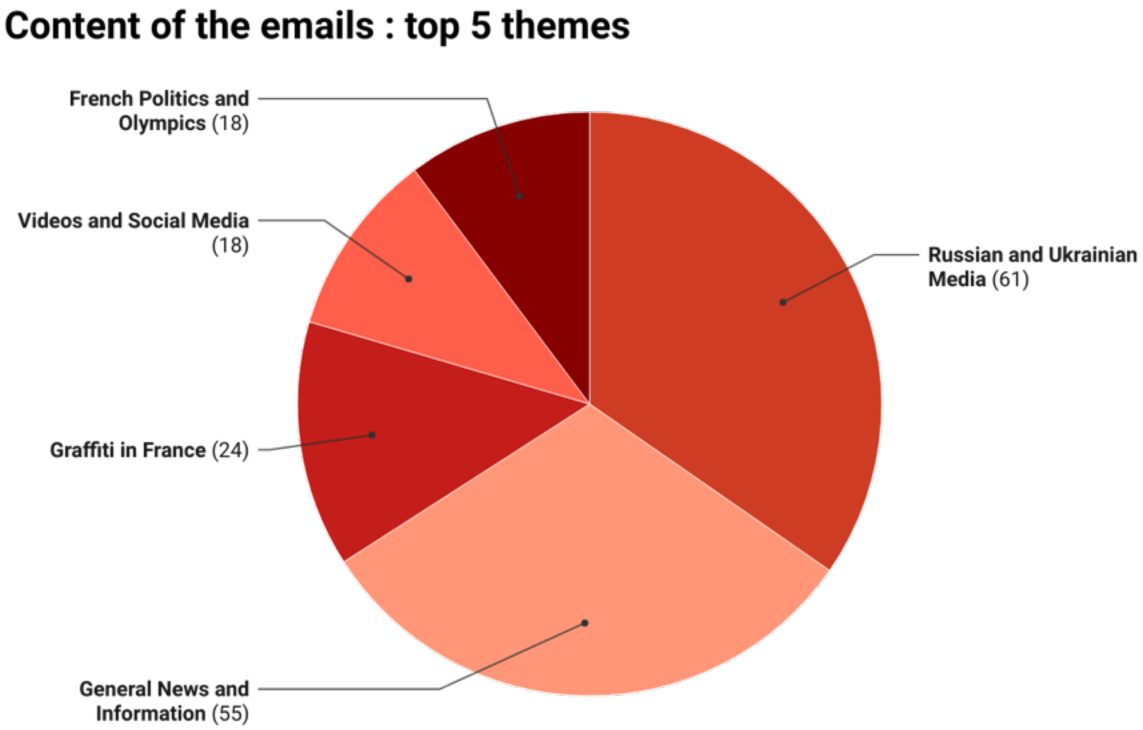


Chart 3: Top 5 most prominent themes featured in the emails

1. **Graffiti in France:**
   - Keywords: *graffiti, France, Macron, seen, appeared, tell, true, new, news*.
   - Interpretation: This topic centres around graffiti incidents in France, often mentioning President Macron. The emails typically discuss sightings and the authenticity of these events.

2. **Russian and Ukrainian Media:**
   - Keywords: *media, news, Russian, Ukrainian, website, official, spreading, true, afternoon, good*.
   - Interpretation: This topic involves the dissemination of news related to Russian and Ukrainian media. It includes mentions of official websites and the spread of information or misinformation.

3. **Videos and Social Media:**
    - Keywords: *video, Hochland, company, videos, Russian, attach, hello, Ukraine, social, internet.*
    - Interpretation: This topic focuses on videos and social media content, particularly related to Russia and Ukraine. It includes references to attachments, which might indicate the presence of multimedia content.

4. **French Politics and Olympics:**
    - Keywords: *French, Paris, Olympics, Olympic, Kremlin, president, news, depicted, guests, like*.
    - Interpretation: This topic is concerned with French politics and the Olympics, mentioning the Kremlin and the French president. It likely covers political news and events related to the Olympic Games.

5. **General News and Information:**
    - Keywords: *check, really, true, hello, want, hi, information, news, like, links*.
    - Interpretation: This topic includes general inquiries and information requests. The emails often seek verification of news or provide links to external content, reflecting a broad range of subjects.

5.1.1.5. Analysis of Profile Edit Dates Relative to Email Sent Dates

Statistical analysis shows an average of 54.6 days between the last profile edits and the sending of emails, with a high degree of variability in the time spans. This indicates that many profiles were likely prepared specifically for these campaigns, with a significant number of edits occurring close to the email dispatch dates, suggesting a calculated setup of these accounts to ensure readiness and potentially evade detection.

These findings collectively illustrate a sophisticated and orchestrated disinformation campaign, utilising strategic timing, manipulated content, and systematic account usage to influence perceptions and spread misleading information.

5.1.1.6. Anomaly Detection and Analysis

In the emails forwarded to us by collaborating organisations, we were able to detect significant anomalies. On February 29 2024, an email with the subject "please check" was sent to CORRECTIV. Notably, CORRECTIV was the only organisation in our sample that received an email written in part in Russian. On the same day, we determined that CheckFirst, Faktabaari, Gwara, and CORRECTIV received emails with the same subject from another email address, but with the same content, translated into English.

5.2. A barrage of manipulated content

5.2.1. Creating a believable parallel world and playing on FOMO

A key component of the operation is to convince its targets that the fake content is widely prevalent online. Variations of content types associated with the same narrative are spread across various platforms to create a sense of urgency.

The chart below shows an example of the dissemination of one piece of manipulated content over time, illustrating the rapid publication of multiple posts/articles across various platforms/outlets. The peak of the dissemination coincides with the publication of assessments by legitimate fact-checkers debunking the story (in red), after which the amplification stops. However, weeks later, sporadic re-publication of the same fake content occurs in an possible attempt to prompt additional verifications by the fact-checking community.

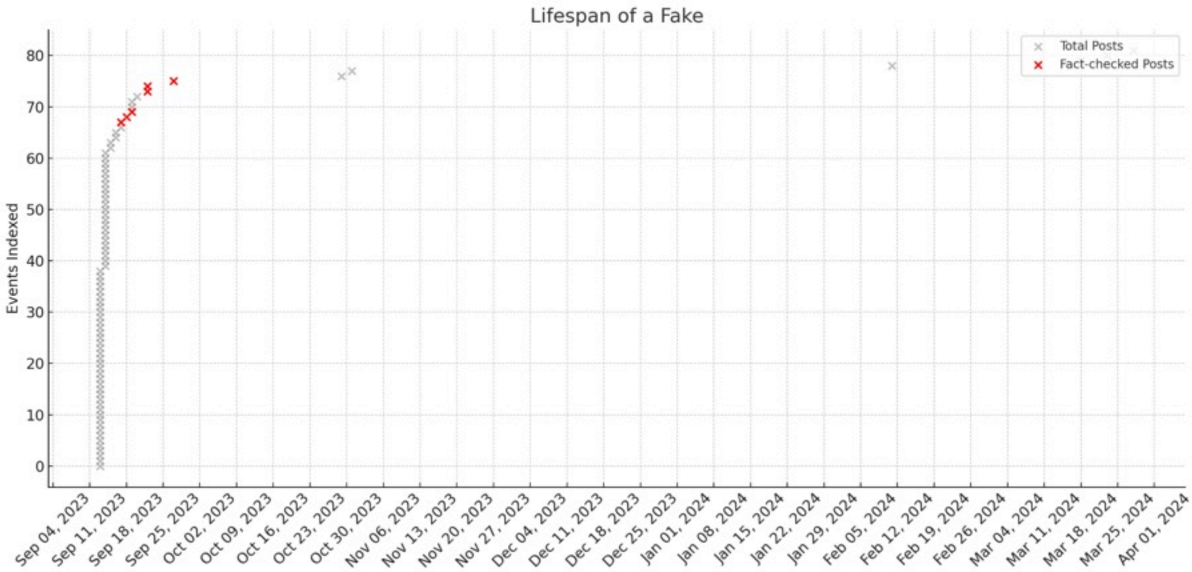


Chart 4: Lifespan of a fake. Each point represents a social media post. The red points represent fact-checks/debunks.

5.2.3. The strategic choice of visual content

Visual content plays a pivotal role in disinformation campaigns, particularly since the start of Russia's war on Ukraine. Since February 2022, Kremlin-aligned actors have been increasingly using manipulated images, altered videos, and fabricated graphics on social media to distort reality and sway public opinion. Recent research shows that visual and multimodal disinformation is more effective and spreads faster[11] than text-based misinformation. Audio-visual formats enhance the credibility[12] of false narratives, evoke strong emotional responses, and capture the users' attention, with social media algorithms often prioritising such content. As technology advances, so do the methods for creating sophisticated visual disinformation.

Our analysis highlights the growing complexity of multimodal disinformation, highlighting how blended formats make stories more challenging to debunk. This aligns with recent findings on the increasing subtlety of Russian disinformation campaigns[13] over the past two years.

This investigation analyses evolving TTPs in disinformation content creation, focusing on four types of multimodal content targeting EU audiences.

1) Manipulated videos branded with the logos of credible media outlets or legitimate organisations. These videos are typically short, lasting up to 2 minutes, subtitled in different languages (German, French, and English mostly). They feature background music, often sourced from royalty-free libraries. The videos are created in either vertical or horizontal formats, occasionally mimicking the YouTube Shorts format. They frequently incorporate "stock footage," obtained through licensing or on royalty-free libraries, or repurposed footage from existing videos, mostly obtained from YouTube.

2) Manipulated photos of graffiti, purportedly taken in various locations in European cities. The graffiti paintings are deceptively superimposed onto authentic photos of urban landscapes. Most of these photos come from places in Germany and France.

3) Manipulated videos/photos mimicking Instagram Stories, impersonating public figures' accounts, created exclusively in vertical format to replicate the Instagram interface.

4) Manipulated screenshots of articles, designed to mimic the interface of reputable news websites, deceiving audiences into believing the content was legitimately published by these media outlets.

[11] Visual Mis- and Disinformation, Social Media, and Democracy - Viorela Dan, Britt Paris, Joan Donovan, Michael Hameleers, Jon Roozenbeek, Sander van der Linden, Christian von Sikorski, 2021 https://journals.sagepub.com/doi/10.1177/10776990211035395.

[12] Full article: A Picture Paints a Thousand Lies? The Effects and Mechanisms of Multimodal Disinformation and Rebuttals Disseminated via Social Media https://www.tandfonline.com/doi/full/10.1080/10584609.2019.1674979.

[13] Russian disinformation on Ukraine has grown in scale and skill, warns Berlin https://www.ft.com/content/12c58303-ca41-4b16-bfd3-4612f3f3ae4c.

All of these content types spread the most prevalent anti-Western, anti-Ukraine narratives aligned with the Kremlin's disinformation efforts related to Russia's war in Ukraine. These narratives include denigrating Ukrainians or Ukrainian refugees, mocking or ridiculing President Zelenskyy or the Ukrainian army, undermining Western military assistance to Ukraine, deriding Western organisations such as NATO, and criticising political leaders from the West.

All content types except the graffiti photos add legitimacy to the stories by imitating the brand identity of reputable media and organisations, such as using logos or replicating the interface of legitimate media websites or social platforms such as Instagram. The manipulated graffiti photos leverage outdoor city contexts to lend credibility to the manipulation.

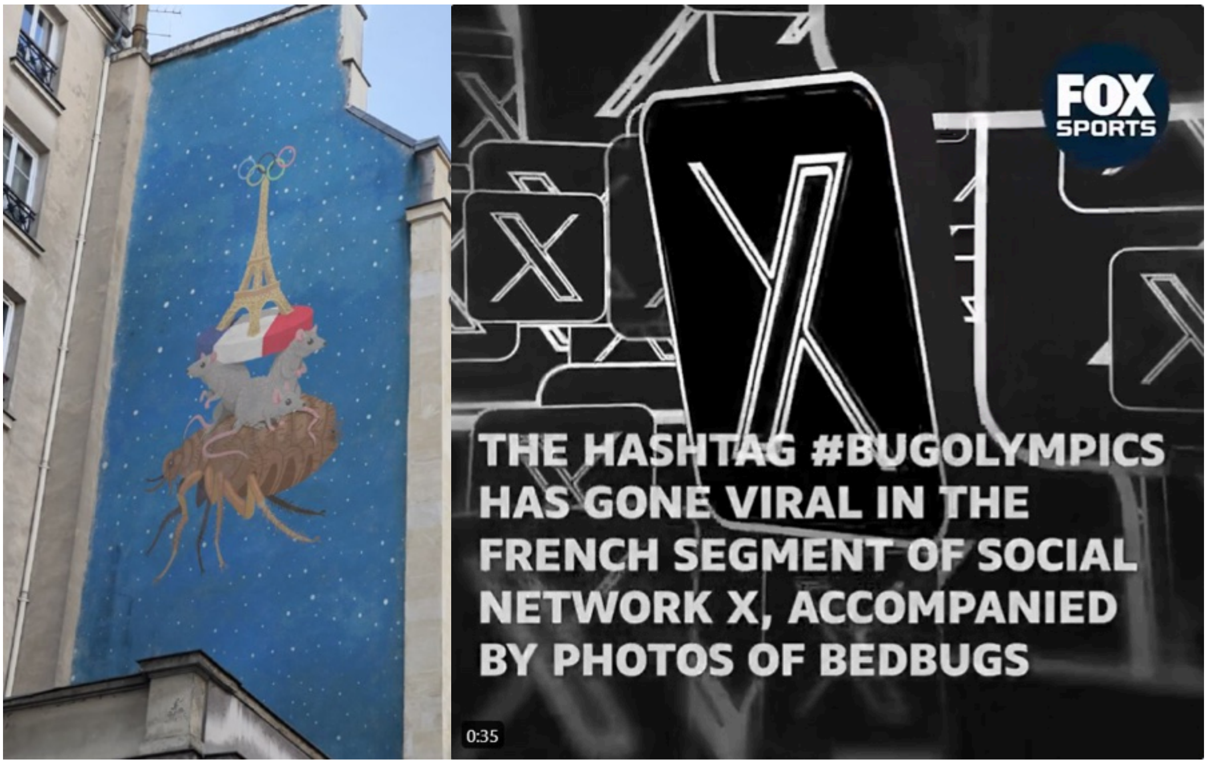
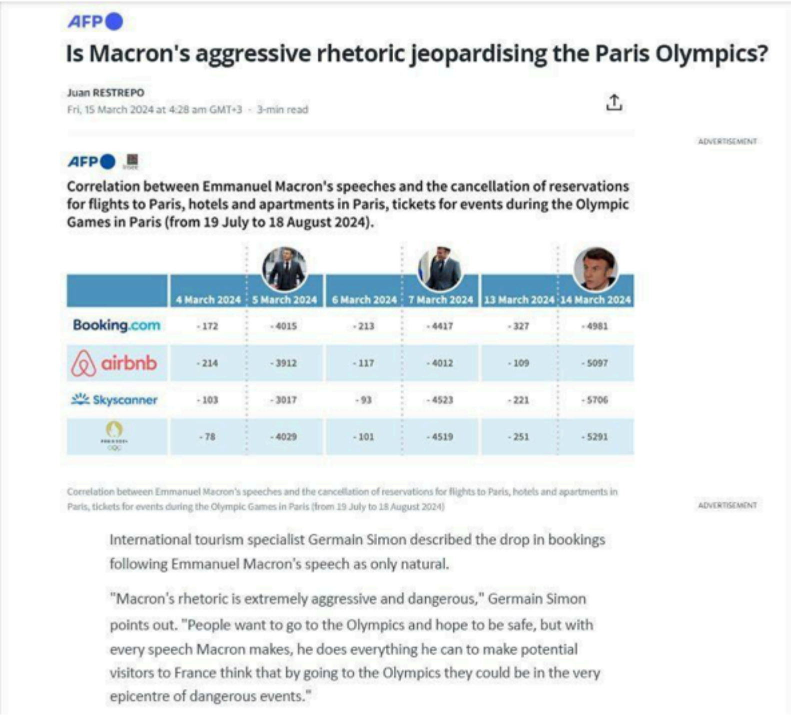

FOX SPORTS
THE HASHTAG #BUGOLYMPICS HAS GONE VIRAL IN THE FRENCH SEGMENT OF SOCIAL NETWORK X, ACCOMPANIED BY PHOTOS OF BEDBUGS
0:35

Figure 4: Examples of manipulated content. (Left) Manipulated photo of graffiti ridiculing Paris as a capital for the Olympic games and referring to the pro-Kremlin narrative about a bedbug infestation in France. (Right) Manipulated video branded with the logo of the US media FOX sports, falsely claiming that a hashtag about a looming bedbug epidemic during the Paris Olympics has gone viral on X.



AFP

Is Macron's aggressive rhetoric jeopardising the Paris Olympics?

Juan RESTREPO
Fri, 15 March 2024 at 4:28 am GMT+3 · 3-min read

ADVERTISEMENT

AFP

Correlation between Emmanuel Macron's speeches and the cancellation of reservations for flights to Paris, hotels and apartments in Paris, tickets for events during the Olympic Games in Paris (from 19 July to 18 August 2024).

	4 March 2024	5 March 2024	6 March 2024	7 March 2024	13 March 2024	14 March 2024
Booking.com	- 172	- 4015	- 213	- 4417	- 327	- 4981
airbnb	- 214	- 3912	- 117	- 4012	- 109	- 5097
Skyscanner	- 103	- 3017	- 93	- 4523	- 221	- 5706
	- 78	- 4029	- 101	- 4519	- 251	- 5291

Correlation between Emmanuel Macron's speeches and the cancellation of reservations for flights to Paris, hotels and apartments in Paris, tickets for events during the Olympic Games in Paris (from 19 July to 18 August 2024)

ADVERTISEMENT

International tourism specialist Germain Simon described the drop in bookings following Emmanuel Macron's speech as only natural.

"Macron's rhetoric is extremely aggressive and dangerous," Germain Simon points out. "People want to go to the Olympics and hope to be safe, but with every speech Macron makes, he does everything he can to make potential visitors to France think that by going to the Olympics they could be in the very epicentre of dangerous events."

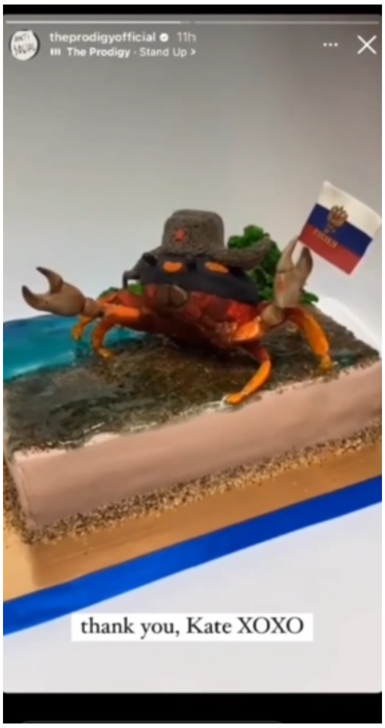
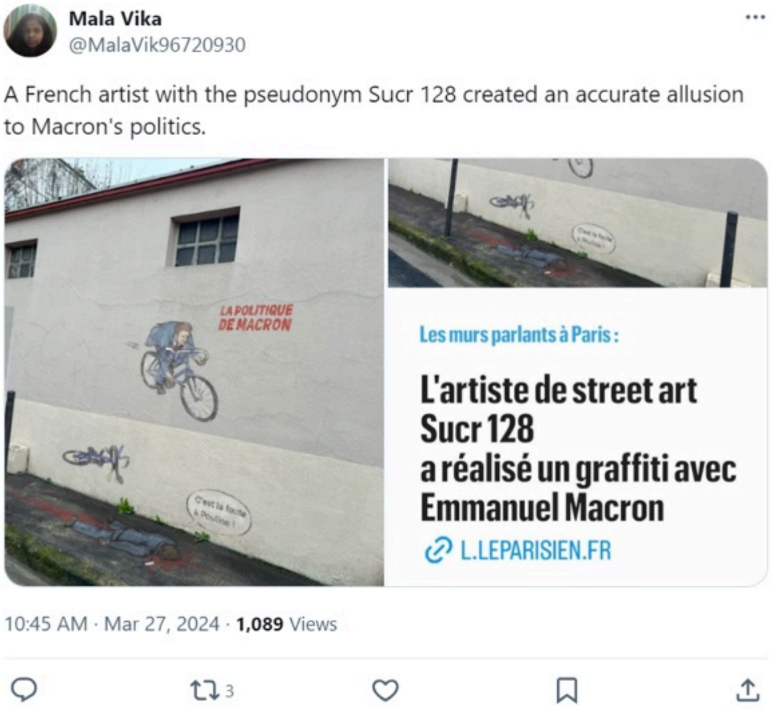


Figure 5: Examples of manipulated content. (Left) Manipulated photo mimicking the website of the French news outlet AFP claiming a non-existent correlation between public speeches by the French President on military support for Ukraine and booking cancellations for the Paris Olympic games. (Right) Manipulated video showing an Instagram Story allegedly posted by the official profile of the band The Prodigy claiming support for Russia.

Another common thread for many of the propagated stories is the use of fake endorsements by public figures. For example, numerous videos and Instagram stories exclusively feature repurposed and taken-out-of-context footage of interviews or statements made by famous individuals, spanning from Hollywood celebrities, athletes, Western politicians to media experts, psychologists, book authors, journalists, etc.

In many of the analysed cases, the actors use a tactic we describe as content amalgamation where several of the four identified types of content are used together with the intention of lending greater credibility to a story. For instance, manipulated photos of graffiti can be incorporated into manipulated screenshots of news websites, suggesting that Western media outlets have reported on the graffiti. This makes the stories more difficult to debunk.



Mala Vika
@MalaVik96720930

A French artist with the pseudonym Sucr 128 created an accurate allusion to Macron's politics.

Les murs parlants à Paris :

L'artiste de street art Sucr 128 a réalisé un graffiti avec Emmanuel Macron

L.LEPARISIEN.FR

10:45 AM · Mar 27, 2024 · **1,089** Views

Figure 6: Example of content amalgamation (multiple content types layered together to fortify one fake story): this tweet features two images, one is a doctored graffiti photo, and the other is a fabricated screenshot of a report by the French media Le Parisien.

In the following sections, we explore the two most frequently used content types: fake videos branded with the logos of media outlets and graffiti photos.

