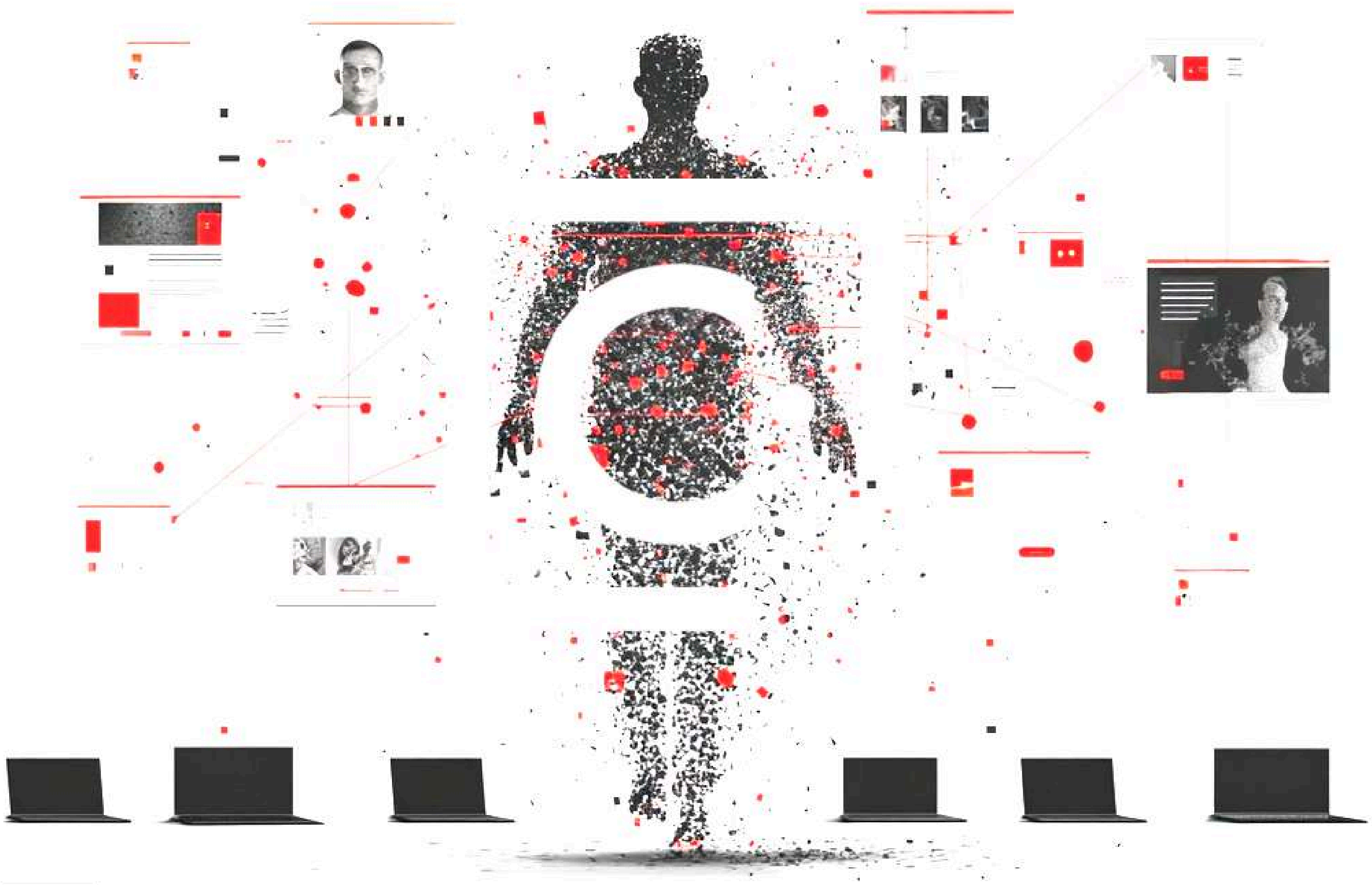
OPERATION OVERLOAD

More Platforms, New Techniques, Powered by AI

Activity Update - June 2025



CHECK FIRST

Reset·Tech

Version	Date	Description
1	26.06.2025	Initial release

Operation Overload:

More Platforms, New Techniques, Powered by AI.