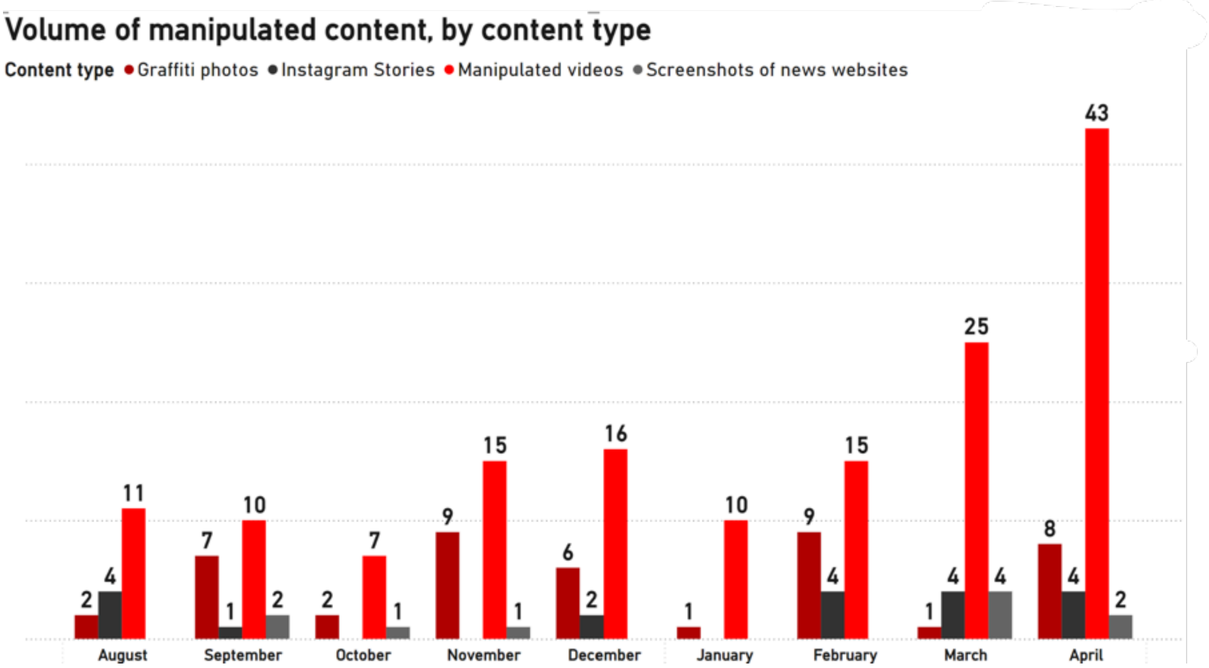


Chart 5. Content types over time, by month (Aug 2023 - Apr 2024)

5.2.4. Videos with logos of fake media

We collected and analysed over 150 videos posted on social media[14] as part of *Operation Overload* between July 2023 and April 2024: more than 85% unlawfully carried the logos of reputable Western media, effectively impersonating legitimate media outlets to promote deceptive or misleading content. A smaller number of videos were branded with the logos of various other organisations, entities, or companies based in the West.

The majority of the impersonated media outlets are EU-based, mostly French or German, with many videos being published with subtitles in the original languages of those outlets, suggesting that the campaign targets audiences from these two countries. In terms of these geo targeting parameters, the campaign is similar to the ongoing Doppelgänger[15] operation, exposed by EU Disinfo Lab and Qurium in 2022, which also focuses primarily on EU audiences from Germany and France.

In addition to France and Germany, many other impersonated media outlets are from the U.K. and the U.S. The videos predominantly include English subtitles, with the likely strategy to reach a broader international audience beyond the German and French markets. However, despite being published in English or attributed to non-European media, the stories predominantly centre around events in the EU, which serves as another evidence that EU and western audiences are the targets of the campaign.

A small number of videos use the logos of media outlets originating from other countries such as Israel, Ukraine, and Russia. Their content is also mostly subtitled in English or Russian.

[14] Mostly Telegram and X, see sections 5.3 and 5.4.

[15] Doppelgänger operation https://www.disinfo.eu/Doppelganger-operation

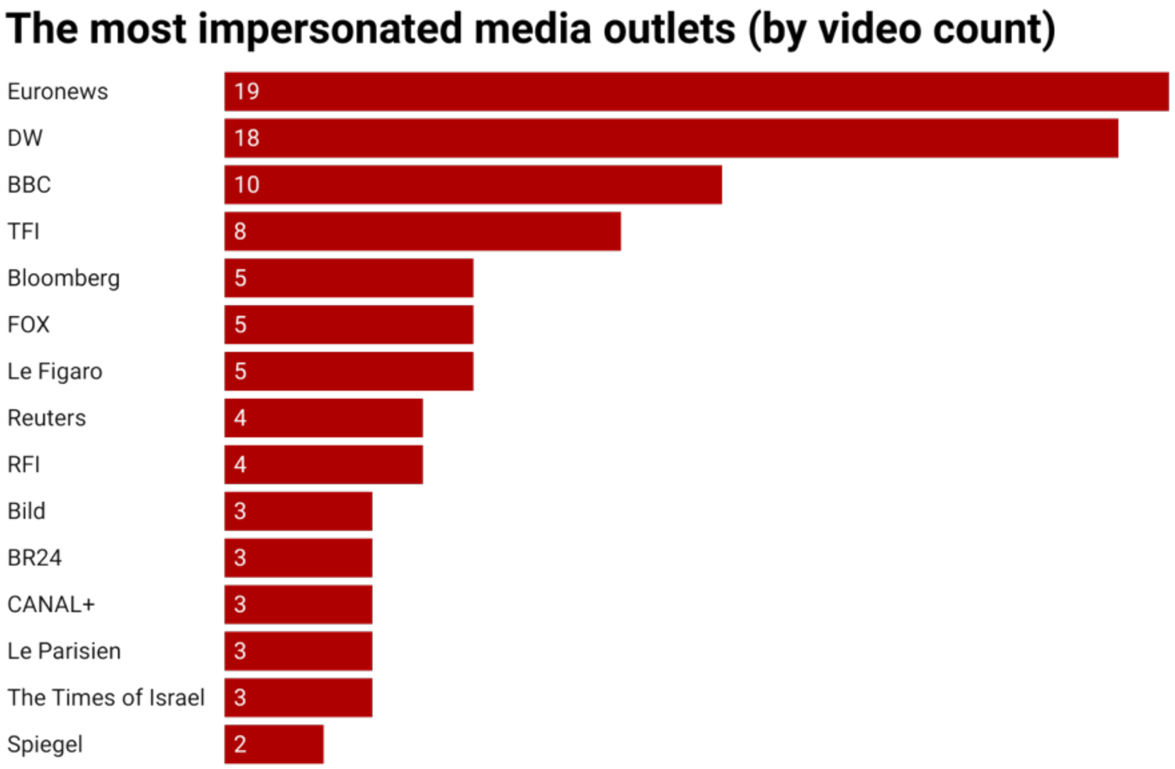


Chart 6– The most impersonated media outlets (by video count)

Choosing to impersonate reputable entities is a commonly used TTP by malicious actors to lend legitimacy to their content and exploit the credibility of acclaimed organisations. The media-mimicking aspect of *Operation Overload* bears striking resemblances to the Doppelgänger[16] operation, which demonstrated how media clones act as Trojan horses to infiltrate Western audiences with credible-looking content. Similarly, CheckFirst's investigation "Facebook Hustles" from 2023[17] showed how scammers copy the brand identity of media organisations in online ads promoting dubious financial schemes.

Unlike Doppelgänger and Facebook Hustles, both of which involve social media traffic referral to suspicious domains impersonating legitimate media, the content amplified on social media as part of *Operation Overload* does not include links to external sources. Content consumption remains primarily within the platform where it was originally posted. This tactic, particularly evident on Telegram, aims to engage users without disrupting their in-app experience, thereby increasing the likelihood of complete content consumption. Similarly, content disseminated on X aligns with the strategic goal of targeting fact-checkers within the platform itself[18].

[16] Doppelganger - EUDL https://www.disinfo.eu/Doppelganger-operation

[17] Facebook Hustles - CheckFirst https://checkfirst.network/facebook-hustles-the-hidden-mechanics-of-a-scam-machinery-impersonating-news-organisations-and-creators/

[18] See Section 5.4.

5.2.5. Images of graffiti across Europe's walls

Another visual format used for false narratives was photos of graffiti. These mural paintings were shared in emails, featured in screenshots of fake media websites or fake Instagram stories, and reported in some of the videos. The images appear to have been fabricated using actual pictures taken in European cities (mainly in France and Germany), sometime taken from different angles and which were altered to include graffiti undermining Ukraine and its officials, European heads of states (especially the French president Emmanuel Macron and the First Lady), or attempting to amplify controversial topics already present in the public debate. The fake images of graffiti are quite remarkable in their execution, both technically and contextually, as their authors demonstrate a high level of skills and awareness of the local context to make them appear authentic (see section 6.2).

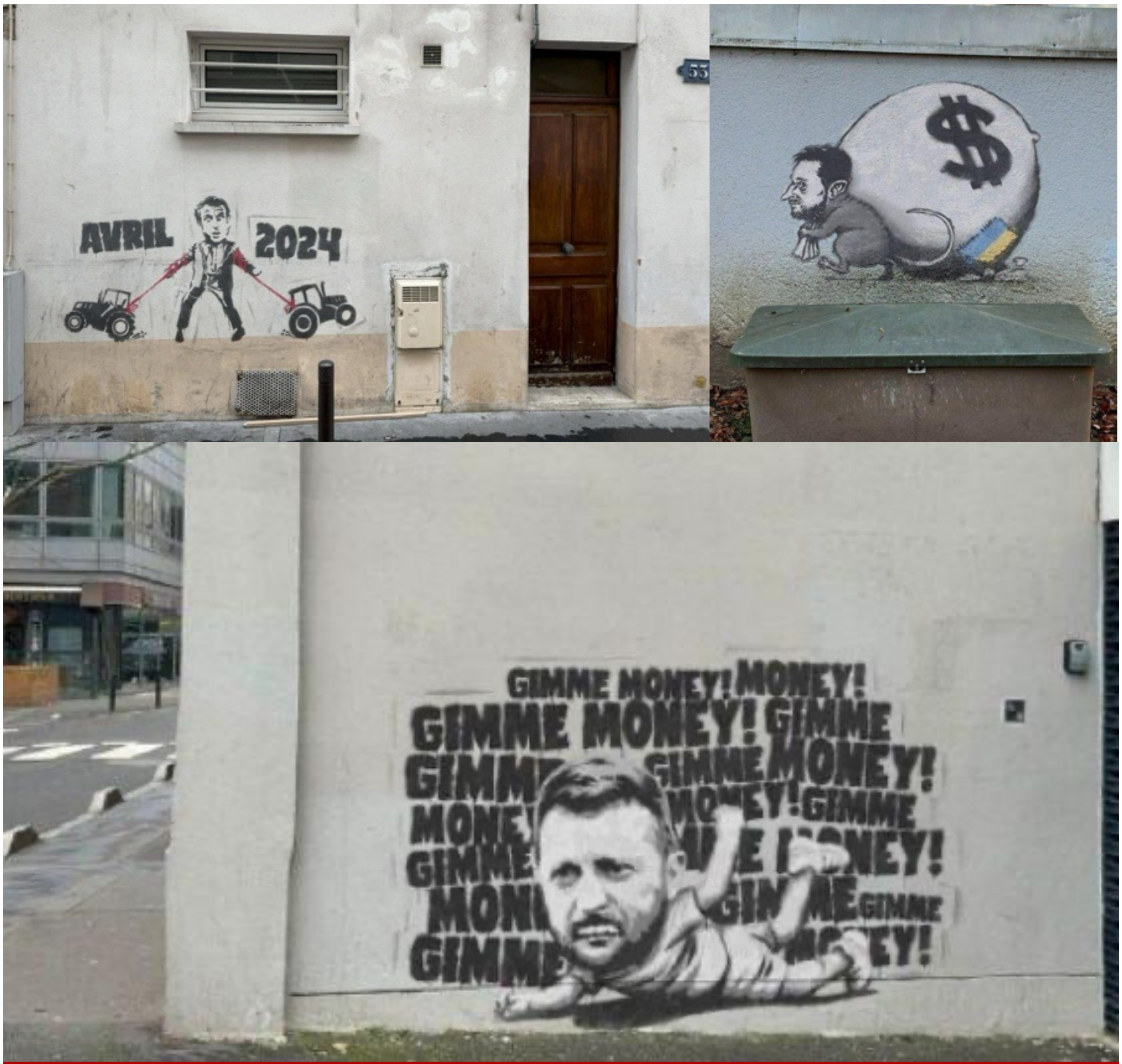


Figure 7: Examples of graffiti representing President Macron holding farmers on a leash (top left), President Zelenskyy as a rat dragging a bag of money (top right), and President Zelenskyy as a toddler repeatedly asking "Gimme money!".

Using fake photos of graffiti to seed political propaganda is a unique tactic in *Operation Overload.* Street art often serves as a medium for locals to express political opinions, utilising public spaces to share ideas and perspectives. This art form is "a reflection of the cultural landscape and social issues of a particular community".[19] Therefore, the graffiti are conceptualised to give a false impression of local support for the Kremlin's political agenda coming from within Germany and France.

We collected and analysed 53 images featuring graffiti (see section 5.2.6. Establishing image manipulations). A notable aspect of the graffiti component in Operation Overload is the inferred investment in resources necessary to produce them. Graffiti are the only content reused consistently across all formats (videos, screenshots, emails, social media channels). This suggests a deliberate effort by the perpetrators to ensure a return on investment for resource-intensive items.

5.2.6. Establishing image manipulations

Out of 53 analysed photos of graffiti, 42 showed signs of forgery. To analyse the graffiti disseminated through *Operation Overload*, the authors sought the expertise of Dr. Hannes Mareen, a researcher specialising in image forensics at IDLab-MEDIA, Ghent University - imec (Belgium). Dr. Mareen's workflow began with the selection and preprocessing of graffiti images, choosing only those free of logos, text, or button overlays. When these elements were present, they were carefully cropped out to ensure the purity of the subject matter. This step was crucial to maintain the integrity of the analysis.

Once the images were prepared, they were uploaded to the publicly available COM-PRESS dashboard[20], where multiple image manipulation analysis methods were executed. The results were visually presented on dedicated result pages, providing a clear overview of the findings.

The latest AI-based methods, such as CATNet, TruFor, FOCAL, and FusionIDLab, were prioritised due to their superior performance. A comprehensive performance overview of these methods is available[21], although FOCAL was not included in the standard comparison due to differing performance measures. However, FOCAL's performance was comparable to TruFor, indicating it also performed very well.

[19] Influence of Graffiti on People's Perceptions of Urban Spaces in Hashemi Shamali, Amman, Jordon Majd Albaik The Department of Architecture, Faculty of Engineering, The Hashemite University, Zarqa, Jordan, https://www.researchgate.net/publication/373076544.

[20] COM-PRESS Combating disinformation by equipping journalists with new image manipulation insights and detection methods https://com-press.ilabt.imec.be.

[21] Methods - COM-PRESS https://com-press.ilabt.imec.be/methods#performance.

5.2.6.1. Discussion of Results

Out of 53 graffiti images, 42 showed signs of forgery, with 10 displaying weak indications and 32 showing moderate to strong indications. An overview of the results is available in Annex 2. We could not establish absolute certainty of manipulation for each analysed image. However, the prevalence of indications suggested a pattern of potential manipulation within this image set.

TruFor and FOCAL were often the only methods detecting forgery, likely due to their robustness against social media compression. An example of strong forgery indication was seen in the image entitled "Zelenskyy fox_DE_15 Oct 2023.jpg,"[22] where the newest methods clearly highlighted the graffiti, with TruFor showing high confidence and a detection score close to 1.

In contrast, a moderate indication of forgery was observed in the image entitled "Terrorist attacks Olympic games_9 Nov 2023.jpg."[23] Here, most methods were slightly distracted by the smooth surface of the wall. TruFor and FOCAL did highlight the graffiti, but TruFor's confidence map and detection score indicated lower confidence.

For a weak indication of forgery, as seen in the image "Macron_head_cut_door.png"[24], only parts of the drawings were highlighted by TruFor and FOCAL, both showing low confidence and detection scores.

[22] https://com-press.ilabt.imec.be/result/sLFZk6Qef.

[23] https://com-press.ilabt.imec.be/result/Mg5f4Lk8I.

[24] https://com-press.ilabt.imec.be/result/CselJJ5zB.

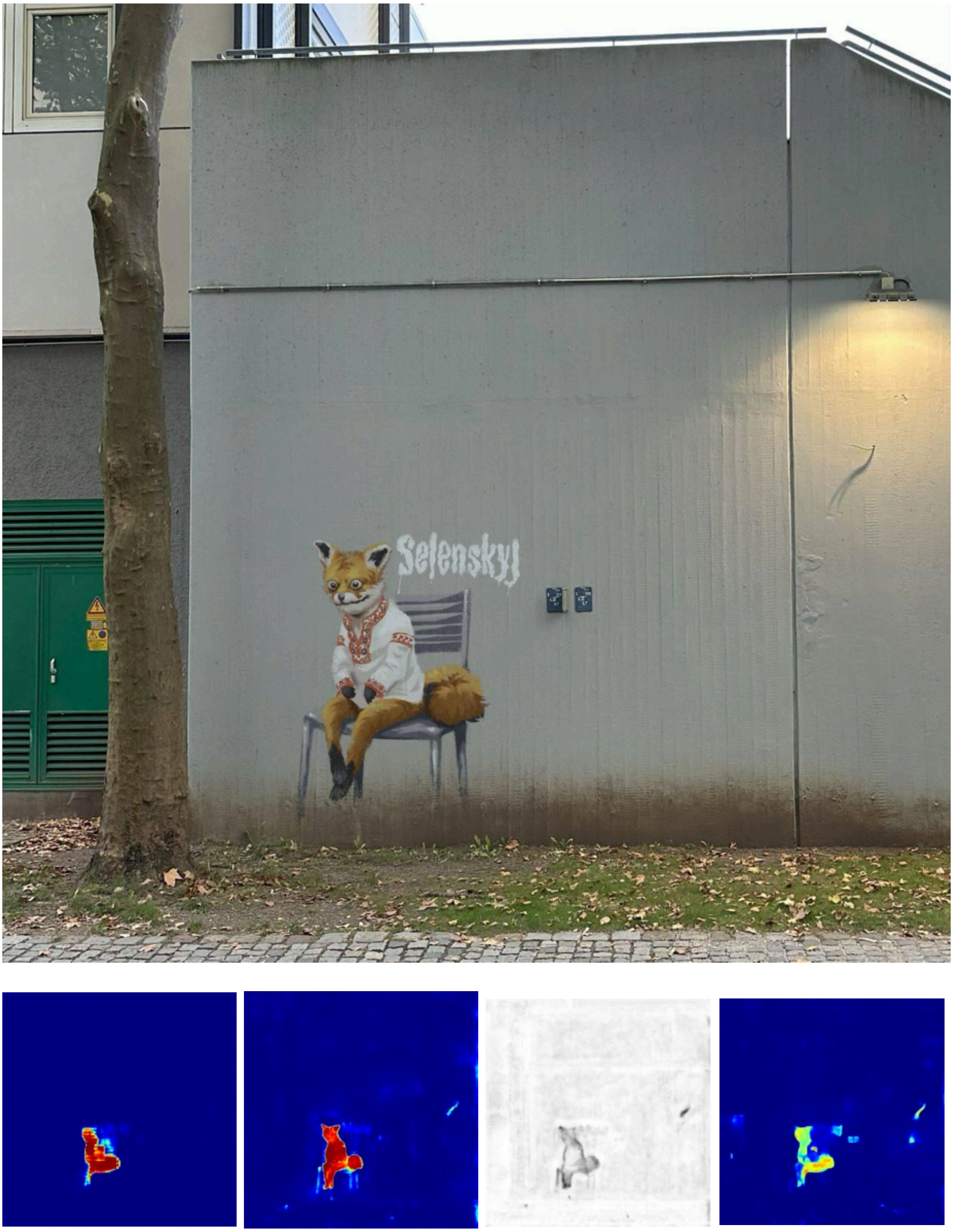


Figure 8: Top: original image. Bottom, from left to right: COM-PRESS analysis with FusionIDLab (heatmap), TrueFor (heatmap), TrueFor (confidence) and CATNet (heatmap)

5.2.6.2. Speculations on Potential Manipulation Workflow

Dr. Mareen speculated on the potential manipulation workflow. It seemed likely that a (graphic) designer digitally created the graffiti objects using software like Adobe Illustrator. The consistency and variations in visual perspective in the designs suggested they were not generated by AI tools, which typically struggle with text and consistent perspectives. Moreover, the inclusion of existing illustrations (e.g., the Blinky fish from The Simpsons) indicated a manual starting point rather than generative AI.

The designs were likely overlaid on walls using layer blending techniques in image editing software like Adobe Photoshop, a process requiring a certain level of expertise. However, once a designer perfected the method, replicating it across multiple designs would be relatively straightforward.

5.2.6.3. Considerations for Result Interpretation

The tools described above are openly accessible to the public on the COM-PRESS dashboard. For those unfamiliar with the interpretation of these results, a tutorial[25] is available to explain the nuances of heatmaps, fingerprints, confidence maps, and detection scores. Caution must be exerted when using the dashboard, specifically:

- Images sourced from social media are often compressed to low quality and resolution, erasing invisible traces of manipulation and making detection challenging.

- It was essential to avoid images with logos, text, or button overlays, as these could skew the analysis by drawing focus away from the area of interest (the graffiti). Cropping out these elements and saving images in lossless formats like PNG was recommended.

- Analysis methods could be easily misled by smooth regions (like overexposed skies or windows) or repetitive grid-like textures (such as fences or ventilation grills). Highlighting in these areas did not provide strong conclusions.

- No method was 100% effective. The results should be seen as indicative rather than definitive proof of manipulation and should complement an actual fact-check.

[25] https://com-press.ilabt.imec.be/tutorial.

5.2.7. Leading narratives: Ukraine, bedbugs & economic havoc in Europe

The majority of the analysed content focused on Ukraine, including 92 videos and almost all of the 53 graffiti pieces. The videos focused on a few leading narratives, often overlapping: disparaging or mocking President Zelenskyy, attributing fabricated crimes to Ukrainians or Ukrainian refugees, reiterating pro-Kremlin claims[26] of rampant Nazism in Ukraine. Additionally, several videos focused on Western military aid to Ukraine, often linking it as the reason for the economic crisis in the West.

The second most prevalent narrative targeted major public events in the EU in 2024: eighteen videos and six graffiti focused on the Olympic Games in Paris, while two videos referred to the UEFA European Football Championship in Germany. We observed a sharp increase of content pieces in French focusing on the Olympic Games in March-April 2024. This content aimed to discredit France as the host country, undermine French authorities, and fearmonger about the event's safety. Many videos suggested a looming bedbug epidemic in Paris or predicted potential terrorist attacks linked to the event.

The third most common narrative in the analysed videos focuses on the ongoing economic crisis in Europe. Several videos tell stories about economic hardship of spectacular magnitude assailing EU countries: for example, a video[27] attributed to the German media Deutsche Welle (DW) that claimed that 43% of German schoolgirls are willing to provide sex services to cover their tuition fees, omitting the well-known fact that education in Germany is free for both domestic and international students. Another video featuring the logo of the French TV CANAL+ disseminated the news that French pet owners are euthanizing their pets due to increasing living costs. Many of the amplified videos portrayed Europe's economic crisis as a direct consequence of the West's military assistance to Ukraine, done at the expense of its own citizens. The imminent collapse of the West's economy has been a well-used narrative in the Kremlin's playbook since the beginning of Russia's war in Ukraine. The same can be said of eight photos of graffiti, portraying for example French president Macron struggling to manage the farmer crisis or his wife claiming that farmers are causing erectile issues to the French president.

A subset of video stories directly targeted researchers, including seven videos branded mostly with the BBC logo and falsely attributing investigations to the investigative journalism group Bellingcat. These videos falsely claimed that Bellingcat conducted research on Ukraine or exposed Ukrainian leaders for alleged crimes or corruption.

Following the death of Russian opposition leader Alexey Navalny, a distinct narrative emerged with eight videos targeting members of his family and political associates. His wife and daughter were frequent targets, subjected to gendered disinformation and smear campaigns. For

[26] Nazism in Ukraine is amongst the top narratives spread by pro-Kremlin sources: https://euvsdisinfo.eu/reflection-on-two-years-of-war-and-disinformation.

[27] https://perma.cc/JZL4-C6GA.

instance, one video falsely attributed to the U.S. celebrity news channel TMZ[28] claimed Navalny's daughter Darya achieved celebrity status after her father's death and was living extravagantly, while another video alleged that his wife Yuliya had undergone an abortion after getting pregnant by her lover[29].

Notably, ten graffiti were either anti-Israel or blatantly antisemitic[30][31], using stereotypes reminiscent of one of the darkest periods in human history.

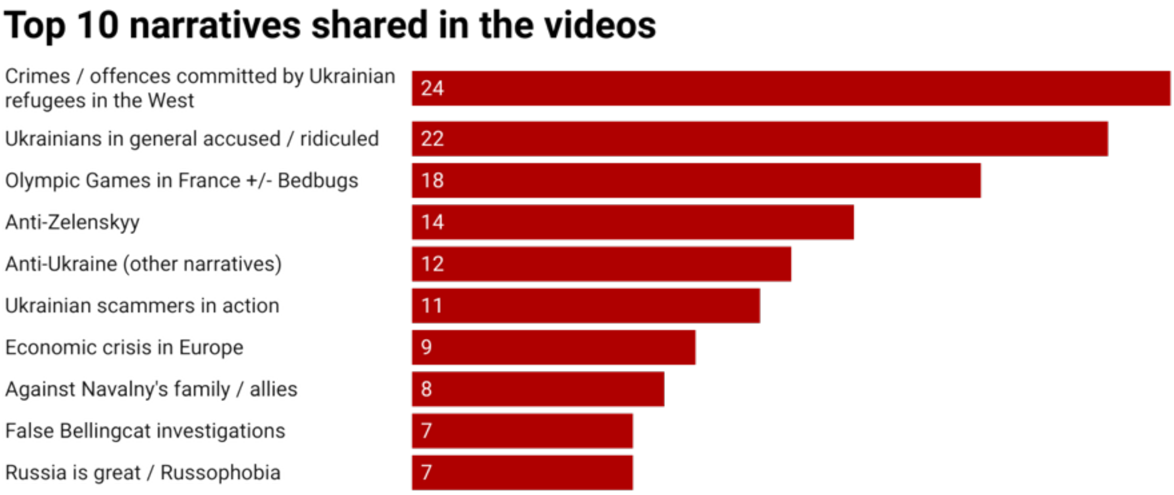


Chart 7: Top 10 narratives shared in the videos

5.2.8. Connection with real-world events

Similar to the email campaign, many of the stories depicted in the videos and graffiti are rooted in "reality anchors", or real-world events unfolding in parallel. The tactic to create content that coincides timely with actual events adds layers of depth to the narrative. Grounding the fictional stories in reality also increases their emotional impact. Blurring the lines between fictional and real confuses the audiences, additionally making the stories more challenging to debunk. The content also becomes psychologically relatable for the targeted audiences, as people can connect the fictional events to their own experiences or the broader cultural context.

The supposedly imminent bedbug epidemic in France promoted massively by the fake videos impersonating French media in April 2024 is a classic example of fear mongering rooted in reality. The narrative, albeit exaggerated, is based on actual facts: in 2023, French authorities have indeed been confronted[32] with an increasing number of bedbug infestations in the country.

[28] https://perma.cc/DXJ4-4KGR.
[29] https://perma.cc/6GH7-QJDF.
[30] https://perma.cc/2GXQ-7JGT.
[31] https://perma.cc/CT5P-MNCU.
[32] France to hold crisis meetings over 'scourge' of bedbugs https://www.france24.com/en/live-news/20231003-france-to-hold-crisis-meetings-on-bedbug-scourge.

Kremlin-aligned actors have since cunningly amplified this narrative[33] with the aim to deride France.

Another example of an actual event that spurred increased content production targeting France was President Macron's statement[34] about sending French military troops to Ukraine. The statement can explain the huge number of videos related to France in recent months, as well as the increase of graffiti photos mocking the French President or the First Lady.

The videos and graffiti are often produced in close proximity with real-world events, establishing a clear-cut connection between the fabricated content and the incident that prompted it. For example, immediately after the U.S. House of Representatives approved[35] military aid for Ukraine on April 21, the actors started disseminating stories aimed to undermine the U.S.: one video[36], branded with the logo of The New York Times and posted on April 22, claimed HAMAS had warned that weapons sent to Ukraine would end up with terrorists. Another video[37], attributed to Bloomberg and posted on April 23, linked rising U.S. arms industry prices to the country's support for Ukraine.

5.3. Telegram used as a cornerstone of the operation

The overwhelming majority of the links embedded in the emails sent to fact-checkers and newsrooms point to specific Telegram messages. In this section, we outline clear markers of coordinated inauthentic behaviour (CIB) by the analysed network of Telegram channels.

5.3.1 Context and approach

A Telegram channel provides two sources of information:

1. The channel metadata (e.g.: title and ID)
2. The channel's content (i.e. messages and users, if any)

We first focus on the content analysis, therefore the messages given the venues of interest are only channels.

Once the content is acquired, we perform an analysis by looking for cross-venue collisions[38]. We use this term to describe the following event: when a single Telegram account has administrative

[33] Bedbug panic was stoked by Russia, says France https://www.lemonde.fr/en/france/article/2024/03/01/bedbug-panic-was-stoked-by-russia-says-france_6575870_7.html.

[34] Macron still doesn't rule out sending troops to Ukraine | Euronews https://www.euronews.com/2024/03/15/macron-still-doesnt-rule-out-sending-troops-to-ukraine.

[35] The House passes billions in aid for Ukraine and Israel after months of struggle. Next is the Senate https://apnews.com/article/ukraine-aid-israel-tiktok-congress-a8910452e623413bf1da1e491d1d94ba.

[36] https://perma.cc/CJE7-U9D6.

[37] https://perma.cc/RYP2-E3WP.

[38] See annex 4

access to two different Telegram channels and sends each a message containing the same image, it creates a cross-venue collision[39].

After having identified the colliding messages, we analyse the channels' metadata. We first identify which Telegram server the image is stored on and then compare this information with the Telegram channel's picture. This helps us determine if a message was sent by the same Telegram account that created the channel.

Let's elaborate more on the nature of this broad attribution: if a media belongs to a specific Telegram storage server, and the same is valid for the Telegram channel's picture, it doesn't mean it was the owner who sent it. Likewise if the Telegram storage server assigned to the media differs from the one assigned to the Telegram channel's picture, we can conclude[40] that the administrator who sent the message is not the one who created[41] the channel.

This technique is more focused on excluding the creation of a channel by a Telegram account and possibly determining the presence of other mutual administrators, with the limit of not being completely accurate.

[39] We should not exclude the existence of false negatives, which by their nature cannot be identified.

[40] The analyst who conducted the research has never seen something in contradiction with this principle.

[41] We'd like to stress on the fact that ownership can be transferred anytime.

5.3.2 Colliding media analysis

We came to the conclusion that when Telegram compresses images it leaves traces, as a digital watermarking system would do, inevitably differentiating for each user the images uploaded to the Telegram storage server. This process creates a unique variation of the original image that can be spotted by conducting a noise analysis. This uniquely ties a specific image upload to a specific user. The following describes how we came to this conclusion.

Let's begin with the first two rows of the graffiti table, both pertaining to graffiti with ID number 5. Although they may appear identical to the human eye, they are actually different, both in terms of collision value and SHA fingerprint.

The media of the first row has SHA 256 equal to:
fbf7bb7fc3c1f3a7901e546d2cc28bedc81956bb85c5d5eaaa3f955060ad6a7f, whereas the

The second has SHA 256 equal to:
a30d7d691b5e18c80532abcee9cbd214eabb755bc2e7e049bd72d77bea1775e4.

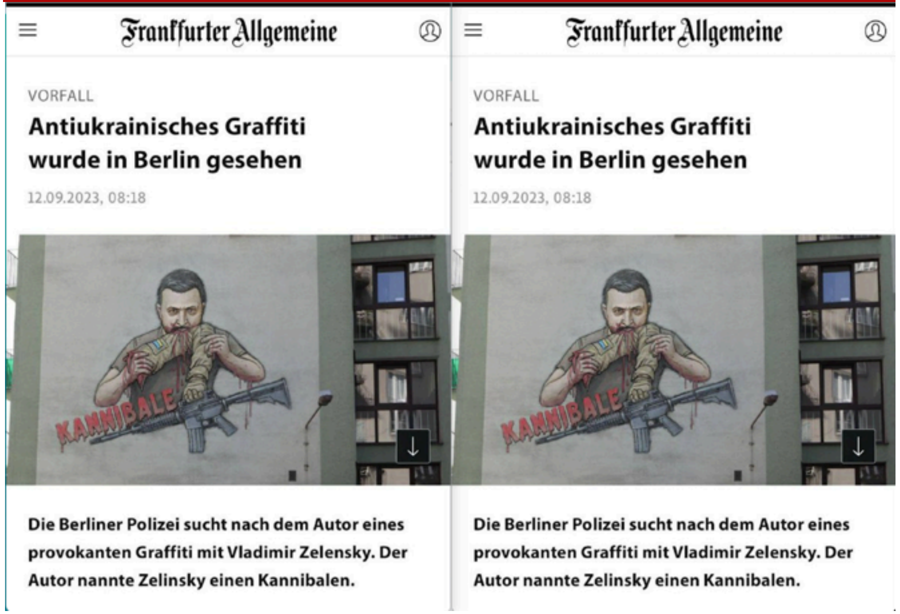
We may associate the discrepancy between the two due to one having different metadata than the other. After removing metadata from both images, we have the corresponding hashes:

- ce4ff63c44c7c33311b4f1aa74b9de9037958fcbac9f75a8c0d9e08a7a2f7169
- 983b134b2c26b56c282c36687457d275a1295878cdf78a88f805ca9439fad3c1

Still, they do not match. There must be a difference in terms of bits. To detect this, we conduct a Noise Analysis using the Forensically Beta[42] tool.

[42] Forensically, free online photo forensics tools - 29a.ch https://29a.ch/photo-forensics/.

Figure 9: Original images of the graffiti with ID 5. Image of the table's first row on the left, image of the table's second row on the right.



Frankfurter Allgemeine

VORFALL

Antiukrainisches Graffiti wurde in Berlin gesehen

12.09.2023, 08:18

Die Berliner Polizei sucht nach dem Autor eines provokanten Graffiti mit Vladimir Zelensky. Der Autor nannte Zelinsky einen Kannibalen.

Frankfurter Allgemeine

VORFALL

Antiukrainisches Graffiti wurde in Berlin gesehen

12.09.2023, 08:18

Die Berliner Polizei sucht nach dem Autor eines provokanten Graffiti mit Vladimir Zelensky. Der Autor nannte Zelinsky einen Kannibalen.

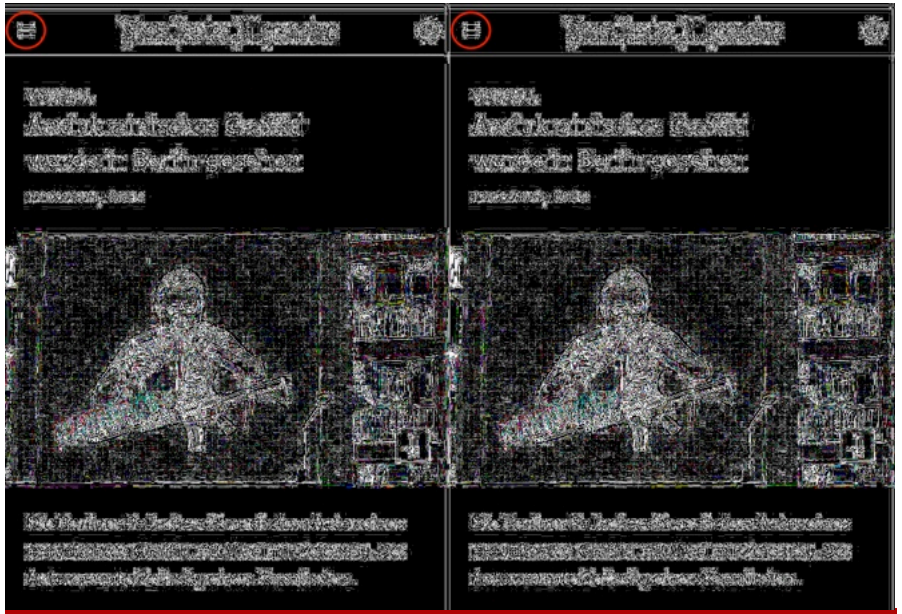


Figure 10: Noise present in the original images of the graffiti with ID 5. Image of the table's first row on the left, image of the table's second row on the right.

We may focus on a specific part of the image and spot little differences.

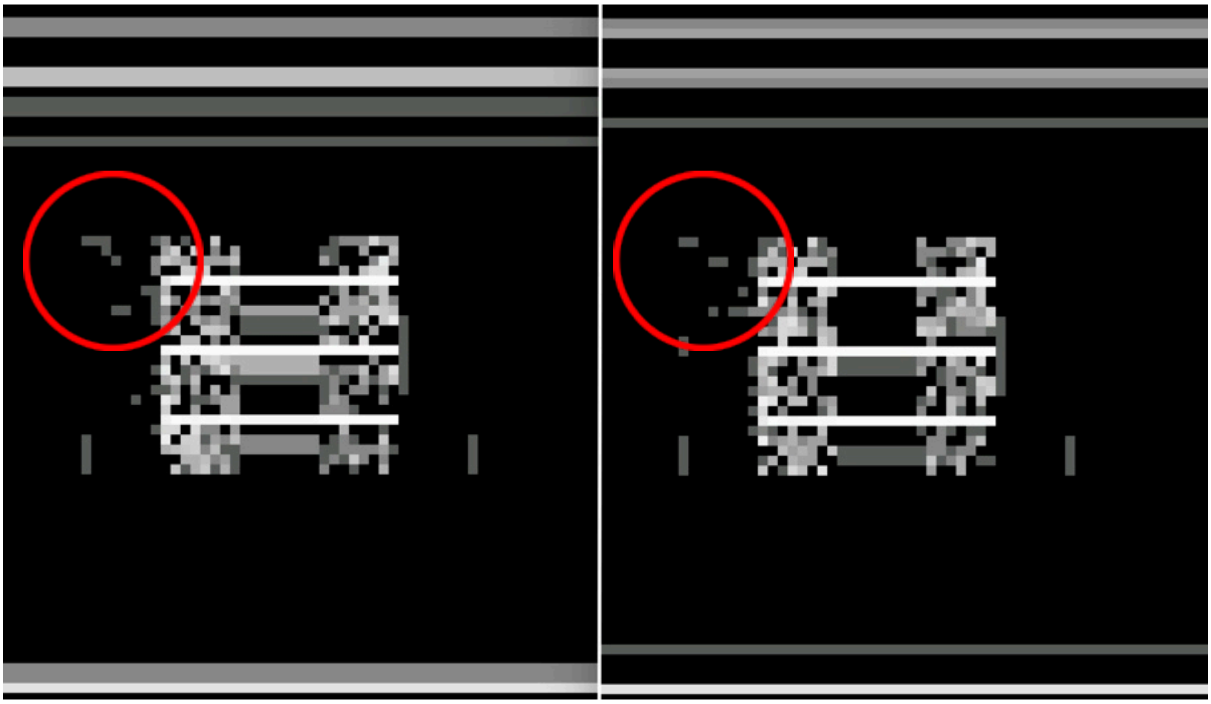


Figure 11: 7x zoom of the top left corner of the image reported above.

An interesting fact to note is that when we upload to Telegram an image which was already uploaded, regardless of the channel, Telegram does not actually create a new file. This is the main concept behind the collision principle: Telegram stores information about which Telegram account uploaded which media and when.

A more insightful fact comes to light when analysing the evidence about the graffiti with ID number 44. Again we have the same collision value and SHA fingerprint, so we are talking about the same media sent by one single Telegram account.

If we take a closer look at which Telegram storage servers were assigned to the graffiti images and the channel's one, we can observe an important clue. Only for the channel "*rus_criminaltg_voblya*" the Telegram storage server of the graffiti image matches with the channel picture's one.

Based on the evidence acquired, we state that the administrator who sent the message containing the media in question probably is not the principal administrator of neither "*pravdivostytg*" nor "*putin_intg*". These two channels have a different Telegram Storage server assigned to their channel's picture than the one assigned for the media. However, we should also consider the eventuality that it could actually be the creator of "*rus_criminaltg_voblya*" to be the multi-partisan administrator who sent the media also to the other two channels. From this standpoint, the situation is pretty vague due to the limited amount of intelligence currently available.

When we also consider the timestamp at which the messages were sent, we find that all actions occur within the span of a second. Coordinated inauthentic behaviour (CIB) activity is characterised by the repetition of a single action by different entities within a short period. In our analysis, we observed three channels sharing the same media within one second. Notably, the media was uploaded to Telegram for the first time approximately fifteen seconds before being shared on those channels.

This raises further questions about the first sender of the media, and where it was shared first.

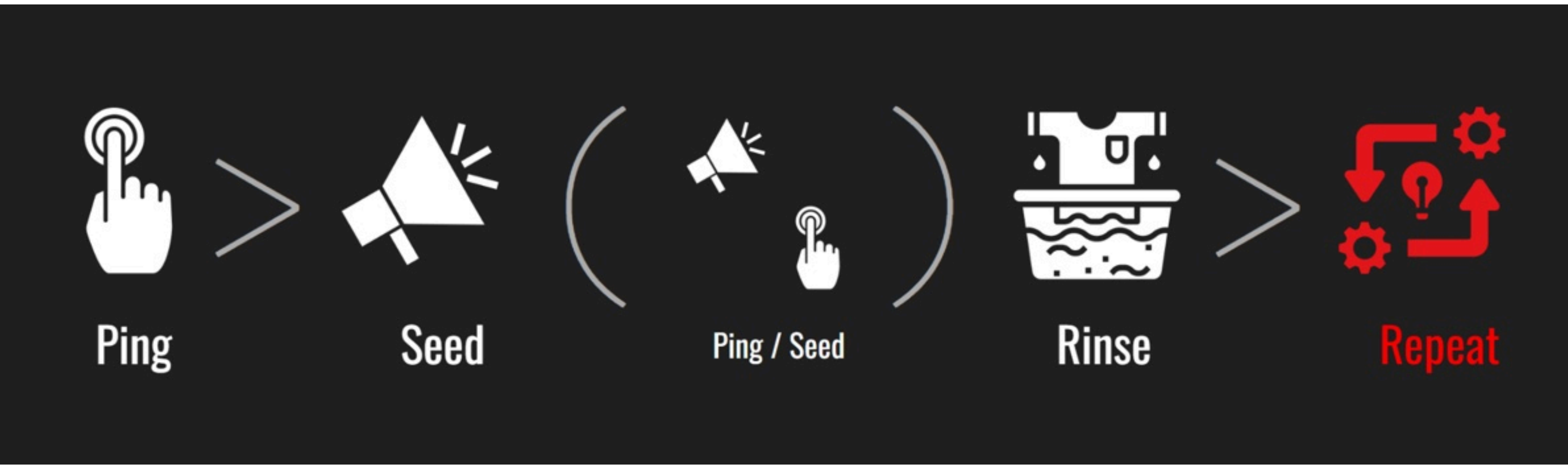
5.4. Amplification on X

The section explains the use of X as a platform of choice. We identified 100 accounts on X that had amplified the content since October 2023. Using external monitoring tools (Brandwatch, Meltwater), we obtained complete activity data for a sample of this network (35 accounts)[43].

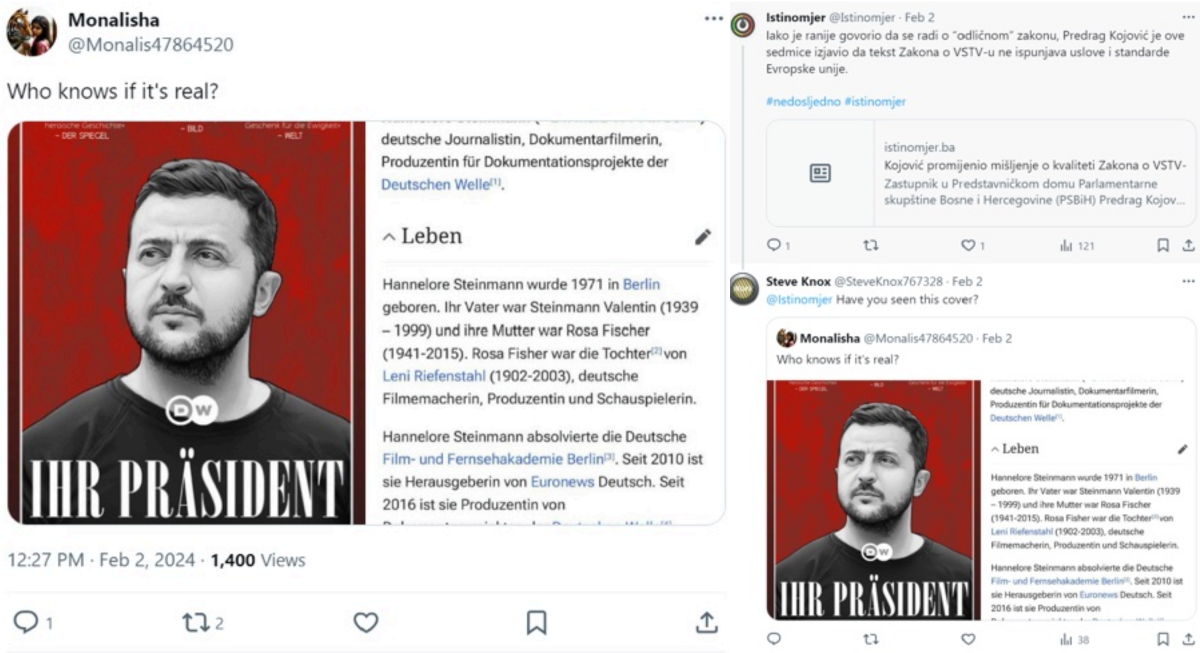
The analysed accounts exhibit clear markers of coordinated inauthentic behaviour (CIB). They are activated in pairs over a time span, and assigned specific roles in the amplification process, a tactic likely designed to minimise detection by the platform.