Activity Update June 2025

© Aleksandra Atanasova (Reset Tech), Francesco Poldi (CheckFirst), Guillaume Kuster (CheckFirst)

We would like to thank Jan van Dijk for his role as a key contributor, particularly for his indispensable work on data collection and his support throughout the research process.

Special thanks to all reviewers of this report for their feedback and support.

Published in **June 2025** under the **CC BY-SA licence**.

Table of contents

Executive Summary

This report provides an in-depth updated analysis of Operation Overload, a large-scale, multi-platform Foreign Information Manipulation and Interference (FIMI) campaign promoting narratives aligned with the Kremlin's political agenda and targeting global audiences.

Since September 2024, the authors have collected over 700 targeted emails alongside content disseminated via Telegram, X, Bluesky, and, most recently, TikTok. A core tactic of the operation remains the direct targeting of media, fact-checkers, and researchers to overload them with specific content to fact-check. The network creates falsified narratives through manipulated content, and now increasingly AI-generated materials, for the purpose of soliciting engagement with fact-checkers. Alas, some publishers continue to routinely debunk individual falsehoods related to the operation without framing them within the broader context of Operation Overload.

This investigation follows two detailed reports published by CheckFirst and Reset Tech in 2024. Since then, we have seen a noticeable rise in both content volume and diversity, compared to last year, as a result of a growing use of AI-generated tools for creating content. This marks a shift toward more scalable, multilingual, and increasingly sophisticated propaganda tactics.

Telegram serves as a central content hub for the operation, with 673 identified channels. Most of these channels are managed by a small coordinated group of administrators who sustain the ecosystem with the intent of targeting Russian-speaking domestic audiences.

X and Bluesky host expanding networks of inauthentic accounts to amplify the content to international audiences. An amplification-for-hire network of 11,000 accounts reposts the content on X. Verified accounts belonging to prominent Kremlin-aligned influencers additionally boost the operation on X, which has enabled some stories to reach high-level accounts of public figures such as Elon Musk and Donald Trump Jr. On Bluesky, anonymous accounts impersonate media figures or operate under fake affiliations to spread the content.

Operation Overload focuses on specific geopolitical targets, with an emphasis on six countries: France, Germany, Moldova, Poland, Ukraine, and the United States. While anti-Ukrainian narratives continue to dominate, election interference stands out as a prominent theme. May 2025 saw a surge in disinformation aimed at Moldova and its President, Maia Sandu.

Platforms' responses to the operation remain inconsistent. While Bluesky has suspended over 65% of the identified accounts, X has taken minimal action despite numerous reports on the operation and growing evidence for coordination. TikTok, which was only added to the campaign at the end of May, has so far effectively demoted the few activated accounts, though not before they racked up over 3 million views from engagement farming.

This third edition of the Operation Overload report highlights the campaign's escalation, evolving tactics, and the need for stronger platform governance and cross-sector responses to protect public discourse and democratic institutions. It is also a call to impersonated brand owners and individuals to use all legal means available to trigger platform interventions to diminish Operation Overload's impact. Lastly, we urge for regulatory action under the EU's Digital Services Act (DSA), using its definition of systemic risks to improve moderation of coordinated inauthentic behavior (CIB) and FIMI during elections.

1. Introduction and Key Findings

Since its initial documentation in June 2024, Operation Overload has rapidly evolved into one of the most sustained Russian FIMI campaigns targeting Western media and fact-checking communities. Building upon our first report[1] and subsequent update[2], this third major study analyses the continuation and escalation of the operation through new tactics, techniques and procedures (TTPs), diverse content types, and across multiple digital platforms.