5.4.1. An easy formula: Ping>Seed>Rinse>Repeat

We identified two main phases of the accounts' activity: the seeding phase, during which one account shares fake content as a regular post, and the pinging phase, where another account shares the link to the original post in multiple replies to targeted accounts of fact-checkers, media, and various others. The roles of "seeders" and "pingers" fluctuate over time: one account can perform both roles, seeding one type of content while pinging another, with pauses between activities. We call this role-switching tactic "rinse and repeat." Most accounts become dormant after completing a full cycle of seeding/pinging phases.



[43] The sampling is partly due to X shadow banning some of the accounts, which hampered the monitoring tools from collecting data on their posting activity, and also to the fact that some accounts were suspended by the platform too swiftly and before we managed to collect their activity.



Monalisha @Monalis47864520

Who knows if it's real?

deutsche Journalistin, Dokumentarfilmerin, Produzentin für Dokumentationsprojekte der Deutschen Welle[1].

Leben

Hannelore Steinmann wurde 1971 in Berlin geboren. Ihr Vater war Steinmann Valentin (1939 – 1999) und ihre Mutter war Rosa Fischer (1941-2015). Rosa Fisher war die Tochter[2] von Leni Riefenstahl (1902-2003), deutsche Filmemacherin, Produzentin und Schauspielerin.

Hannelore Steinmann absolvierte die Deutsche Film- und Fernsehakademie Berlin[3]. Seit 2010 ist sie Herausgeberin von Euronews Deutsch. Seit 2016 ist sie Produzentin von

12:27 PM · Feb 2, 2024 · 1,400 Views

Istinomjer @Istinomjer · Feb 2

Iako je ranije govorio da se radi o "odličnom" zakonu, Predrag Kojović je ove sedmice izjavio da tekst Zakona o VSTV-u ne ispunjava uslove i standarde Evropske unije.

#nedosljedno #istinomjer

istinomjer.ba
Kojović promijenio mišljenje o kvaliteti Zakona o VSTV-
Zastupnik u Predstavničkom domu Parlamentarne skupštine Bosne i Hercegovine (PSBiH) Predrag Kojov...

Steve Knox @SteveKnox767328 · Feb 2

@Istinomjer Have you seen this cover?

Monalisha @Monalis47864520 · Feb 2

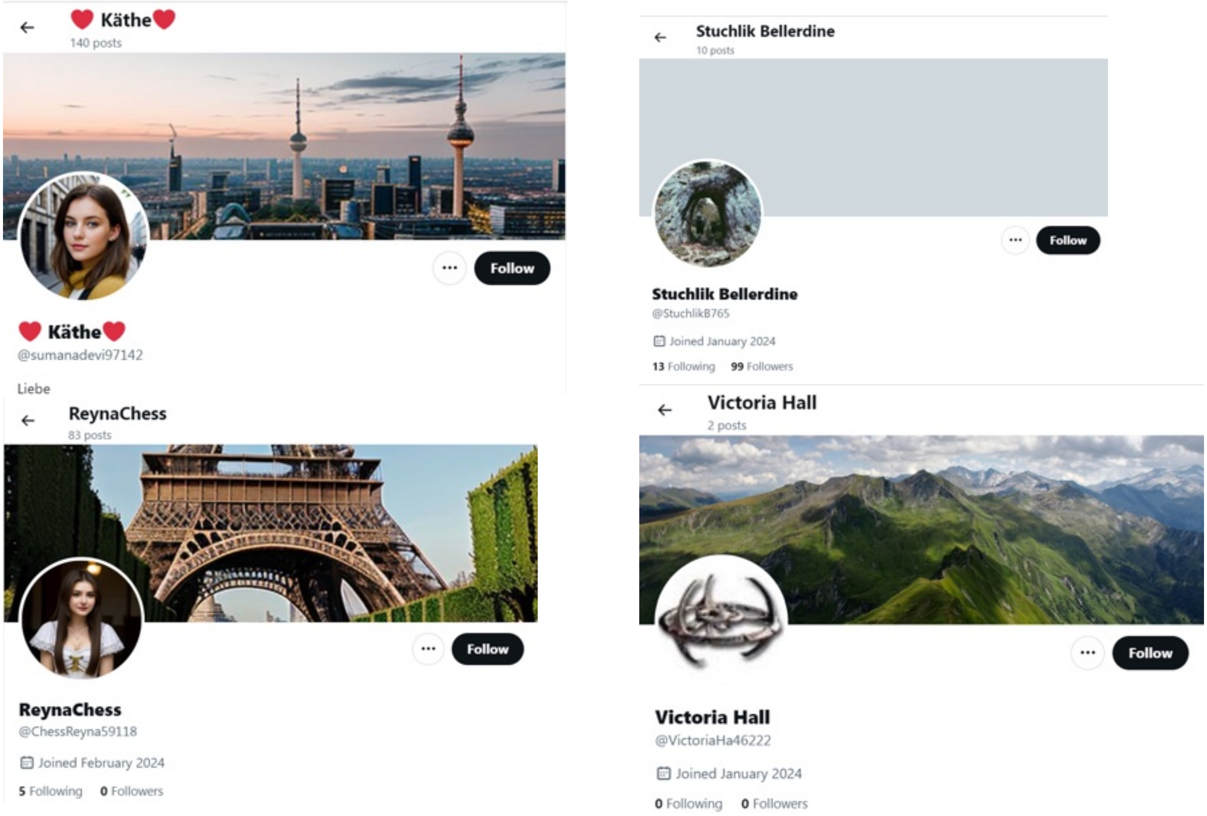
Who knows if it's real?

Figure 12: On February 2, the account @Monalis47864520 (seeder) posted a fake movie poster about Zelenskyy, allegedly produced by German media DW. A few hours later, another account, @SteveKnox767328 (pinger), began replying to posts from various X accounts, including @Istinomjer, a Bosnian fact-checking organisation. Within a few hours, @SteveKnox767328 posted 128 replies targeting over 140 organisations. Despite the evident pattern of coordinated inauthentic behaviour (CIB), both accounts remain active. Additionally, @Monalis47864520 was used to ping another fake story in November 2023, as seen in the reply section.

5.4.2. Two groups of accounts

The analysed amplifiers are all inauthentic accounts, predominantly anonymous or using stolen identities. They can be categorised in two groups: new accounts and re-purposed accounts. The new accounts are typically created just days or weeks before their activity began, evidently intended solely for the campaign. The older accounts are repurposed and display clear indicators of having been illegally expropriated from their previous owners. Seeders often create only one or two posts before becoming dormant or shifting their roles. Pingers, on the other hand, post multiple replies within short time spans and sometimes no other posting activity. Other accounts retweet content irrelevant to the campaign before being activated as either pingers or seeders.

The new accounts are mostly created in 2024 and show signs of automated creation. Many of these accounts use AI-generated images of individuals as profile photos. Some display clear patterns in their usernames (e.g., a personal name followed by a string of numbers). Judging from common username patterns, overlapping retweeting activity, and similar visual identity, it is evident that some of the analysed accounts belong to larger networks of automated X accounts. Additionally, some of the analysed accounts also promote different cryptocurrencies, implying that these may be assets activated for different campaigns. The current investigation does not go into further details around the broader ecosystem of inauthentic newly created accounts.



❤️ Käthe❤️
140 posts
❤️ Käthe❤️
@sumanadevi97142
Liebe

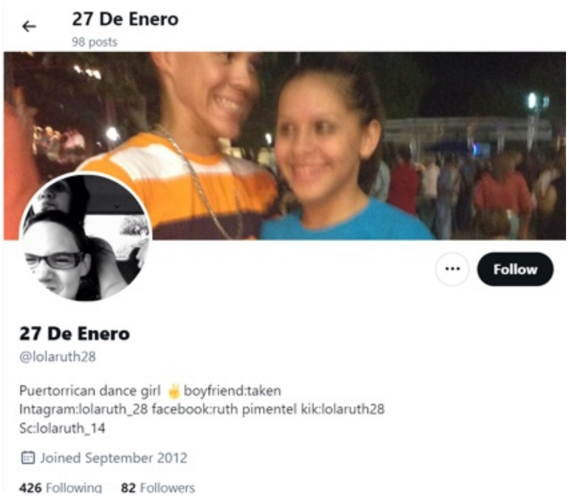
ReynaChess
83 posts
ReynaChess
@ChessReyna59118
Joined February 2024
5 Following 0 Followers

Stuchlik Bellerdine
10 posts
Stuchlik Bellerdine
@StuchlikB765
Joined January 2024
13 Following 99 Followers

Victoria Hall
2 posts
Victoria Hall
@VictoriaHa46222
Joined January 2024
0 Following 0 Followers

Figure 13: Anonymous newly created accounts (2024) used as pingers/seeders. All accounts are still active at the moment of writing of this report (May 2024). The account @sumanadevi97142 joined X in September 2023: in December 2023, it pinged one fake video to over 30 accounts. In February 2024, it seeded another video. The account has since become dormant. The account @VictotiaHa46222 was created in January 2024 and was used exclusively as a seeder: it posted only two videos on February 2 and February 21, 2024. The account @ChessReyna59118 joined X in February 2024: it was used as a pinger on March 4, and it seeded a video on March 18. The account @StuchlikB765 was created in January 2024. It was activated in March when it did a couple of irrelevant retweets and later pinged a fake video to 5 accounts. On March 8, it seeded one video.

The second group of X accounts used in the campaign consists of older, repurposed accounts, with some dating back to 2012-2013. There are clear indications that some of these accounts were hacked and repurposed for the campaign. This is evidenced by their older content remaining intact, as well as the authentic profile photos of individuals that were not changed. We identified at least 20 re-purposed accounts.



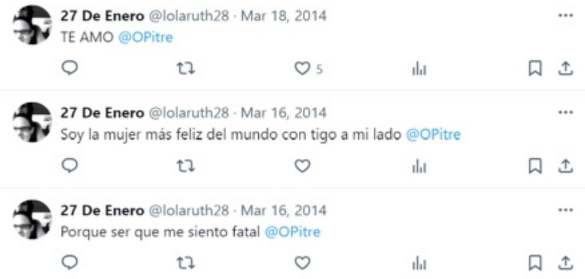
27 De Enero
98 posts

27 De Enero
@lolaruth28

Puertorrican dance girl ✌ boyfriend:taken
Intagram:lolaruth_28 facebook:ruth pimentel kik:lolaruth28
Sc:lolaruth_14

Joined September 2012

426 Following 82 Followers

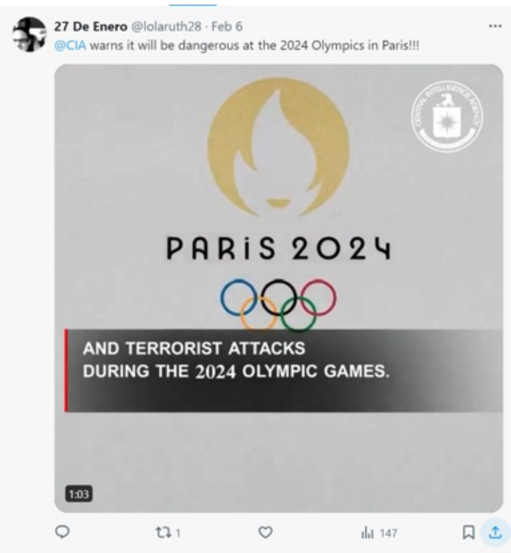


27 De Enero @lolaruth28 · Mar 18, 2014
TE AMO @OPitre

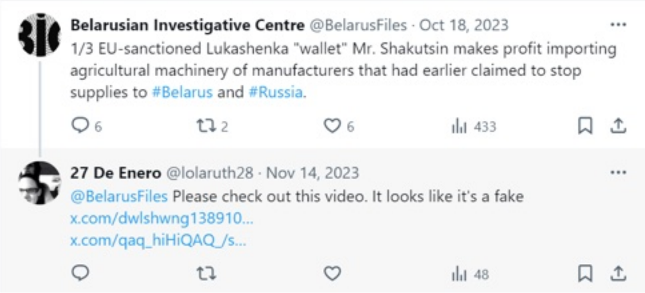
27 De Enero @lolaruth28 · Mar 16, 2014
Soy la mujer más feliz del mundo con tigo a mi lado @OPitre

27 De Enero @lolaruth28 · Mar 16, 2014
Porque ser que me siento fatal @OPitre

Fig. 14: (Left) One hacked account @lolaruth28 features a photo of a teenager from Puerto Rico. The bio seconts lists profiles with the same username on other platforms (Instagram, Facebook, Kik). Created in 2012, the account posted content in Spanish until March 2014, then remained dormant for nine years before being repurposed as a pinger/seeder in the disinformation campaign.



27 De Enero @lolaruth28 · Feb 6
@CIA warns it will be dangerous at the 2024 Olympics in Paris!!!



Belarusian Investigative Centre @BelarusFiles · Oct 18, 2023
1/3 EU-sanctioned Lukashenka "wallet" Mr. Shakutsin makes profit importing agricultural machinery of manufacturers that had earlier claimed to stop supplies to #Belarus and #Russia.

27 De Enero @lolaruth28 · Nov 14, 2023
@BelarusFiles Please check out this video. It looks like it's a fake
x.com/dwlshwng138910...
x.com/qaq_hiHiQAQ_/s...

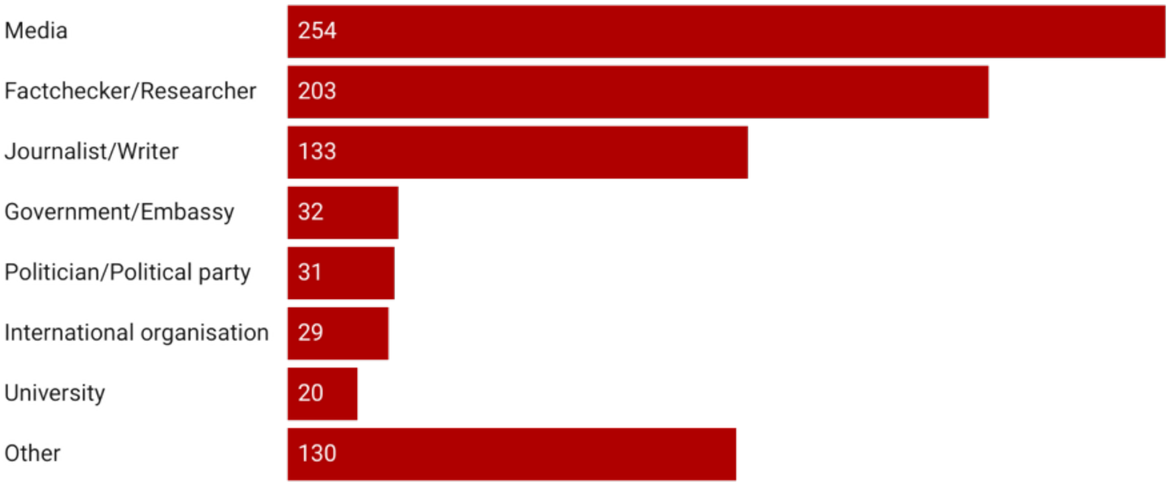
Fig. 15: (Left) The expropriated account @lolaruth28 was used to ping a video in November 2023. In February 2024, it seeded another video branded with the CIA logo. Despite this obvious inauthentic activity, the account remains active as of May 2024.

5.4.3. Targeted organisations

In total, the accounts of over 800 organisations from more than 75 countries were targeted by the network of pingers, including over 200 accounts belonging to fact-checking organisations. The chart below illustrates the number of targeted accounts by entity type.

Nearly 70% of the total accounts targeted in the campaign belong to journalists, news outlets, and fact-checkers, indicating that the operation's primary focus has been on media-related entities. Government accounts, along with accounts belonging to politicians, political parties, and international organisations such as the UN and the EU, comprise the second largest group of targeted entities. In the category "Other" we find mostly accounts of commercial companies, different associations, NGOs, as well as the so-called collaterals. These are accounts mentioned together with the targeted accounts due to the logic of the platform: for instance, when replying to a post on X, all accounts mentioned in the original post will also appear tagged in the reply.

Operation Overload: Who was Targeted on X?



Source: CheckFirst/Reset.Tech • Created with Datawrapper

Chart 8: Targeted accounts on X, by entity type

5.4.4. X's (in)action

Our findings show that X has taken inconsistent measures against the network of inauthentic accounts: while the platform has swiftly deactivated or temporarily blocked some of the accounts, others exhibiting the same patterns of activity remain open months after they were first used in the operation. More than half of the identified 100 accounts are still open. The accounts that are still active can potentially be re-used to amplify new content in a new activation cycle following the dormant phase.

6. Case studies

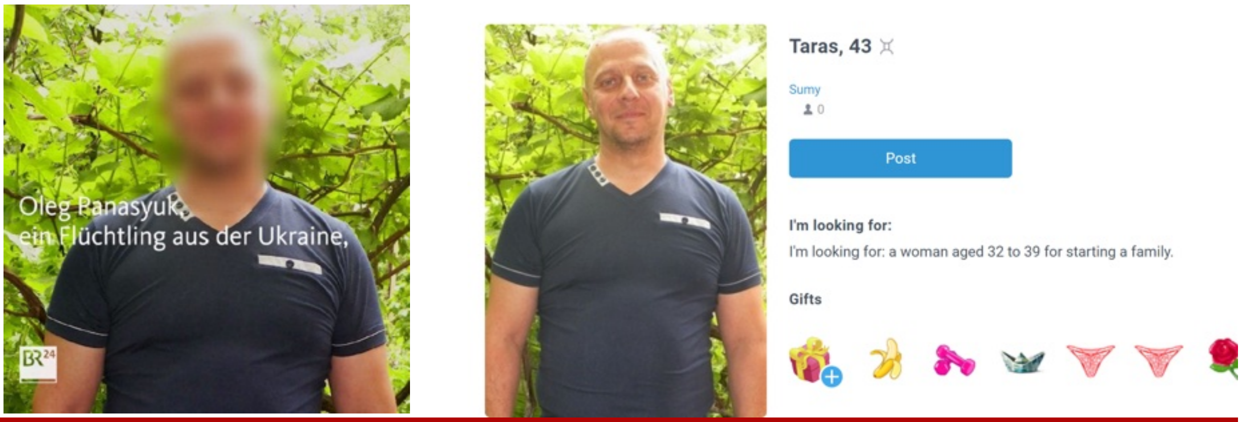
6.1. Video case studies

All of the analysed videos are made from old footage scavenged from YouTube and patched together to create a manipulative plot. We have observed numerous TTPs employed to lend validity and authenticity to the plots: impersonating real individuals, inventing characters, crafting complex stories with multiple characters, using fabricated letters, forged documents, and fake statements to validate claims, and introducing plot twists over time to reinforce the narratives in the public consciousness.

The archetype of the **angry, disgruntled, ridiculous or outright criminal Ukrainian refugee** living in the West is one of the leading narratives promoted by the videos. Many of these videos contain blurred photos of individuals with invented Ukrainian names. Others incorporate video footage featuring individuals who are not Ukrainian, with this footage taken directly from existing YouTube videos and easily traceable.

One example is of a video[44] falsely attributed to the German media BR24. The fabricated story ridicules a Ukrainian refugee who allegedly worked at the Berlin Aquarium, claiming he stole tropical fish from his workplace, cooked and ate it, and subsequently suffered food poisoning, leading to his hospitalisation. Within the frames of the video, a photo of the Ukrainian man, identified as Oleg Panasyuk, is presented. A reverse image search reveals that this photo was taken from a Russian dating website and features the profile of an individual based in Russia.

[44] Archived link to the fake video (shared on Telegram): https://perma.cc/NX7Q-WQ6A.



Taras, 43

Sumy

0

Post

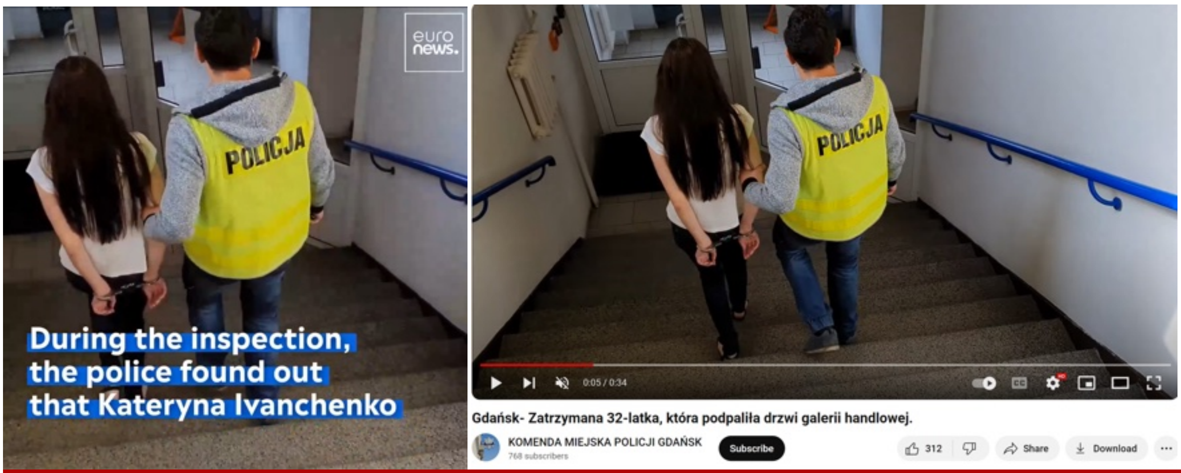
I'm looking for:

I'm looking for: a woman aged 32 to 39 for starting a family.

Gifts

Figure 16: (Left) A single frame extracted from the video attributed to BR24 showing the silhouette of a man with a blurred face. (Right) Reverse image search shows the photo exists on a personal profile of on the Russian dating website loveplanet.ru[45]

Another example of a video[46] falsely impersonating a Ukrainian refugee uses the logo of Euronews to spread the story that a Ukrainian woman named Kateryna Ivanchenko has established a beauty salon in Poland, where clients are purportedly exposed to mosquito bites as a weight loss method. A reverse image search shows that the footage was taken from a YouTube video[47] dating back to 2021. The original video depicts the arrest of a Polish woman in Gdansk, not the individual portrayed as a Ukrainian refugee in the fabricated narrative.



Gdańsk- Zatrzymana 32-latka, która podpaliła drzwi galerii handlowej.

KOMENDA MIEJSKA POLICJI GDAŃSK

768 subscribers

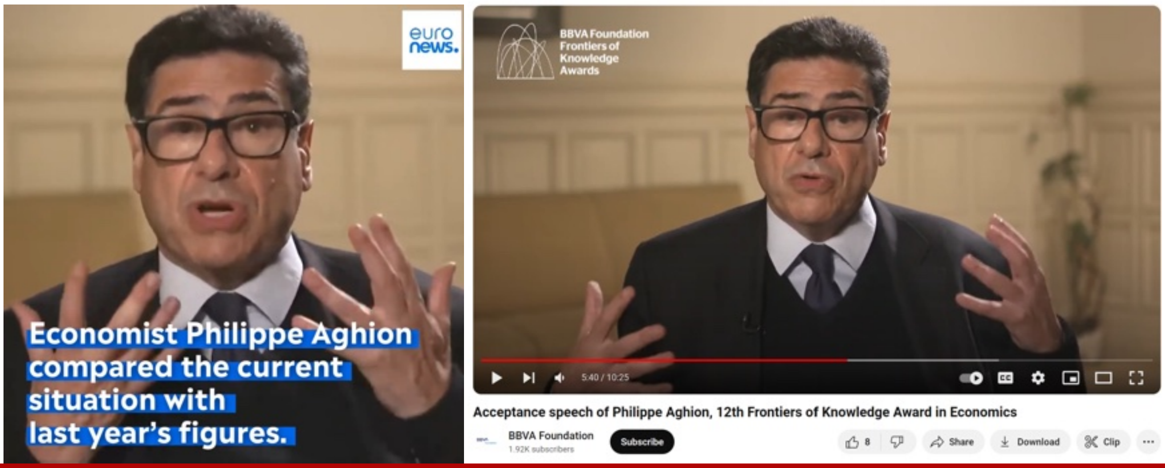
Figure 17: (Left) Footage from the video attributed to Euronews showing the arrest of the Ukrainian refugee. (Right) The original Youtube video published by the official channel of the City Police in Gdansk in 2021 and showing the arrest of a Polish individual.

[45] Archived link to loveplanet.ru: https://perma.cc/ZYD3-Q9QC .

[46] Archived link to the fake video (shared on VKontakte): https://perma.cc/JS3F-8JAH.

[47] Archived link to YouTube: https://perma.cc/9J9K-99R5.

A recurrent TTP used in the plots of the videos is the incorporation of existing footage from the **public appearances of prominent figures** in the West. For example, a video[48] attributed to Euronews on the topic a deepening economic crisis in France uses footage of a YouTube interview[49] with the French economist Philippe Aghion from 2022.



Economist Philippe Aghion compared the current situation with last year's figures.

Acceptance speech of Philippe Aghion, 12th Frontiers of Knowledge Award in Economics

Figure 18: (Left) Footage from a video attributed to Euronews featuring Phillippe Aghion. (Right) The original Youtube video with Aghion's interview published by the official channel of BBVA Foundation in 2022.

A distinct trend we observed over time is **the development of more complex plots**, incorporating an increasing number of impersonated individuals with the aim to make the stories more credible and harder to debunk. The impersonated individuals include well-known politicians, celebrities, athletes, businessmen, and journalists. These videos typically include at least two counterpoints, presented as "Opinion 1" and "Opinion 2". For example, one video[50], branded with the BBC logo, falsely quotes researchers from Bellingcat and NATO's former Secretary General Anders Fogh Rasmussen to fabricate the story that the Head of the Office of the President of Ukraine, Andriy Yermak, paid $27 million to be included in Time's Top 100.

[48] Archived link to the fake video (shared on Telegram): https://perma.cc/YQ4M-WVJD.
[49] Archived link to YouTube: https://perma.cc/59CA-NGLNchived.
[50] Archived link to the fake video (shared on Telegram): https://perma.cc/FVG7-UGKJ.

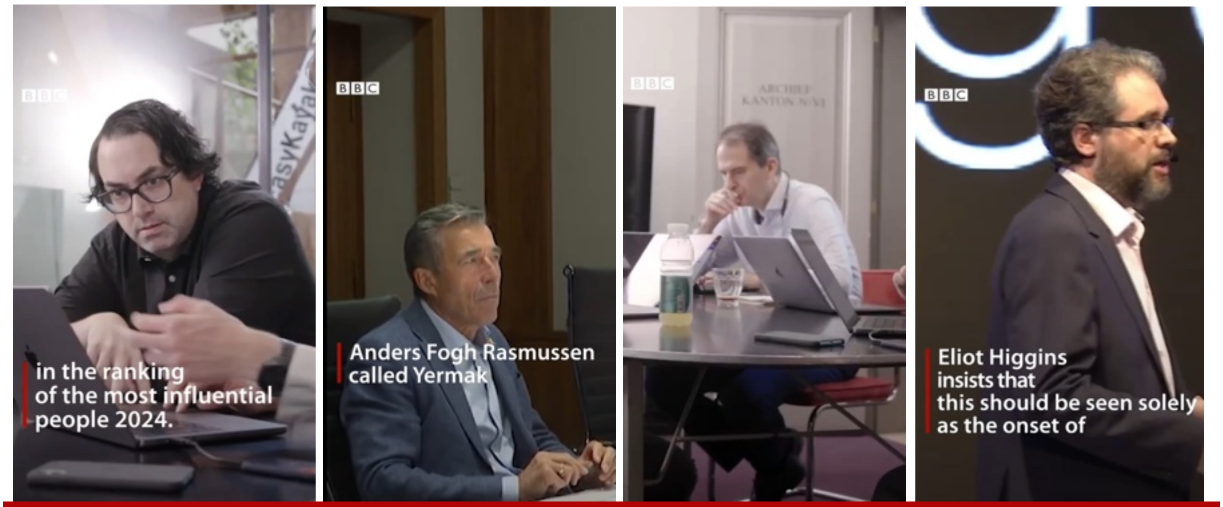
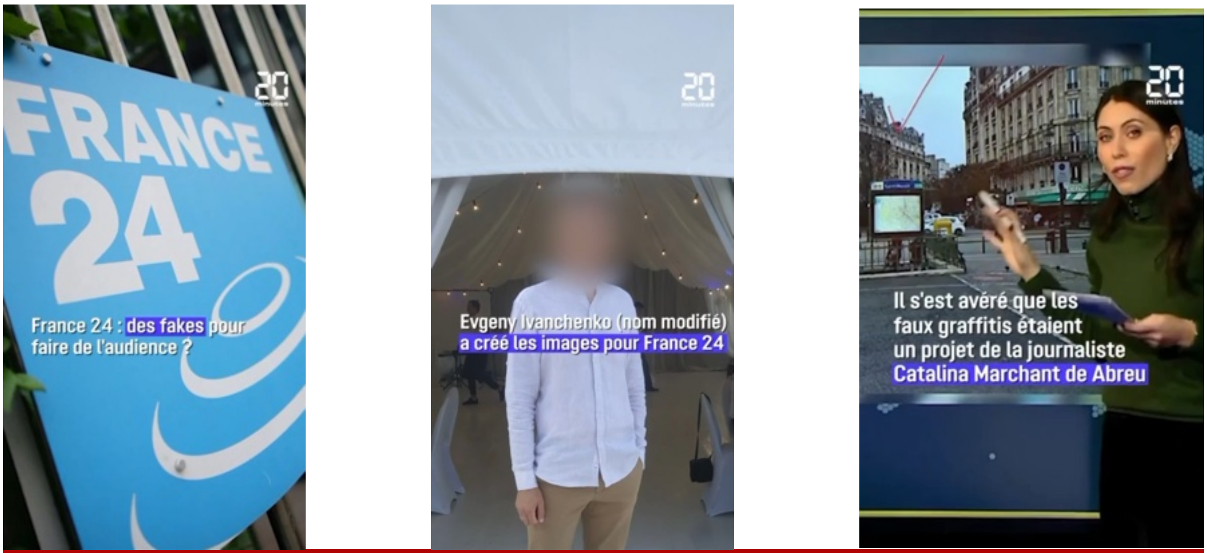


Figure 19: A video branded with the BBC logo promotes a fake story about Andriy Yermak, attributing false statements to various public figures, including Bellingcat researchers Eliot Higgins, Christo Grozev, Michael Colborne, and former NATO Secretary General Anders Fogh Rasmussen.

Many of the analysed videos unveil **fantastical and outright unimaginable plots**. For instance, a video[51] attributed to Al Jazeera claimed that a Ukrainian refugee set fire to a DNA testing centre because he was upset that his results showed he was only 8% Ukrainian. Another video[52] reports that 43% of schoolgirls in Germany between the ages of 14 and 16 consider prostitution as an option to earn money for their education. This story neglects the fact that education in Germany is free. Another video[53] attributed to Euronews claims that Bellingcat has uncovered evidence suggesting that the French President Macron was blackmailed by the US to escalate the conflict in Ukraine in order to prevent the leak of a sex tape.

Several videos present borderline delusional plots directly **targeting European fact-checkers** and researchers countering Russian disinformation. This video[54] attributed to the French media 20minutes makes the claim that Catalina Marchant De Abreu, the lead journalist of France24's fact-checking section, has commissioned the anti-Zelenskyy graffiti and paid a Ukrainian artist to paint them in Western cities so that she and her team could use the stories against Russia.

[51] Archived link to the fake video (shared on Telegram): https://perma.cc/MS7L-AT6U.
[52] Archived link to the fake video (shared on Telegram): https://perma.cc/DC5U-3LJX.
[53] Archived link to the fake video (shared on Telegram): https://perma.cc/8LHG-WN3Q.
[54] Archived link to the fake video (shared on Telegram): https://perma.cc/F5EF-AMRC.



France 24 : des fakes pour faire de l'audience ?

Evgeny Ivanchenko (nom modifié) a créé les images pour France 24

Il s'est avéré que les faux graffitis étaient un projet de la journaliste Catalina Marchant de Abreu

Figure 20: Unexpected plot twist: A video attributed to 20 minutes claims a French journalist paid a poor Ukrainian artist to paint anti-Zelenskyy graffiti so that France24 could later blame it on Russia.

A TTP we observed in many videos is the use of **fake reports, letters and documents** as external endorsements to fortify the validity of the narratives: e.g. a video[55] attributed to DW contains footage of a letter allegedly sent by the Director of the Auschwitz-Birkenau State Museum Piotr Cywiński inviting members of the Azov battalion to a WWII commemoration event.

Some of the videos are more professionally done, others appear to have been crafted hastily. One sloppy example[56] posted on Telegram in February added just a few additional fake screenshots to an original video published on the official YouTube[57] channel of DW. The fake video claims that European farmers protest against military support for Ukraine, while the original video makes no such statement.

The background music featured in certain videos could be traced back to Epidemic Sound, a global provider of royalty-free soundtracks. Additionally, a few videos were produced using the free video editor Wibbitz, while the creators inadvertently left the company's watermarked logo.

Some videos lack closing frames, while others include credits screens with the **names of journalists** supposedly involved in the report. For instance, 10 videos attributed to the French media outlets Le Figaro and RFI end with frames featuring the names of journalists working at both newsrooms. Featuring frames of names of actual individuals is a tactic to add additional veneer of credibility to the stories while misusing the names of media professionals.

[55] Archived link to the fake video (shared on VKontakte): https://perma.cc/8QZ6-XDL2.

[56] Archived link to the fake video (shared on Telegram): https://perma.cc/YEF2-FSHL.

[57] Farmers protests in Europe | DW News - YouTube https://www.youtube.com/shorts/soHeTmrPmiw.

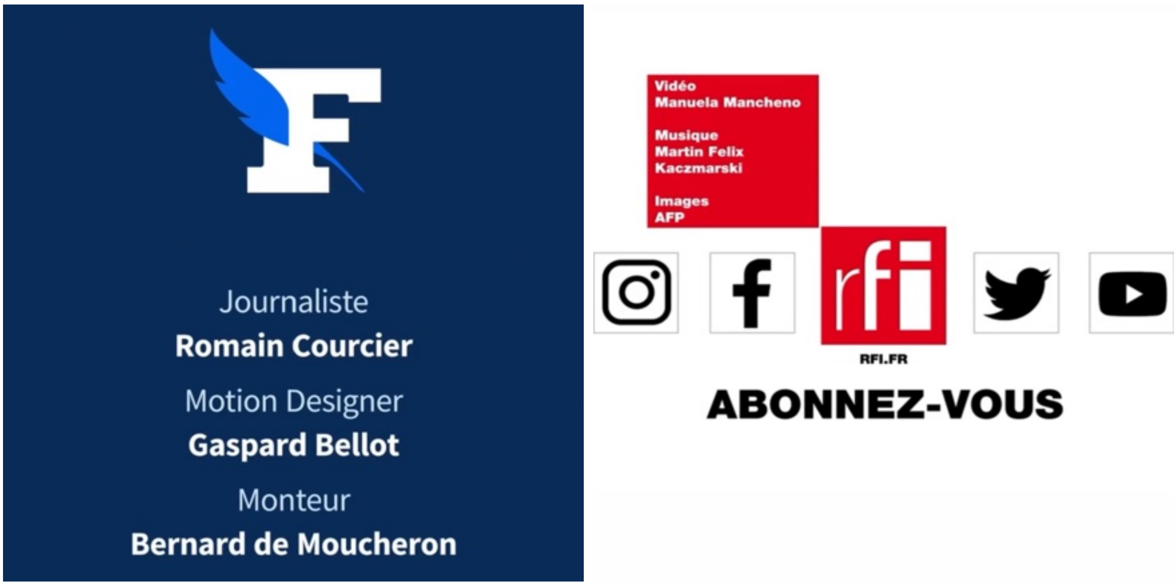


Figure 21: Romain Courcier, Gaspart Bellot, Bernard de Moucheron (Le Figaro), and Manuela Mancheno (RFI) are among the impersonated journalists and media workers credited for supposedly creating the fake videos.

The creators of these videos strategically and repeatedly expose viewers to the same false stories, exploiting the **illusory truth effect**— the human tendency to believe falsehoods after encountering them multiple times. This tactic, reinforced by producing a series of videos with minor plot twists, makes the narratives more challenging to debunk while embedding them in the public consciousness. For instance, videos about Ukrainian scammers targeting Israel are frequently circulated. In November 2023, a video[58] attributed to The Times of Israel claimed scammers extorted over $30 million, and in April, two videos from the same media alleged a $1.8 million[59] and $2 million[60] scams.

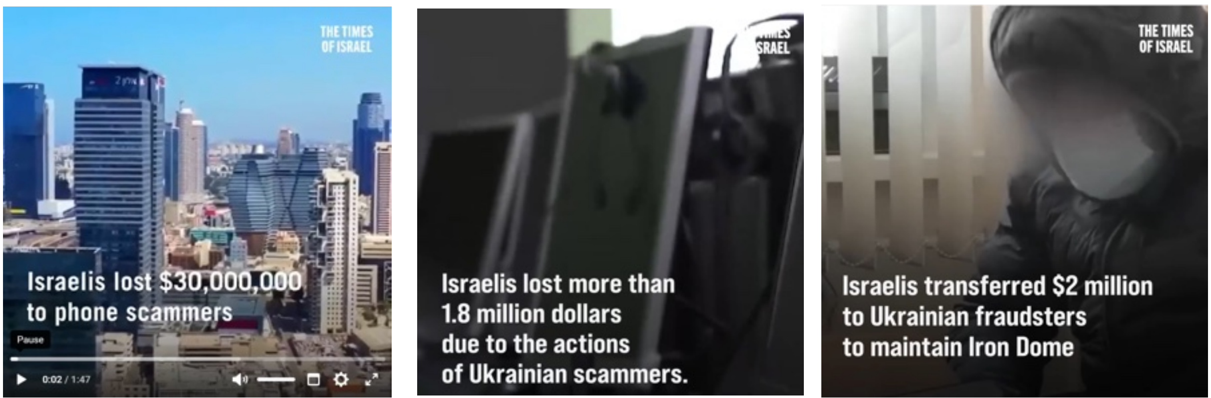

THE TIMES OF ISRAEL
Israelis lost $30,000,000 to phone scammers
Pause
0:02 / 1:47
THE TIMES OF ISRAEL
Israelis lost more than 1.8 million dollars due to the actions of Ukrainian scammers.
THE TIMES OF ISRAEL
Israelis transferred $2 million to Ukrainian fraudsters to maintain Iron Dome

Figure 22: Three videos falsely attributed by The Times of Israel aim to create an illusory truth effect by repeatedly exposing viewers to the narrative about Ukrainian scammers in Israel.

[58] Archived link to the fake video (shared on VKontakte): https://perma.cc/823P-9DVL.

[59] Archived link to the fake video (shared on Telegram): https://perma.cc/4TRU-2VWG.

[60] Archived link to the fake video (shared on Telegram): https://perma.cc/J4QP-WB9B.

6.2. Graffiti case studies

6.2.1. Imitating known artists

The following images of most likely fabricated graffiti were part of the false content sent via email to media outlets.

The mural depicts French President Emmanuel Macron on his knees, accompanied by a text reading “Thank God, there is Russia to which one can attribute all of France’s problems”. The graffiti is signed “LEKTO”. LEKTO is the pseudonym of the French street artist Léonard Petotte who was prosecuted (and discharged)[61] for an antisemitic mural in France, and is known for his proximity to conspiracy theorists.[62] However, forensics analysis made with the TruFor model show patterns of manipulation of the image around Macron’s face and the bottom-left signature.

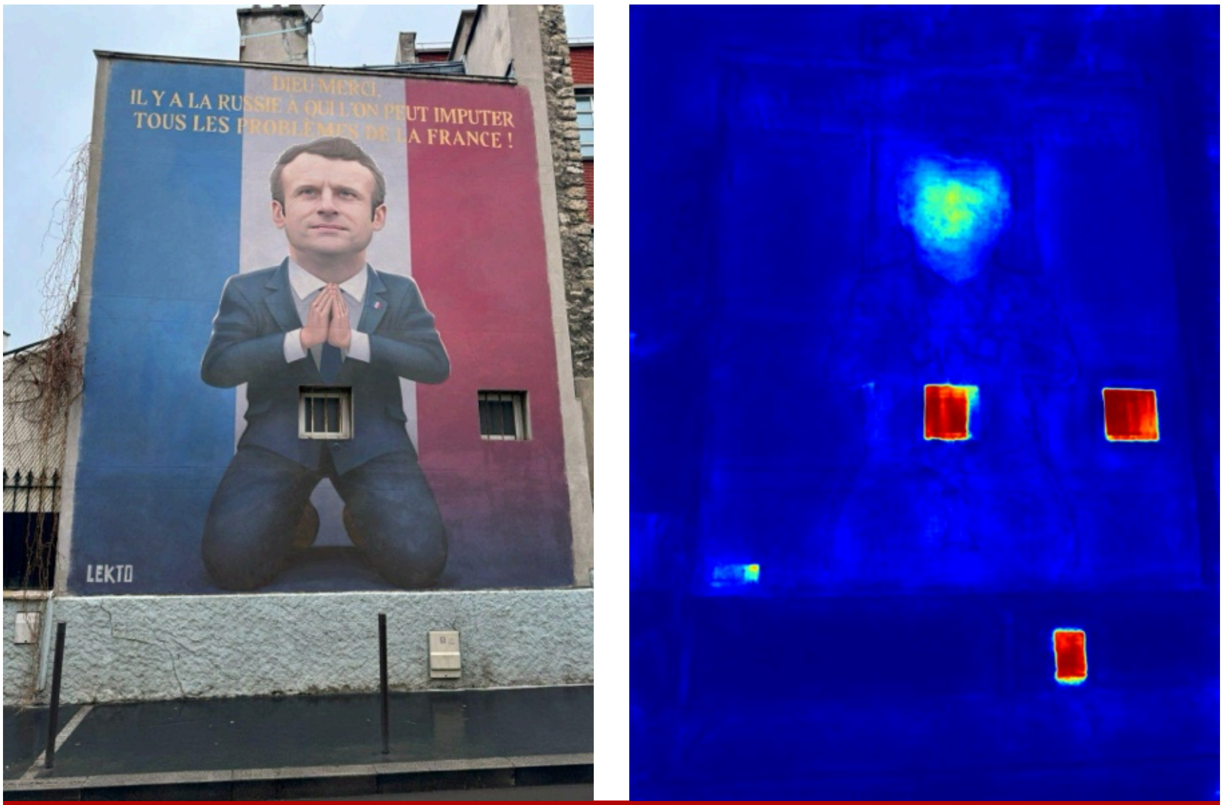

DIEU MERCI,
IL Y A LA RUSSIE A QUI L'ON PEUT IMPUTER
TOUS LES PROBLEMES DE LA FRANCE !
LEKTO

Figure 23: Left: original graffiti image, Right, COM-PRESS analysis with TruFor (heatmap)

[61] Avignon : le graffeur Lekto raille la justice après sa relaxe https://www.laprovence.com/article/region/2650751620710315/avignon-le-graffeur-lekto-raille-la-justice-apres-sa-relaxe.

[62] Lekto - Conspiracy Watch | L'Observatoire du conspirationnisme https://www.conspiracywatch.info/notice/lekto.

This example shows the perpetrators are well aware of local political and cultural context. The impersonation of an artist known for his proximity with conspiracy theorists would make the image of graffiti believable to a French national.

Another example of probable impersonation of an artist's work is the following photo, depicting Ukrainian President Volodomir Zelinskyy as a toddler screaming for money. The graffiti is made in the style of the French artist Blek le rat. The TruFor model shows clear signs of image manipulation on Zelenskyy's face.