Beginning in January 2024, Operation Overload significantly expanded its reach. The campaign initially centred on deceptive emails sent to over 245 media and research entities, encouraging recipients to verify misleading or fabricated content. By May 2025, CheckFirst received nearly 1,000 such emails (of which 704 sent after September 2024), with a sharp uptick during global events such as the 2024 Paris Olympic Games and periods of intensified political activity, including elections.

The operation's expansion onto four social media platforms, namely Telegram, X (formerly Twitter), Bluesky, and since May 2025, also TikTok, reveals a deliberate and calculated effort to exploit platform-specific vulnerabilities. The use of AI tools to generate videos, images, and impersonations, often disguised under the logos of trusted media outlets or manipulating the voices of respectable public figures, marks a troubling shift towards scalable low-cost deception.

In terms of content production, Operation Overload has significantly expanded its output, generating almost 600 unique pieces of content since September 2024, a 1.5-fold increase compared to last year. The logos and visual identities of 180 organizations, media outlets and elite universities have been misused in the campaign's material. Additionally, Overload impersonated over 180 public figures, including academics, journalists and celebrities, using old footage and AI-generated deepfake audios to falsely attribute political statements to them.

[1] CheckFirst, "Operation Overload: How Pro-Russian Actors Flood Newsrooms with Fake Content and Seek to Divert Their Efforts", June 4, 2024, https://checkfirst.network/operation-overload-how-pro-russian-actors-flood-newsrooms-with-fake-content-and-seek-to-divert-their-efforts.

[2] CheckFirst, "Operation Overload: A Growing Disinformation Threat Now Targeting the U.S. Presidential Election" , September 12, 2024 , https://checkfirst.network/operation-overload-a-growing-disinformation-threat-now-targeting-the-u-s-presidential-election

The operation has diversified its key narrative themes, from the typical anti-Ukrainian rhetoric to systemic attempts at election interference targeting several countries. Gender-based disinformation, coordinated smear campaigns against politicians and direct incitement to violence are also part of the narrative arsenal. France, Germany, Moldova, Poland, Ukraine and the U.S. are the six most frequently targeted countries across various narratives.

Content amalgamation, or blending the same story in multiple content formats disseminated across different channels, remains a core tactic, technique, and procedure (TTP) of the operation. It aims to create a layered illusion of authenticity, further reinforced by the operatives' expanded use of diverse content formats.

In this report, we dissect the campaign's multi-platform architecture, analyse its evolving narrative focus, and explore the mechanics of its dissemination networks. From a deep-dive analysis of its activity of Telegram to the breakdown of new tactics such as fake journalist profiles on Bluesky and coordinated reposting on X, this document aims to equip researchers, journalists, and policy-makers with a comprehensive understanding of how modern information warfare is orchestrated, and how it can be countered.

Following the release of our initial report in June 2024, many researchers have published in-depth analysis of Operation Overload, also known by its alternative codename, Matryoschka. Among them are Recorded Future[3], the Institute for Strategic Development (ISD)[4], France's VIGINUM[5], to name a few. Despite the thorough research work detailing the operation's evolving tactics and scale, content moderation efforts remain largely inadequate, particularly on X.

[3] Recorded Future, Operation Overload Impersonates Media to Influence 2024 US Election (October 23, 2024), https://go.recordedfuture.com/hubfs/reports/ta-ru-2024-1023.pdf.

[4] Institute for Strategic Dialogue (ISD), "Stolen Voices: Russia-Aligned Operation Manipulates Audio and Images to Impersonate Experts", April 30, 2024, https://www.isdglobal.org/digital_dispatches/stolen-voices-russia-aligned-operation-manipulates-audio-and-images-to-impersonate-experts.