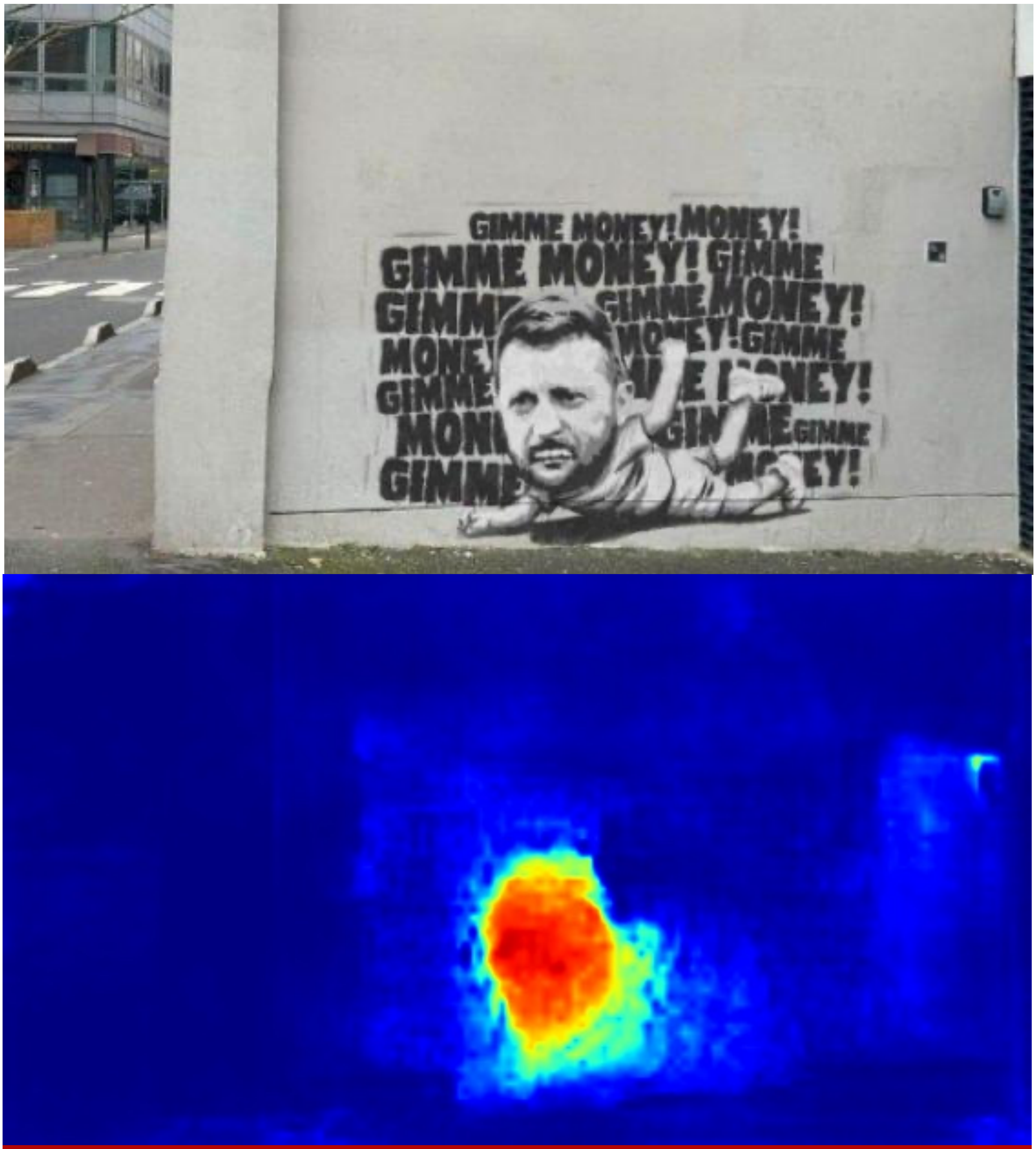


Figure 24: Top: original image, Bottom: COM-PRESS analysis with TruFor (heatmap)

6.2.2. Using memes

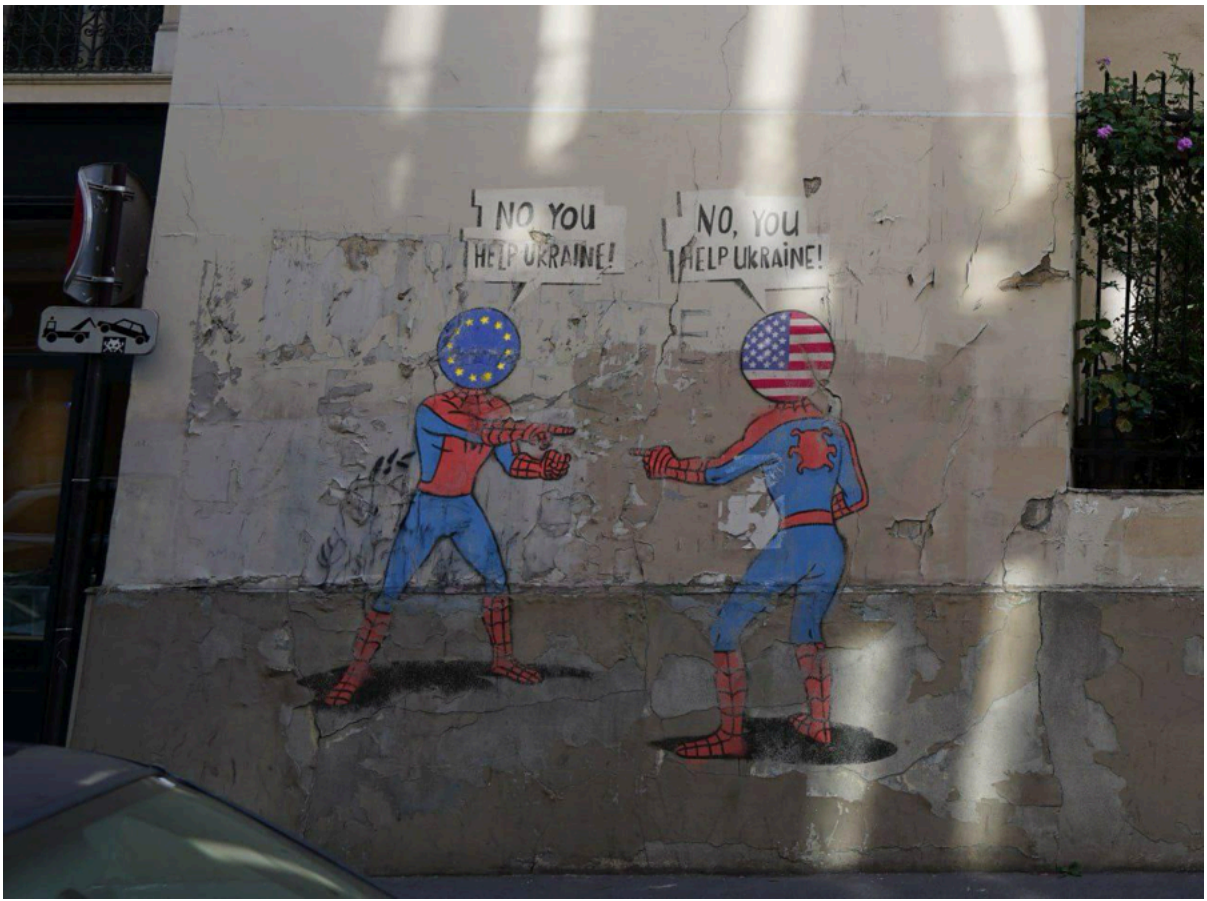


Figure 25: Image of a graffiti made in the style of a well-know Spiderman meme

The above example of a seemingly manipulated image shows the usage of a famous internet meme, the Spider-mans pointing fingers at each other (Figure 25). The meme[63], often used to illustrate confusion, is altered in this example, showing the characters bearing the European and American flags, each shouting "No, you help Ukraine". The graffiti exemplifies once again the ability of its authors to surf the news cycle as this picture was sent to newsrooms via email as debates arose both in Europe and the U.S. about the continuation of financially supporting Ukraine's war effort. The meme-like graffiti also recalls the now defunct Russian "Meme factory" or "Internet Research Agency" or "Glavset", a company linked to Yevgeny Prigozhin and specialised in the fabrication of propaganda social media content. The company was described as the "information warfare branch" by Lt Col Jarred Prier, USAF[64] and was active to create and spread fake content sometimes in the form of internet memes.[65]

[63] Spider-Man Pointing at Spider-Man | Know Your Meme https://knowyourmeme.com/memes/spider-man-pointing-at-spider-man.

[64] Strategic Studies Quarterly, Vol. 11, No. 4 (WINTER 2017), pp. 50-85.

[65] Exclusive: Russians Impersonated Real American Muslims to Stir Chaos on Facebook and Instagram http://www.thedailybeast.com/exclusive-russians-impersonated-real-american-muslims-to-stir-chaos-on-facebook-and-instagram.

6.2.3. Using pop culture references

This other example shows the ability of the perpetrators to quickly adapt to new narratives and use popular culture references to attempt to make their fake content more appealing to the audience. The image below was circulated via email on 9 May, just a few days after mainstream media in France reported on water quality concerns in the Seine, following a report by one NGO. Olympic Games swimming competitions will be held in the river.

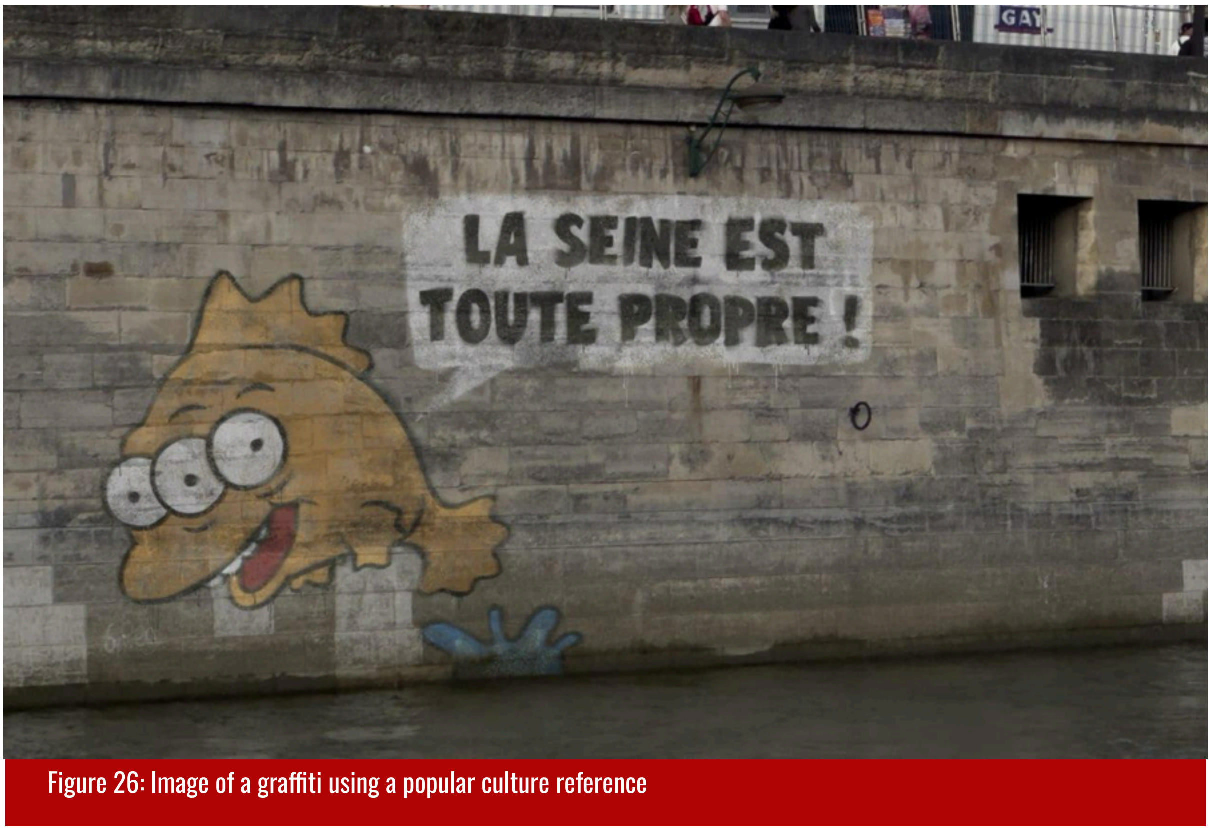


Figure 26: Image of a graffiti using a popular culture reference

Aside from the timing, which shows a clear intention to exploit the French newscycle, the seemingly manipulated image uses a popular culture reference. The three-eyed cartoon fish is drawn in the style of the TV series "The Simpsons" and is a reference to "Blinky", a fish character presented in the series as a product of the nuclear waste water of fictitious city Springfield's Nuclear power plant[66]. TruFor image analysis shows heavy signs of manipulation of this picture, clearly outlining the fish's silhouette.

[66] Blinky | Simpsons Wiki | Fandom https://simpsons.fandom.com/wiki/Blinky.

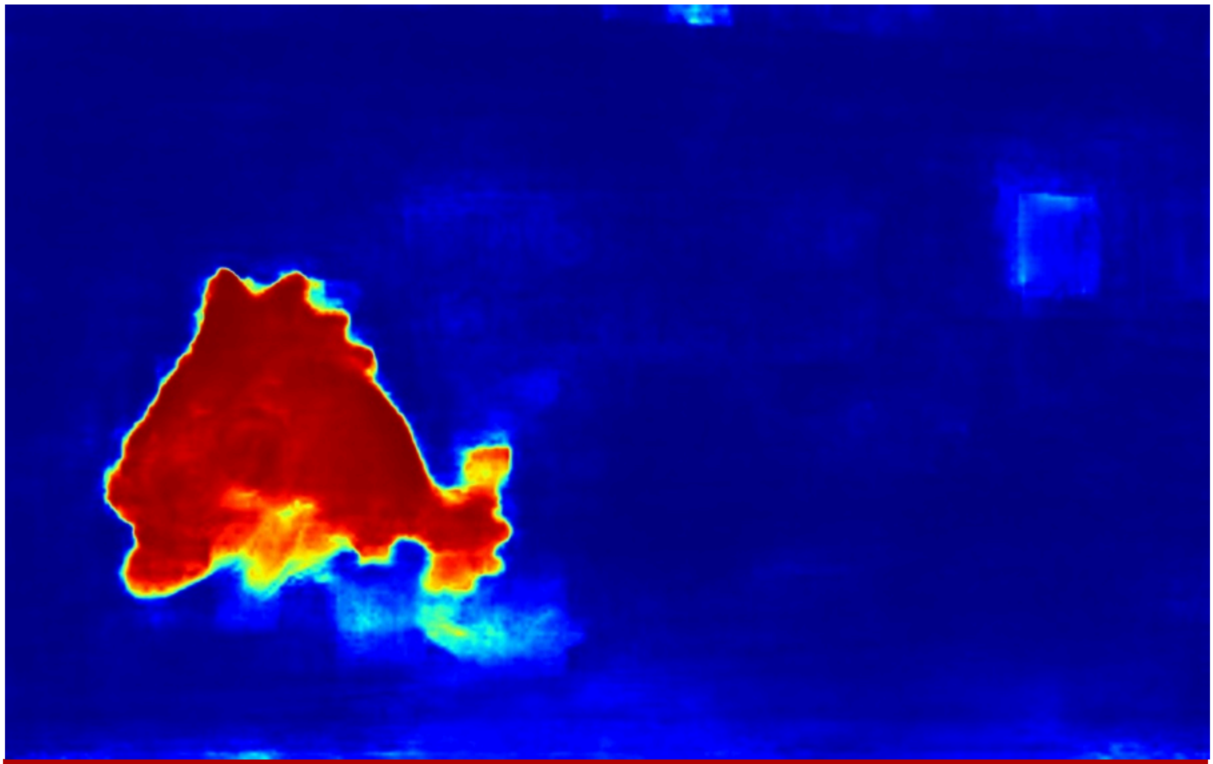


Figure 27: COM-PRESS analysis with TruFor showing signs of manipulation of the image in the area where the simpson fish is visible

7. Impact assessment

In this section, we aim to evaluate the impact of *Operation Overload* on the global fact-checking and research community throughout the monitored period. To achieve this, we collected articles published by legitimate fact-checking organisations that debunked the fake stories shared via email, focusing particularly on videos impersonating legitimate media and graffiti photos. Additionally, we gathered all coverage by reputable Western media reporting on these debunks.

For a sample of content pieces (comprising approximately 50 videos and graffiti images), we collected 250 articles linking to websites of fact-checking organisations and legitimate media outlets reporting on the fakes. This number would likely be at least two to three times higher, if we include the entire sample of fake content pieces that we collected.

In our analysis of the articles, we observed three distinct trends:

1) Fact-checking organisations from Eastern Europe and specifically Ukraine (STOPFAKE[67], Detector Media[68], Gwara[69], VOX Ukraine[70], Provereno Media[71]) have been among the most actively engaged in debunking stories since the onset of our monitoring in August 2023. Their sustained efforts persisted throughout the entire monitored period up to May 2024. This underscores the pivotal role of Eastern European fact-checking organisations in detecting and addressing disinformation that initially propagates within the Russian online ecosystem before reaching the West. It also highlights the need for closer cooperation and knowledge exchange between fact-checkers in Eastern and Western Europe.

2) Extensive media coverage of particular stories enhances their perceived validity (illusory truth effect) and amplifies their organic dissemination within the public domain. This phenomenon is compounded by the deliberate effort to create content intended to penetrate the Western informational landscape, utilising both reputable media outlets and accredited fact-checkers as conduits to reach broader audiences.

3) Fact-checking organisations exhibit a clear tendency to duplicate each other's efforts, with certain stories accumulating dozens of articles from various organisations and media outlets. While this may be rational from the perspective of media interest peaking around specific topics, it is a concerning trend in terms of the efficient use of research resources.

[67] StopFake | Struggle against fake information about events in Ukraine https://www.stopfake.org/en/main.
[68] Детектор медіа https://detector.media.
[69] Ґвара Медіа https://gwaramedia.com.
[70] VoxUkraine https://voxukraine.org/en.
[71] Проверено.Медиа https://provereno.media.

7.1. Operation Overload’s goals in a nutshell

Strategic Submission:

- Deliberately submit controversial or false information to fact-checkers and media.
- Aim for these entities to cover the content, spreading it further — even if debunked.

Amplification Through Controversy:

- Utilise the ensuing debate and media coverage to increase visibility of the narrative.
- Public discussion, even in the context of debunking, serves to publicise the false claims.

Exploiting the Streisand Effect: Trigger this phenomenon where attempts to debunk or censor information only increase its exposure.

Credibility Baiting: Use nuanced conclusions from fact-checkers (e.g., "partially true") to claim credibility for misleading campaigns.

Distracting Fact-Checkers: Overload fact-checkers with trivial or misleading claims to delay or dilute responses to more significant misinformation.

7.2. Recommendations to fact-checkers and journalists

Based on our findings and the intricacies of operations sur as Overload, the authors would like to make some recommendations to media professionals to help them recognise similar tactics and avoid becoming victims of adversarial operatives. Early detection, collaboration and reporting of such manipulation attempts are key to impede them.

Stay vigilant: When receiving emails or DMs, especially when alluding to "Kremlin propaganda", be wary of unsolicited emails and direct messages that contain links or attachments related to Ukraine, Russia, or other politically sensitive topics. Be particularly wary of unknown contacts. Verify the sender's identity and cross-check with known contacts or official channels before engaging with the content.

Coordinate with others: Keep a record of suspicious emails and DMs to identify patterns and potential coordinated efforts. Share this information with other fact-checkers and journalists to enhance collective awareness and response. Joining or monitoring established networks with other fact-checkers and journalists can be very useful to share insights and strategies for dealing with targeted disinformation campaigns. Collaborative efforts can accelerate the detection of coordinated campaigns.

Use the resources of your organisation: Report suspicious emails and DMs to your organisation’s IT department (if you have one) or relevant authorities to help track and mitigate these threats. Encourage your organisation to invest in cybersecurity training for all staff members to recognize and handle potential threats. Report suspicious accounts and DMs to platforms.

Prepare for Content Amalgamation Tactics: Train your team to recognise content amalgamation, where different types of manipulated content are combined to create a more convincing false narrative. This includes understanding how related videos, images, and text can be spotted on multiple dubious outlets or posted by suspect accounts on social media.

8. Conclusion

Operation Overload stands out as an incredibly intricate campaign due to its omnipresence, extensive outreach, and significant impact. Coordinated across multiple layers using a variety of TTPs, the campaign aims to amplify false narratives, sow discord, create confusion, and polarise public opinion on Ukraine, all in service of the Kremlin's political agenda. With over 250 pieces of manipulated content, the campaign's intensity is marked by frequent, well-coordinated attacks, especially during key events in Europe. Sophisticated tactics such as content amalgamation and media impersonation further enhance the campaign's credibility and effectiveness.

While our efforts concentrated on exposing the different layers of the campaign, we did not cover the complete amplification across all platforms and websites. We focused on revealing the strategies used on key platforms like Telegram and X, zooming in on the most active clusters of accounts/channels. Assessing the total amplification across different platforms opens avenues for future research, such as investigating the role of known pro-Kremlin websites in amplifying the narratives to both local and Western audiences, or analysing the broader underlying ecosystems on X and Telegram.

We consider the breaking scale of Operation Overload is **high** due to its extensive reach and impact. Targeting over 800 organisations, including fact-checkers, newsrooms, and researchers in Western nations like France and Germany, the operation uses platforms like Telegram and X (formerly Twitter) to spread false narratives. With over 250 pieces of manipulated content, the campaign's intensity is marked by frequent, well-coordinated attacks, especially during key events like protests. At the time of writing, this undertaking is still ongoing and this report cannot be considered as an exhaustive piece on the operation. Sophisticated techniques, such as content amalgamation and media impersonation, enhance the campaign's credibility and effectiveness. This disinformation effort strains the resources of fact-checkers and journalists, sows discord, creates confusion, and polarises public opinion. Fear-mongering tactics further amplify public anxiety and distrust.

9. Annexes

9.1. Review Process

This document has been reviewed by two external reviewers qualified in the field of the research. The process assessment grid used by the reviewers is available on Check First's website[72].

The external reviewers for this document are :

- Team Leader at VIGINUM
- Executive at EU DisinfoLab

This document has scored 86,11 out of 100 after review.

9.2. Google's review

As *Operation Overload* is mainly using Gmail addresses we reached out to Google's security Team (Mandiant) with our findings. After review here's their comment :

"*Recent research into Operation Overload information operations campaign underscores the value of maintaining open conversations through public research within the community of defenders against information operations and disinformation. This work builds on previous analysis to more fully expose the extent of an IO campaign that appears to be specifically targeting fact checkers and the journalist community. Documenting the unique combination of TTPs leveraged by an actor is essential to tracking and defending against those threats. Capturing vectors of direct dissemination, such as email, is inherently more challenging than other types of activity, but it can provide critical information not only about how content is being promoted but also about the intended audience.*

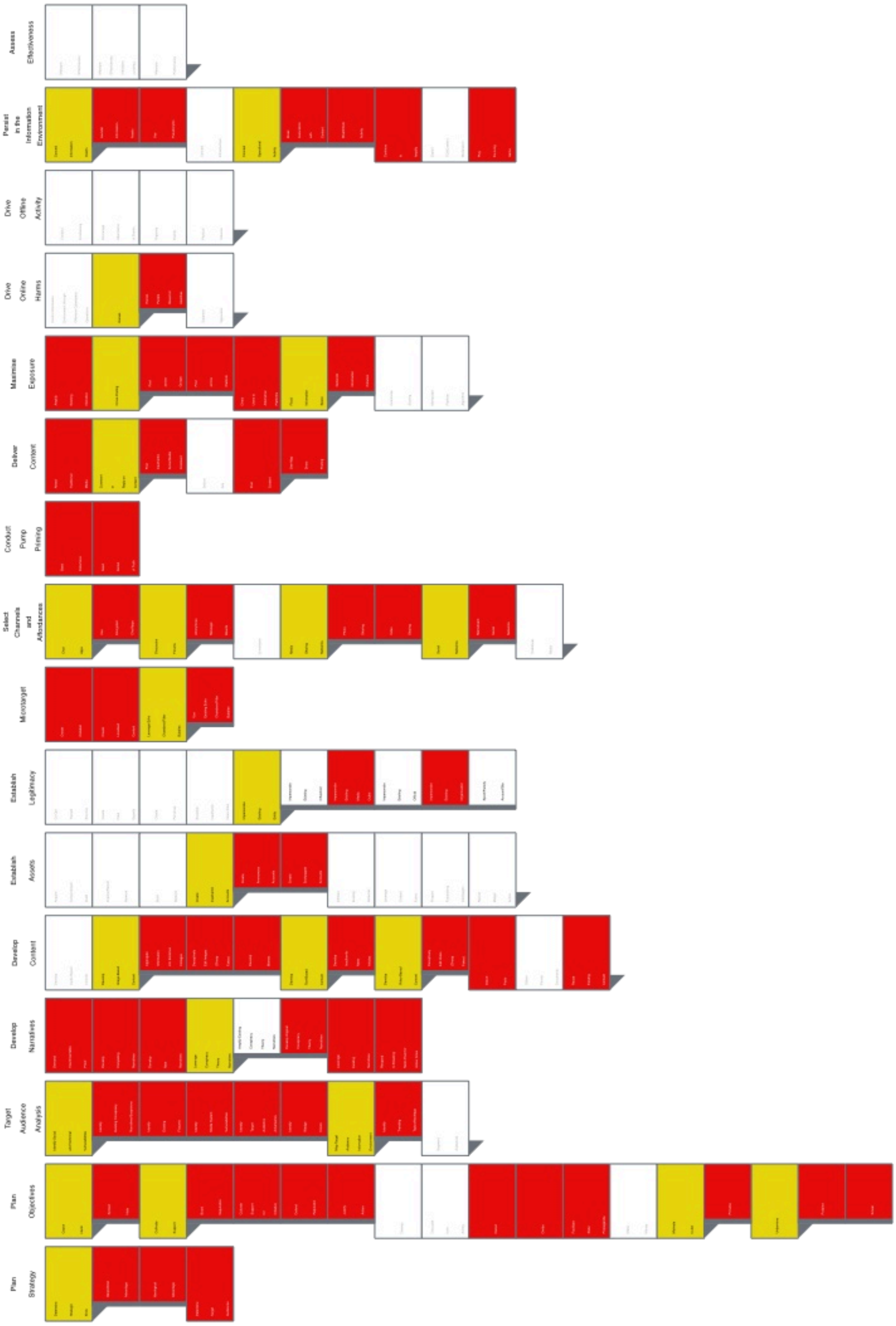
Additionally, this research highlights a narrative trend in Russia-aligned IO that is consistent with what Mandiant has observed in activity that we track. While Russia's war in Ukraine remains a clear and consistent priority, more than two years into the war, Russia-aligned IO has begun to re-expand its narrative scope to target major events, such as the upcoming Paris Olympics, both in relation to Russian interests vis-a-vis Ukraine and potentially also to other independent Russian strategic objectives." - **Alden Wahlstrom, Mandiant Principal Analyst - Google Cloud**

[72] CheckFirst - Operation investigation assesment https://docs.google.com/spreadsheets/d/1ka2rcMAmiUgDKIiTxXNS5cB0poax8C-GCC2Gl1_sRmY/edit#gid=0.

9.3. Archiving policy

All the assets captured by Check First and Reset.Tech were archived and are available upon request at info@checkfirst.network

9.4. Annex 1: DISARM



DISARM TTPs	
Plan Strategy	
	TA01: Plan Strategy
	T0074.001: Geopolitical Advantage
	T0074.004: Ideological Advantage
	T0073: Determine Target Audiences
Plan Objectives	
	T0140: Cause Harm
	T0140.003: Spread Hate
	T0136: Cultivate Support
	T0136.001: Defend Reputation
	T0136.002: Justify Action
	T0136.004: Boost Reputation
	T0136.005: Cultivate Support for Initiative
	T0076: Distort
	T0079: Divide
	T0002: Facilitate State Propaganda
	T0138: Motivate to Act
	T0138.002: Provoke
	T0135: Undermine
	T0135.001: Smear
	T0135.004: Polarise
Target Audience Analysis	
	T0081: Identify Social and Technical Vulnerabilities
	T0081.004: Identify Existing Fissures
	T0081.005: Identify Existing Conspiracy

	Narratives/Suspicions
	T0081.006: Identify Wedge Issues
	T0081.007: Identify Target Audience Adversaries
	T0081.008: Identify Media System Vulnerabilities
	T0080: Map Target Audience Information Environment
	T0080.003: Identify Trending Topics/Hashtags
Develop Narratives	
	T0040: Demand Insurmountable Proof
	T0004: Develop Competing Narratives
	T0082: Develop New Narratives
	T0022: Leverage Conspiracy Theory Narratives
	T0022.002: Develop Original Conspiracy Theory Narratives
	T0003: Leverage Existing Narratives
	T0068: Respond to Breaking News Event or Active Crisis
Develop Content	
	T0086: Develop Image-Based Content
	T0086.001: Develop Memes
	T0086.003: Deceptively Edit Images (Cheap Fakes)
	T0086.004: Aggregate Information into Evidence Collages
	[New TTP Proposal]: Fake Graffiti
	T0085: Develop Text-Based Content
	T0085.001: Develop AI-Generated Text
	T0085.003: Develop Inauthentic News Articles
	T0087: Develop Video-Based Content

	T0087.002: Deceptively Edit Video (Cheap Fakes)
	T0023: Distort Facts
	T0084: Reuse Existing Content
	[New TTP Proposal]: Content Amalgamation
Establish Assets	
	T0090: Create Inauthentic Accounts
	T0090.001: Create Anonymous Accounts
	T0090.004: Create Sockpuppet Accounts
Establish Legitimacy	
	T0099: Impersonate Existing Entity
	T0099.003: Impersonate Existing Organisation
	T0099.004: Impersonate Existing Media Outlet
Microtarget	
	T0101: Create Localised Content
	T0016: Create Clickbait
	T0102: Leverage Echo Chambers/Filter Bubbles
	T0102.001: Use Existing Echo Chambers/Filter Bubbles
Select Channels and Affordances	T0043: Chat Apps
	T0043.001: Use Encrypted Chat Apps
	T0106: Discussion Forums
	T0106.001: Anonymous Message Boards
	T0115: Post Content
	T0115.003: One-Way Direct Posting
Conduct Pump Priming	
	T0044: Seed Distortions

	T0042: Seed Kernel of Truth
Deliver Content	
	T0117: Attract Traditional Media
	T0116: Comment or Reply on Content
	T0116.001: Post Inauthentic Social Media Comment
Maximise Exposure	
	T0118: Amplify Existing Narrative
	T0119: Cross-Posting
	T0119.001: Post across Groups
	T0119.002: Post across Platform
	T0122: Direct Users to Alternative Platforms
	T0049: Flood Information Space
	T0049.008: Generate Information Pollution
Drive Online Harms	
	T0048: Harass
	T0048.002: Harass People Based on Identities
Persist in the Information Environment	
	T0128: Conceal Information Assets
	T0128.001: Use Pseudonyms
	T0128.004: Launder Information Assets
	T0129: Conceal Operational Activity
	T0129.010: Misattribute Activity
	T0129.003: Break Association with Content
	T0060: Continue to Amplify
	T0059: Play the Long Game

9.5. Annex 2: ABCDE Framework

A: Actor

Actors Involved:

- **Primary Actors:** The operation is primarily orchestrated by actors aligned with Russian interests. These include networks of accounts on platforms like Telegram and X (formerly Twitter), and an ecosystem of Russia-aligned websites.
- **Affiliations:** These actors are likely affiliated with or supported by Russian state mechanisms or pro-Kremlin groups.

B: Behaviour

Activities Exhibited:

- **Coordination:** Clear markers of coordinated inauthentic behaviour (CIB) are evident, particularly on social media platforms like X.
- **Techniques:** The operation employs tactics such as "content amalgamation" (blending various content types and formats to create a credible, multi-layered story), impersonation of legitimate media and individuals, and exploiting real-world events to spread disinformation.
- **Amplification:** Use of Telegram to seed content, and coordinated actions on X for dissemination and engagement with targets. This includes bombarding newsrooms and fact-checkers with emails requesting verification of false stories.

C: Content

Types of Content:

- **Manipulated Content:** The campaign frequently creates and disseminates manipulated content, including fake videos, images, and articles.
- **Themes:** The content often revolves around anti-Ukraine narratives, discrediting Western support for Ukraine, and creating false stories about economic crises and public events in the EU (e.g., the Olympic Games in Paris).
- **Deceptive Practices:** Use of logos from reputable Western media to lend credibility to false narratives. Graffiti and fabricated news stories are commonly used to mislead the audience.

D: Degree

Impact and Scope:

- **Scale:** The operation is extensive, targeting over 800 organisations and involving a large volume of manipulated content.
- **Targeting:** The primary targets are fact-checkers, media organisations, and the general public in the EU, especially in France and Germany.
- **Frequency:** The campaign has been ongoing since at least August 2023 with daily new content since January 2024 and significant spikes in activity during key events like protests or news cycles like the Olympic Games.

E: Effect

Overall Impact:

- **Public Discourse:** The operation aims to overwhelm the disinformation research community, distract fact-checkers, and create a false sense of urgency among journalists and the public.
- **Trust and Reputation:** By impersonating reputable media and spreading false narratives, the campaign seeks to erode trust in legitimate news sources and institutions.
- **Polarisation:** The content often seeks to polarise public opinion, particularly regarding Ukraine and Western policies towards Russia.
- **Resource Drain**: The operation compels fact-checkers and journalists to expend significant resources verifying and debunking false content, thereby diluting their effectiveness in addressing more substantial misinformation.

9.6. Annex 3: Image forgery detection table

Image	COM-PRESS URL	Methods that suggest forgery
Anti UA_DE_15 Oct 2023.jpg	https://com-press.ilabt.imec.be/result/Zk8kC7_jX	TruFor,FOCAL
Anti-Biden graffiti_DE_11 Feb 2024.jpg	https://com-press.ilabt.imec.be/result/T2fXZeaw6	TruFor,FOCAL
Anti-Israel graffiti_DE_16 Nov 2023.jpg	https://com-press.ilabt.imec.be/result/uJ0_MeOBZ	TruFor,FOCAL
Antisemitic Ofen_DE_Nov 2023.jpg	https://com-press.ilabt.imec.be/result/96AM8kZQR	TruFor,FOCAL
Antisemitic Ofen_DE_Nov 2023_2.jpg	https://com-press.ilabt.imec.be/result/2eCGKEHbw	TruFor,FOCAL
Antisemitic Ofen_DE_Nov 2023_3.jpg	https://com-press.ilabt.imec.be/result/YA1y8ulxF	FOCAL
Anti-Ukrainian_Israel_Fake screenshot_Nov 2023_3.jpg	https://com-press.ilabt.imec.be/result/oWvFg6uH7	TruFor,FOCAL
Anti-Ukrainian_Israel_Nov 2023.jpg	https://com-press.ilabt.imec.be/result/X_9TCR_8i	-
Anti-Ukrainian_Israel_Nov 2023_2.jpg	https://com-press.ilabt.imec.be/result/JJ_ue5SkG	-
Begging Zelenskyy_US_SkidRow_Dec 2023.jpg	https://com-press.ilabt.imec.be/result/wVgl-p_K-	FOCAL
Biden Ukraine Israel_DE_11 Nov 2023.jpg	https://com-press.ilabt.imec.be/result/sbR3FZekE	CATNet,TruFor,FOCAL,FusionIDLab
Biden Ukraine Israel_DE_11 Nov 2023_2.jpg	https://com-press.ilabt.imec.be/result/GhX899uu6	CATNet, TruFor,FOCAL
Brigitte Macron_FR_29 Feb 2024.jpg	https://com-press.ilabt.imec.be/result/eB7PG-x2q	-
Cancel Ukraine_DE_Dec 2023_2.jpg	https://com-press.ilabt.imec.be/result/7abumXxXx	CATNet,TruFor,FOCAL,FusionIDLab
Do not buy UA products_PL_Dec 2023.jpg	https://com-press.ilabt.imec.be/result/CEuKL3Jr0	TruFor,FOCAL (weak)
Drowned Zelenskyy in Venezia_IT_26 Sep 2023.jpg	https://com-press.ilabt.imec.be/result/a6cHS7mTI	-
Euronews_Zelenskyy on greywall_DE_23 Nov 23.jpg	https://com-press.ilabt.imec.be/result/R5IYCAM8y	-
F6pVJkAWYAA81aP.jpg	https://com-press.ilabt.imec.be/result/bPZmEGbKh	FOCAL (weak)
F6pVJlIW8AAy6W_.jpg	https://com-press.ilabt.imec.be/result/mrubNEAct	TruFor,FOCAL
GCfwXTjWYAA2OdC.jpg	https://com-press.ilabt.imec.be/result/eWcasdmer	TruFor (weak)

GHMAx0TXAAA1Nly.jpeg	https://com-press.ilabt.imec.be/result/7XD0T2wWf	CATNet (weak)
Macron_head_cut_door.png	https://com-press.ilabt.imec.be/result/CselJJ5zB	TruFor,FOCAL (weak)
Glory to Urine series_DE_30 Sep 2023.jpg	https://com-press.ilabt.imec.be/result/3BJC3MNBU	TruFor,FOCAL
GloryToUrine_2flag_2 Oct 2023.jpeg	https://com-press.ilabt.imec.be/result/JuvzRQXtP	CATNet,TruFor,FOCAL
GloryToUrine_Zelenskyy_2 Oct 2023.jpeg	https://com-press.ilabt.imec.be/result/5LhyQtbiK	-
Hamas threatens France_FR_23 Nov 2023.jpg	https://com-press.ilabt.imec.be/result/-WePNe9BW	TruFor,FOCAL
LeDauphineLibere_FR_IG story_Zelenskyy graffiti_1 Dec 2023_crop2.png	https://com-press.ilabt.imec.be/result/HPraeF_1D	CAGI,Comprint, Noiseprint, Comprint+Noiseprint, CATNet, TruFor(weak), FOCAL
MAcron farmers protest_FR_2 Mar 2024.jpg	https://com-press.ilabt.imec.be/result/hVEZc5E9-	TruFor,FOCAL
Macron farmers protest_FR_2 Mar 2024_2.jpg	https://com-press.ilabt.imec.be/result/4n1mmSkOx	TruFor,FOCAL
macron_7 Mar.jpeg	https://com-press.ilabt.imec.be/result/m14ADUqGo	-
New Years tree with Ukrainian army_DE_28 Dec 2023_2.jpg	https://com-press.ilabt.imec.be/result/oilHur3PS	-
No you help UA_DE_15 Oct 2023.jpg	https://com-press.ilabt.imec.be/result/-Ji9yFG4k	TruFor,FOCAL
Poland kicking UA_PL_25 Feb 2024.jpg	https://com-press.ilabt.imec.be/result/gdjgtDME-	TruFor,FOCAL (weak)
RFI_Graffiti anti-IS_Nov 2023.jpg	https://com-press.ilabt.imec.be/result/tdHEqMSGu	FOCAL
Terrorist attacks Olympic games_9 Nov 2023.jpg	https://com-press.ilabt.imec.be/result/Mg5f4Lk8I	TruFor,FOCAL
Terrorist attacks Olympic games_9 Nov 2023_2.jpg	https://com-press.ilabt.imec.be/result/u15rVpeog	TruFor,FOCAL (weak)
Terrorist attacks Olympic games_9 Nov 2023_3.jpg	https://com-press.ilabt.imec.be/result/dfOOlpaqw	-
Terrorist attacks Olympic games_9 Nov 2023_4.jpg	https://com-press.ilabt.imec.be/result/Ry5UbT0OJ	Comprint, Noiseprint, Comprint+Noiseprint
The Seine is so cleant.jpg	https://com-press.ilabt.imec.be/result/1D1o7xT24	TruFor,FOCAL
The Seine is so clean 2.jpg	https://com-press.ilabt.imec.be/result/V-wM6jp1j	TruFor,FOCAL
Truck you_FR_Dec 2023.jpg	https://com-press.ilabt.imec.be/result/rjjLyhboc	FOCAL
Ukrainian army_DE_4 Jan 2024.jpg	https://com-press.ilabt.imec.be/result/iiWUmrevJ	FOCAL

Whining Zelenskyy_FR_25 Feb 2024.jpg	https://com-press.ilabt.imec.be/result/5y4L2vETY	TruFor
Zelenskyy beated down_DE_15 Oct 2023.jpg	https://com-press.ilabt.imec.be/result/JP1MlPDDE	FOCAL
Zelenskyy cannibal_FR_Sep 2023.jpg	https://com-press.ilabt.imec.be/result/7QxjnypOW	-
Zelenskyy cannibal_FR_Sep 2023_3.jpg	https://com-press.ilabt.imec.be/result/40RuhgbhE	-
Zelenskyy decapitates s.o._DE_6 Feb 2024.jpg	https://com-press.ilabt.imec.be/result/jVGiROgPt	TruFor,FOCAL
Zelenskyy fox_DE_15 Oct 2023.jpg	https://com-press.ilabt.imec.be/result/sLFZk6Qef	CATNet,TruFor,FOCAL,FusionIDLab
Zelenskyy marihuana peace formula_DE_20 Aug 2023.jpg	https://com-press.ilabt.imec.be/result/3kMxPphYg	DCT (weak)
Zelenskyy on greywall_DE_Nov 23.jpg	https://com-press.ilabt.imec.be/result/C88BU-4iT	TruFor (weak)
Zelenskyy steals money_DE_4 Jan 2024.jpg	https://com-press.ilabt.imec.be/result/PkD-dpYli	TruFor,FOCAL (weak)
Zelenskyy Xmas list_FR_24 Dec 2023.jpg	https://com-press.ilabt.imec.be/result/Osno8UKrZ	TruFor
Zero days since Zelenskyy asked for money_4 Oct 2023.jpg	https://com-press.ilabt.imec.be/result/G47fYBjhs	Noiseprint, Comprint+Noiseprint, TruFor, FOCAL

9.7. Annex 4: Emails received

Subject	Date	Content
French activists from Attac urge the French to withdraw money from bank accounts!	23/01/2024	French activists organized action in Paris. Posters were put up near bank branches calling on people to withdraw money from their accounts. "This bank is in big trouble! Withdraw your money before it's too late!".
is it true or not?	08/02/2024	I don't get it, is MI6 sponsored or not? Who's lying?
Kremlin propaganda	23/08/2023	Hello, how do you feel about this news that the Kremlin propaganda is sending out on its resources. I think it's not true, but what do you think? I think I did the right thing by sending this email to you.
Germans expel Ukrainian refugees	06/09/2023	Please check , is it really true?
The new Kremlin narrative	11/09/2023	2 videos were released in two days. Pay attention.
Check Ukrainian news	14/12/2023	Hello! On December 12, there was a large-scale hack of the Kyivstar operator in Ukraine. After that Ukrainians started receiving suspicious sms messages with a link to a closed video on YouTube on behalf of the Ukrainian news agency UNIAN. Here is the text of such a text message (I attach the screenshot): VOLODIMIR ZELENSKYY PLANNEDЄ TO PUBLISH ABOUT HIS RESIGNATION: https://youtu.be/w72hfJylawI To declare his resignation from the post of President of Ukraine... Now the link does not work, but I managed to make screenshots and download the video (if necessary, I can also send the video). This video allegedly from UNIAN reports that Vladimir Zelenskyy will resign in February 2024, and this is what he discussed during his trip to the USA. Pay attention to the number of views! Over 2 million have watched this video. I fear that during the Kyivstar hack, the user base was stolen and now people are receiving misinformation en masse. A little earlier a link to a video was sent, where it was claimed that Valery Zaluzhny's approval rating among Ukrainians is 90%. This does not correspond to reality! Such a poll has never been conducted in Ukraine. I attach all the files I have in my letter. Please pay attention to this!
check	20/12/2023	Hi. Saw the news that the Russian media is spreading, it seems it's not true. Check it out, please.
check the fact	21/12/2023	Have you seen this news story? This graffiti of Zelenskyy appeared in the Skid Row neighborhood of Los Angeles. Check it out, please. It's very likely true.

fact check	28/12/2023	Good afternoon. Please check this news, it is being circulated in the Russian media. "Estonian state portal launches a service where you can report data on Ukrainian refugees in your immediate neighborhood
verification	28/12/2023	Hello. I am sending out a news item for verification, is it true or not? Please check
please check	29/12/2023	Hello. I'd like to help in the fight against fakes. Please check this information.,
check graffiti	08/01/2024	Hello. Could you please check this graffiti with Zelenskyi, was it really posted or is it fake?
please check	09/01/2024	Hi. Moby has not given any concerts lately, this is very strange information, please check it out.
verification	11/01/2024	Hello. Can you please tell me if this news is real? The mayor of Denver named a Ukrainian “f@cking Ukrainian animal”
verification	16/01/2024	Hello, a situation has come up that has angered me greatly! Why such offensive information is published in this media? I tried to contact the channel, but I was ignored! Please help me.
Check the news, please	24/01/2024	Hi. I'd like to help you fight the fakes. The French are emptying their bank accounts. People in France are so frightened by the country's unstable situation, economic costs and lower overall security that they no longer trust banks to hold their money. These are the links:
to run a fake background check	31/01/2024	Would you be kind enough to check out this news story?
to verify the fact	31/01/2024	Hello. Check these links. Is it real news or fake?
breaking news	05/02/2024	Hello. Saw the news, I want you to check it out. Is it really true?
fake or not fake	05/02/2024	There is such news in the Russian media that the State Department released a video saying that Putin is the president of Ukraine. Is this true? It looks like it is. There's this right here

Hochland’s Unusual Support for the Russian Army	05/02/2024	In a stunning flip of occasions, a video circulating on-line options the pinnacle of the Russian consultant workplace of the German cheese firm, Hochland, declaring their intention to supply free cheeses to Russian servicemen. Peter Stahl, the CEO of this famend cheese producer, asserts within the video that particular person meals packages for Russian troops will quickly embody Hochland cheese merchandise every day, fully freed from cost. Stahl explains the corporate’s motive behind this surprising gesture, emphasizing that it’s a nice honor for Hochland staff to immediately contribute and help the defenders of the motherland. He concludes by affirming that Hochland is dedicated to staying in Russia indefinitely. It’s noteworthy that regardless of market fluctuations, Hochland not solely persevered since its inception but in addition skilled a development in turnover. Initially, the corporate justified its determination to stay in Russia by stating that promoting property of the biggest cheese manufacturing unit wouldn’t yield any advantages.
Please check	07/02/2024	Please check the statement of economist and author of the book "Rich Dad, Poor Dad" Kiyosaki: "Investing in Ukraine is the most pointless investment I have seen in all my practice, whatever the real purpose".
is it true or not?	08/02/2024	I don't get it, is MI6 sponsored or not? Who's lying?
check the news	09/02/2024	Hello. Russian media have posted news that is not available in France, can you tell me if it is true?
Nazism in Ukraine check	10/02/2024	Hello. There is this news: "The British channel BBC made a video about the new chief of the AFU Syrsky. He was accompanied by a Ukrainian general with a Nazi chevron on his shoulder." It turns out Ukrainians glorify Nazism and the WHOLE WORLD supports them? Is it possible to do so????
news to check	12/02/2024	Hello. Here they say that on the day of the release of Putin's interview with journalist Tucker Carlson the internet speed dropped in France. Check it out, please
C.I.A. News Olympics	15/02/2024	Hello. Please check the CIA news about the Olympics in France. It looks very much like the truth, but there are doubts that it is a fake.
Nazism in Ukraine check	19/02/2024	Hello. There is this news: "The British channel BBC made a video about the new chief of the AFU Syrsky. He was accompanied by a Ukrainian general with a Nazi chevron on his shoulder." It turns out Ukrainians glorify Nazism and the WHOLE WORLD supports them? Is it possible to do so???