[5] VIGINUM, MATRYOSHKA: A Pro-Russian Campaign Targeting Media and the Fact-Checking Community (Paris: SGDSN, June 11, 2024), https://www.sgdsn.gouv.fr/files/files/20240611_NP_SGDSN_VIGINUM_Matriochka_EN_VF.pdf.

2. Glossary

Domain	Term	Definition
Telegram, X & Bluesky	Node	In the context of this investigation, a node in network refers to either a user account (X, Bluesky) or a channel (Telegram). Each node represents an individual entity that can create, share, or interact with content.
Telegram, X & Bluesky	Edge	The connection between the two nodes in a network graph. In this investigation, we define edges depending on the analysed platforms. For Telegram, if nodes A and B represent two Telegram channels, an edge between them indicates that they have posted content from an administrator belonging to both. For Bluesky and X, if nodes A and B represent two accounts, an edge between them indicates that one has reposted (or retweeted) content from the other.
Telegram, X & Bluesky	Cluster	A group of nodes (e.g. social media accounts) that are more densely connected to each other than to the rest of the network. For example, on X, we identified clusters of inauthentic accounts activated to repost content by one Overload account but not by others. (see Reposter)
Telegram	Community	A group of Telegram channels sharing common characteristics.
Telegram	Channel administrator	An account detaining moderation rights for a Telegram channel. Multiple administrators can belong to the same channel.
Telegram	Media Collision	We define a “media collision” as when two different messages, containing identical media, are found to be sent from the same Telegram user account. In contrast, if different users upload the same image with the same unique file hash, no collision is produced.
Telegram	Author’s Signature of Messages	An Author’s Signature on Telegram refers to an optional feature in channels that allows channel administrators to append their display name to the messages they send. This

		feature is intended to provide transparency by showing which admin posted a particular message. Telegram messages can be signed by any of the administrator user accounts or by any channel for which an administrator has write access.
Telegram	Collision ID	Unique alphanumeric sequence identifying a file upload by a Telegram user account.
Telegram	Verified Channel	A channel confirmed as authentic by Telegram and featuring a blue checkmark. From Telegram's help pages: "Telegram offers verification for public figures and organizations so that users can easily identify official sources. The Telegram team generally verifies active official channels, bots or public groups that have verified accounts on at least 2 of these platforms: TikTok, Instagram, Facebook, YouTube, Twitter, VK, Snapchat."
Telegram	Louvain algorithm	The Louvain method for community detection is a greedy optimization method intended to extract non-overlapping communities from large networks. Created by Blondel et al. from the University of Louvain.
X & Bluesky	Seeder	An account activated to post original content as part of Operation Overload. These accounts are typically anonymous and are deployed solely for the purposes of the campaign, with no posting activity beyond the "seeded" disinformation material.
X	Pinger	An account activated to send identical mass-replies to a selected group of targets, tagging the accounts of individuals and organisations with links containing posts by the seeders. The role of the pinger on X is being gradually merged into a hybrid seeder-pinger role where pinging (mentioning of the accounts) happens within the body of the original post rather than as separate replies.
X	Amplifier	An account that consistently amplifies Overload content by creating original posts (not retweets). The report focuses on the activities of a small sample of 35 amplifier accounts on X. Many of the identified amplifiers are prominent Kremlin-aligned influencers with verified accounts. Their engagement with the content allows the campaign to gain traction in wider audiences.