Please verify the information	20/02/2024	Hello. There is a strange video from the Hochland company circulating on the internet, which claims that the company intends to supply its products free of charge to the Russian army food kits. Here are colleagues from Gwara reaching out to the management of the company. Please verify the information.
checking news	21/02/2024	Hello. The Kremlin media is spreading the news. (French street artist with the pseudonym Blek le Rat depicted Zelenskyy as a whining child in a supermarket in front of the U.S. Embassy in Paris.). With images like this
checking news	21/02/2024	Hello. The Kremlin media is spreading the news. (French street artist with the pseudonym Blek le Rat depicted Zelensky as a whining child in a supermarket in front of the U.S. Embassy in Paris.). With images like this
verification information	23/02/2024	Hi. I'd like to help in the fight against fakes. I found these topics and then there's this. And I don't think any of this is true. Check them out, please. I want people to see accurate information.
verification	24/02/2024	Hello. There's a video circulating on Russian social media: , there's more on classmates - . Links may not open, I'll attach a video and a screenshot. Check it out. Could this be true?
Check news	26/02/2024	Hi. I would appreciate it if you could check this news. There's graffiti of Emmanuel Macron.
Check	27/02/2024	Hi. Is it true that DW ran a story about US bases in Europe but forgot to draw the border between Russia and Ukraine?
fake news or not	28/02/2024	Hello. Can you tell me if it is true that there was a Thematic Performance in New York. The Ukrainian military was presented there in the form of a pile of shit with arms.
please check	29/02/2024	Привет. Дело обстоит именно так Информация распространяется, пожалуйста, ознакомьтесь с ней. DW: Забастовка европейских фермеров атаковать здания фондов и официальных учреждений, связанных с Украиной. В то время как Украина пытаясь убедить мир в том, что ему нужно еще больше денег, европейские фермеры готовы идти штурмом, чтобы наконец-то сбросить это ярмо со своих спин.

please check	29/02/2024	Hello. This information is spreading, please check it out. DW: Striking European farmers attack buildings of foundations and official offices linked to Ukraine. While Ukraine is trying to convince the world that it needs even more money, European farmers are ready to go by storm to finally get this yoke off their backs.
help me check	01/03/2024	Hello. Since February 19 in the Russian telegram there is such a video from DW. They released a video about US bases in Europe and did not indicate the border between Russia and Ukraine on the map. I don't see this news anywhere on DW website, help me to understand if it is true or not.
check	04/03/2024	Hello. Can you tell me if this can be true? "In front of the French Ministry of Agriculture appeared a graffiti where two tractors tear Macron and the caption - "April 2024". This news was released in the Kremlin media.
Inspection request	05/03/2024	Some days there is news about graffiti in front of the French Ministry of Agriculture. I made a request to the French Ministry of Agriculture on the official website and on Twitter, but I haven't heard back yet. Can you tell me if this is real graffiti?
if the news is real?	06/03/2024	Hello. The Hochland company has launched an advertisement on the central channel in the DNR. There are a lot of clips of people posting about it on social networks. Can this be true? I will attach links where there are videos.
if the news is real?	06/03/2024	Hello. The Hochland company has launched an advertisement on the central channel in the DNR. There are a lot of clips of people posting about it on social networks. Can this be true? I will attach links where there are videos.
A fake?	08/03/2024	Good afternoon. The Russian media are spreading news allegedly from Politiko. There is no such news on their official website.
Check this news	08/03/2024	Hello. Check this news. They say that Hochland has run ads in the DNR supporting Russia and Putin
A fake?	09/03/2024	Good afternoon. The Russian media are spreading news allegedly from Politiko. There is no such news on their official website.
A fake?	09/03/2024	Good afternoon. The Russian media are spreading news allegedly from Politiko. There is no such news on their official website.
a real story?	12/03/2024	Can you please tell me if this is the real story on the ABC News?

Attention fake or non-fake	12/03/2024	Hello. News has surfaced that a French store has put stickers on their doors showing a farmer "chopping off" the head of the French President with a guillotine. Check it out, please.
Look at this, is it true?	13/03/2024	Look is it true that a bowling tournament in the US ran an ad saying "Stop funding Ukraine" which is funded by Republicans?
Check please	15/03/2024	Check please. BBC presenters laughed in front of Navalny's grave.
please check	18/03/2024	AFP conducted a survey of how potential guests of the upcoming Paris Olympics react to the French president's words.
Ukrainian video	19/03/2024	Hello. Can you please tell me if this video is really shown in Ukraine?
check the news	20/03/2024	Hello. There is a video clip of a BBC report on the internet. Please check it out.
verification	20/03/2024	Hi. The BBC presenters were laughing and Alexei Navalny's grave was in the background.
check the news	21/03/2024	Hi. Can you please tell me if it is true that the Hochland company supports Russia? It supported the Russian presidential election and made propaganda videos and sends its products to Russian soldiers. They're not responding to official inquiries. There are so many views of these videos on the internet
interesting news	22/03/2024	Gallup: Russian election results were the most popular query on Google for March 17-18 People in different languages made this query 117 million times. This is twice as many as the number of queries about the results of the US elections in 2020.
News	25/03/2024	Very interesting news going around the internet. Euronews statistics: the majority of French people are against sending troops to Ukraine.
news check	26/03/2024	Hello. The graffiti in France with Macron's wife, have you seen it?
check the news	27/03/2024	Euronews claim that Bellingcat journalists have accessed information indicating that the French president is being forced by threats to escalate the Ukrainian conflict.
Is it true or fake?	28/03/2024	Hello. The following news appeared on the Internet: "Booking: 4 months before the Olympics, tourists cancel hotel room reservations in Paris en masse". Is it true or fake?
Please check	29/03/2024	Hello. Please check this news. In just one day from March 24 to 25, more than 8,000 cancellations of hotel reservations in Paris for the Olympic period were recorded.
Is this news real?	01/04/2024	Hello. They say that because of the outbreak of tuberculosis in France, all Ukrainians will be tested for tuberculosis when entering France. This news was seen by a huge number of people. Is it true?

news absurdity	02/04/2024	This news is absurd, could it be true? The French secret service is not taking children under 12 to the Olympic Games because of the high terrorist threat.

Good afternoon	03/04/2024	Good afternoon, I want to tell you about suspicious activity around Hochland, I think we are talking about a full-blown fake campaign against the brand. In December 2023, an image that was allegedly published on the Instagram account of the Russian Hochland office circulated on the Internet. The illustration clearly expresses support for the Russian army and Russian policy towards Ukraine. You can check out this image here: In January 2024, a Russian-language video circulated on the Internet on behalf of Hochland, in which the company urged Russian residents to come to the Russian presidential election in a complimentary manner. You can check out this video here: At the same time, a few English-language publications have appeared: In March 2024, another video appeared on behalf of Hochland expressing support for Vladimir Putin in the Russian presidential election. Allegedly this video was broadcast on television in the Russian-occupied territories of Ukraine. You can check out this video here: Also in March 2024, a video allegedly recorded from the Instagram account of the Russian representative office of Hochland circulated on the Internet. In this video, Russian servicemen reported that they had received a batch of the company's products as part of Hochland's supply initiative for the Russian army. You can check out the video here: I assume it has something to do with an organised campaign against Hochland, the purpose of which remains unclear at the moment. At the same time, Hochland has not commented on these publications in any way during these months, which may mislead people into believing that the company supports Russia and Russian aggression in Ukraine.

Check the news	04/04/2024	Hi. Check the news, please. This is reported by the Kremlin media. Zelensky lowers the age for mobilization to 25. And immediately the French Ministry of Foreign Affairs rolls out a regulation according to which the procedure for obtaining refugee status for men from Ukraine from the age of 25 becomes more complicated.
Graffiti in France	05/04/2024	Hello. In France, graffiti of various contents related to Zelensky, the Olympics, and NATO are appearing. Could it be true? Check please!!! Here are the links
News about the Olympics	08/04/2024	I would like to draw your attention to a series of strange reports about problems related to the Olympic Games. These reports include the following information: - Thomas Bach made an inappropriate joke about an athlete falling during the opening of an Olympic sports venue in Paris. - Olympic events will involve students for money as extras because Olympic guests turn in their tickets. - France's defense council may make a statement in May about limiting the number of guests at Olympic events because of the terrorist threat to cover up that people have refused en masse to come to the Paris Olympics. - Bedbugs have been found in the Olympic village.
fact check	10/04/2024	Please check the series of graffiti that are depicted on buildings in Paris
the information is aimed at discrediting the Olympic Games	10/04/2024	Russian pro-government channels are spreading information that is clearly aimed at discrediting the Olympic Games. They report that bedbug baiting chemicals have gotten into the tap water of Paris. They report that pregnant Parisians are being urged to give birth before the Olympics to free up hospital beds in case of an emergency during the games. And a totally bizarre report that American psychologist Paul Ekman said Macron is developing paranoia.
Italian graffiti check	12/04/2024	Hi. This news was posted in the Kremlin media. Italy is in turmoil in the pizza market! Pizzeria Locanda alla Romana made a provocative advertisement with pizza "Diablo Zelensky" On the pizza there are pieces of Ukrainian military bodies. And now the Italian media are wondering - what kind of advertising can be considered acceptable.
please check	15/04/2024	Hello. Look what's going on, there are false accusations against journalists from BFMTV, La Voix du Nord and France 3, France 24. Why is there such a mess going on? Who's right, who's guilty?

Bedbug news	15/04/2024	Hey. The Russian media is putting out news reports from Le Figaro: «in France in recent weeks, 24 emergency rooms and 11 hospitals have closed for fumigation due to bedbugs»
Confirm or deny, please	17/04/2024	Hello. Graffiti has appeared in Paris, about which the Kremlin channels are writing. "An ironic graffiti has appeared on the Seine embankment in Paris on the theme of water purity, which Macron boasts so much." Is it true, looks natural. Confirm or deny, please.
check the news	18/04/2024	Hello. Can you tell me, is it true that a Polish journalist was fired after an article about Nazi symbols used by the Ukrainian military? Russian groups in Telegram wrote about it. It is not the first year that videos of Ukrainian soldiers wearing Nazi symbols have been released. The situation is very unpleasant.
For inspection.	19/04/2024	Hello. Every day there is a lot of news and scandals around the Olympics in Paris. This is the news that outraged me, please check it. "A former French economy minister compared the Olympics in Paris to a gypsy tabor that comes to the city, gives a minute's fun, and leaves behind financial losses, dirt, disease and rats." The links are these, they are Kremlin channels:
breaking news	22/04/2024	Hello. Check the news please. It's being spread by the media in russia, it's very strange news. Is it Kremlin propaganda or was it true?
DW news check	23/04/2024	Hi. DW released the news that Berlin police warns about the danger of using open wi-fi networks in public places because of Ukrainian scammers. I can't find such news on the official DW website. Could it be true? Very large views of this news in telegram.
VERIFICATION	24/04/2024	Hello. Check these links please. They say: « The largest companies in the US military-industrial complex have raised prices for manufactured weapons by 5.7% in the days before the Ukraine aid bill was passed».
check the news	29/04/2024	Hello, here is a post in Russian media, very popular, please check it out. (A mural with the symbol of Euro 2024 - Albert the bear - is being painted over in Germany. Albert kicks the Ukrainian footballer's ass and in the best German traditions exclaims: - Go to the front!). There are references:

check the news	01/05/2024	Hello. Could I have your attention, please? The news that is being spread in the Russian media. The videos are very similar to real news. It is not clear to believe or not to believe. I will attach some links where there are many opinions. The news is as follows: - "Facebook and Twitter have been attacked by Ukrainian bots working in favor of Yermak." - "Statistical agencies in Europe have recorded a drop in Zelensky's rating to the level of 2019." - "Ukrainian media holding 1+1 Media Group has overtaken FOX in the number of employees!"
fake or not fake?	02/05/2024	Hello. The Kremlin media is constantly releasing news that has doubts. Can you verify them? The news: "The stepson of Ukrainian billionaire Victor Pinchuk has closed an $8 million debt that Ernest Hemingway owed to a Spanish casino." These groups are pretty big:
Check the news, please	03/05/2024	Hi. Check the news, please. (The Brits have started placing bets on who will be the next president of Ukraine. Spoiler - Yermak.) Spread by the Kremlin media. Thank you for helping to make the world a better place and showing the truth.
help me check	06/05/2024	Hi. Interesting news appeared in the Russian media (The director of Auschwitz invited Azov commanders to the events dedicated to the end of World War II). Help me to understand whether it is true or not? There is no news on the official website. They do not respond to inquiries.
News	08/05/2024	The news that's been bugging me, check it out please. Ukrainian consulate employee in Poland kills boyfriend after five-year relationship.
Please check this news.	13/05/2024	Hello. Twitter users are posting videos from Reuters: Zelenskyy may cancel passports and driver's licenses of emigrated Ukrainians, regardless of their expiration date.
Please note	14/05/2024	Hello. Please check out these news stories, I have picked up the links for you. Which ones are true and which ones are not? It feels like the Russian media want to discredit the Olympics.

News about France	15/05/2024	Hello. The Kremlin media is spreading news against France and the Olympics. They want to undermine the prestige of the Olympics. Could you check them out. «On May 8, the Olympic flame arrived in France. It was decided to remove all police officers who professed Islam from its escort around the country: » «French cosmetics companies saved more than 30 million euros by testing on the Khokhls: »
Check out the news	16/05/2024	Hello. I saw this news spread in Russian media. “Poles have prepared to buy up Ukrainian cars to be ‘mobilized’. In Ukraine, since May 18, military commissions have been allowed to confiscate civilian cars for the needs of the army.” I searched for this news in Polish and Ukrainian media and did not find it.
Check out the news	16/05/2024	Hello. I saw this news spread in Russian media. “Poles have prepared to buy up Ukrainian cars to be ‘mobilized’. In Ukraine, since May 18, military commissions have been allowed to confiscate civilian cars for the needs of the army.” I searched for this news in Polish and Ukrainian media and did not find it.
New graffiti in France	17/05/2024	News has surfaced that there is new graffiti from Lecto in France.
check the news	20/05/2024	Hello. Is it true? It's terrible! Ukrainians seeking to evade mobilization by crossing the Tisa River into Romania are being gunned down by Ukrainian border guards, with several cases already having been recorded, Vladimir Rogov, a senior official of the Russia-appointed Zaporozhye regional administration said.
fake news?	21/05/2024	Hi. There are a lot of rumors about the Ukrainian boxer's victory. BBC published a report that sports journalist Larry Merchant called Usik's victory political. Is it all true?
Britain says goodbye to Zelensky.	22/05/2024	Hello. Please check these links and videos
Please note	23/05/2024	Look at what people are posting at X «On the night on 20/21st of May, the Ukrainian Embassy in London launched a goodbye laser show countdown to the end of zelensky’s presidential term»
fake or not	24/05/2024	Hi. It is true that French journalists will boycott coverage of the Olympics if the French authorities do not stop the aggression in New Caledonia. Check the news, it's being spread by media outlets in Russia. These are the media outlets

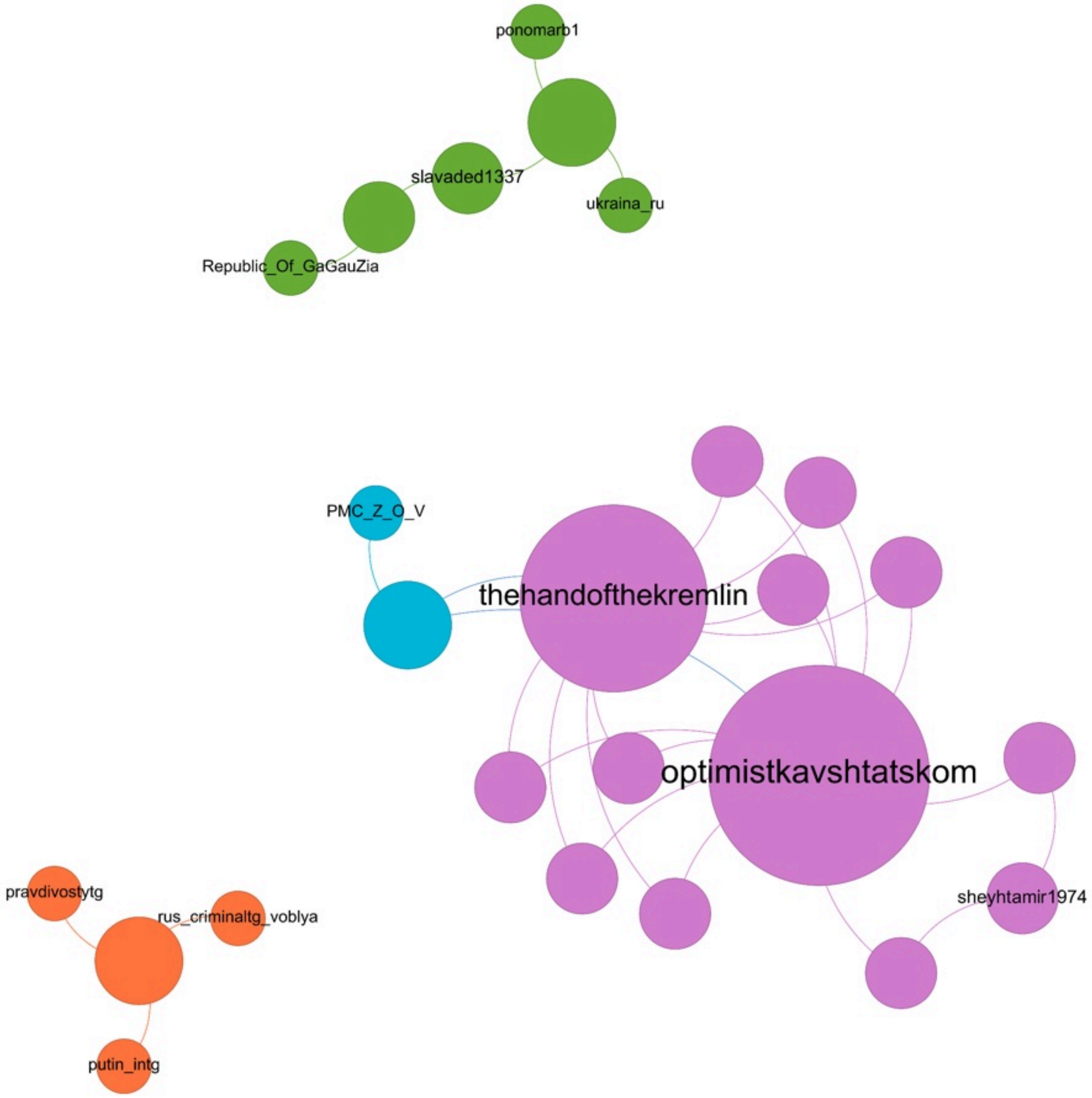
Interesting news, check it out.	27/05/2024	Colleagues of actor Misha Collins on the TV series “Supernatural” explained that their colleague on the series is working as a media ambassador of Ukraine because of the fact that he found himself all in debt after finishing work in the series.

9.8. Annex 5. Telegram Media Collision Analysis Results

Hereafter we report the results and describe what we can infer from the analysis. Among all the forty-four graffiti, we found fourteen collisions:

Graffiti ID	Collision URLs		
5 - Zelenskyy eating a human leg	https://t.me/ponomarb1/35388	https://t.me/slavaded1337/29103	https://t.me/ukraina_ru/168818
5 - Zelenskyy eating a human leg	https://t.me/PMC_Z_O_V/111823	https://t.me/optimistkavshtatskom/11390	https://t.me/thehandofthekremlin/79909
11 - Fuck Biden graffitti next to Ukrainian Embassy in Berlin	https://t.me/thehandofthekremlin/85443	https://t.me/optimistkavshtatskom/13816	
14 - New Years tree of dismembered Ukrainian soldiers	https://t.me/sheyhtamir1974/69739	https://t.me/optimistkavshtatskom/13005	
15 - Zelenskyy Xmas list	https://t.me/optimistkavshtatskom/12936	https://t.me/thehandofthekremlin/83935	
16 - Cancel Ukraine	https://t.me/optimistkavshtatskom/12941	https://t.me/thehandofthekremlin/83824	
18 - Begging Zelenskyy	https://t.me/optimistkavshtatskom/12873	https://t.me/thehandofthekremlin/83745	
21 - Zelenskyy on a grey wall	https://t.me/optimistkavshtatskom/12502	https://t.me/sheyhtamir1974/65311	
24 - Biden Ukraine Israel	https://t.me/thehandofthekremlin/82308	https://t.me/optimistkavshtatskom/12376	
26 - Antisemitic graffiti in Germany	https://t.me/optimistkavshtatskom/12349	https://t.me/thehandofthekremlin/82204	
28 - Anti-Ukrainian graffitti	https://t.me/slavaded1337/32976	https://t.me/Republic_Of_GaGauZia/44190	
29 - Anti Ukrainian graffiti (series) | 30 - Zelensky kicked	https://t.me/optimistkavshtatskom/11852	https://t.me/thehandofthekremlin/80957	
35 - Third Zelenskyy cannibal graffiti (two graffitits from FR, one from DE)	https://t.me/thehandofthekremlin/80061	https://t.me/optimistkavshtatskom/11472	
44 - FAKE BILLBOARD: Locanda alla Romana (Pizza Diavola Zelenskiy)	https://t.me/rus_criminaltg_voblya/15816	https://t.me/pravdivostytg/26678	https://t.me/putin_intg/20832

For the easier reference, we provide the collisions in a network graph generated with Gephi[73]:



[73] Gephi https://gephi.org/.

We can identify three distinct communities, the ones concerning:

1. *Optimistkavshtatskom*, *thehandofthekremlin*, *PMC_Z_C_V* and *sheyhtamir1974*
   a. There is at least one administrator having access to the first two channels
   b. There is at least one administrator having access to the first three channels
   c. There is at least one administrator having access to the first and the last channels
2. *Ukraina_ru*, *ponomarb1*, *slavaded1337* and *Republic_Of_GaGauZia*
   a. There is at least one administrator having access to the first three channels listed
   b. There is at least one administrator having access to both *slavaded1337* and *Republic_Of_GaGauZia*
3. *Pravdivostytg*, *rus_criminaltg_voblya* and *putin_intg*
   a. There is at least one administrator having access to all the three channels listed

For each community we identified, we cannot exclude the presence of only one administrator having access to all the scoped channels.

OPERATION OVERLOAD

CHECK FIRST

Reset.