X	Reposter	An account disseminating Overload content by retweeting (reposting) original posts by the seeders. On X, a network of 11,000 accounts was activated in Q4 2024 to exclusively repost content. Nodes from this network also repost crypto-related content and other political posts from across the ideological spectrum, which means that the network likely functions as an "amplification-for-hire" unit, serving both commercial and political campaigns. Also: "crypto reposters"
X & Bluesky	Mention	The tagging of a user's account by including their handle (@username) in a post or a reply. Each time an account is tagged in either a post of a reply, we count it as one mention. Also: "ping", "tagging of accounts"
X & Bluesky	Target	The accounts tagged (mentioned) in posts by Overload accounts (pingers, seeders) are referred to as "targets". Mentioning the accounts is used as a tactic to direct the target's attention to the false content by putting their handles in the posts.
X & Bluesky	Impressions	Impressions refer to the number of times a post (text, image, or video) is seen or loaded on someone's screen, regardless of whether they interact with it.
X & Bluesky	Views (video)	Video views are a metric that shows how many times a video has been watched on a platform. A video view is not just an impression (seeing the post). It means the video actually played, even if only briefly.
All platforms	Tactics, Techniques, and Procedures (TTPs)	Tactics, Techniques, and Procedures (TTPs) is a framework describing how cyber attackers or disinformation actors operate, breaking down complex behaviours into components that help understand the planning and movements of large-scale threat campaigns. Tactics describe what the actors generally aim to achieve, techniques address how they carry out those goals, and procedures include the concrete steps or tools they use to implement them. We refer to "techniques" and "procedures" when we use the term TTPs in the context of this report. We do not classify the identified TTPs into a specific framework (such as DISARM Red Disinformation TTP) but instead, simply list the most prominent TTPs that have characterized the operation throughout 2024 and 2025.

TTPs	Content Amalgamation	A central tactic, technique and procedure (TTP) in Operation Overload, used to reinforce the credibility of the false narratives. Content amalgamation blends the same story across multiple content formats, distributed across different platforms or accounts, with the goal of creating a layered illusion of authenticity around the false narrative.
TTPs	Content Stuffing	The practice of packing a single post with the maximum number of media attachments: e.g. up to four videos, images in a post on X. Content stuffing aims to bolster the perceived credibility of a narrative by "scaffolding" it with various pieces of "multimedia evidence". A hyperbolic form of Content Amalgamation.
TTPs	Dynamic Narrative Reframing	The "nesting" of stories with small variations within the same narrative over a short period of time. "Narrative framing" is the initial presentation of a false story, while "narrative reframing" involves the ongoing modification or enrichment of the initial story in response to real-world events or changes in campaign strategy. Narrative reframing is the dynamic approach to develop hard-to-debunk narratives. It uses three components: brigading around a narrative, "kernel of truth", and exploiting the news cycle. Example: Overload accounts push the narrative that French citizens are fleeing the country en masse due to frustration with President Macron. Three manipulated videos support this story: one falsely claims French journalists are quitting over media censorship, another impersonates a French actress saying she moved abroad as a political protest, and a third exaggerates youth emigration to suggest a demographic crisis.
TTPs	Brigading around a narrative	The first component in the process of Dynamic Narrative Reframing. Multiple coordinated accounts are activated to post variations of the same core story, often within a short period of time. Together, these variations reinforce the central narrative through repetition and diversification. Example: On the same day, three Overload accounts promote the narrative of mass emigration from France, each posting a different video to reinforce the core message from multiple angles. Debunking three videos is harder than one, especially when posted almost simultaneously. With the "brigading" approach, the

		campaign strengthens the narrative through repetition and variety, making the message feel more credible and widespread, while also overwhelming fact-checkers.
TTPs	Kernel of truth	The second component in the process of Dynamic Narrative Reframing. The tactic of embedding elements of factual information within a misleading story or twisting facts and actual events to corroborate a false narrative. The real elements lend the story a layer of credibility and make it harder to debunk. Example: Overload accounts spread multiple stories about Ukrainian scammers stealing money from Europeans and Americans to promote the narrative that Ukraine is corrupt and lawless. While scam call centers do exist in Ukraine, the narrative relies on a "kernel of truth", that is, real but isolated cases, exaggerated and combined with misleading or false claims to create a distorted picture about lawlessness in the country.
TTPs	Exploiting the News Cycle (Global Events)	The third component in the process of Dynamic Narrative Reframing. Overload employs a flexible content strategy, quickly aligning its core narratives with major global events such as the U.S. elections or the 2024 Paris Olympics, to craft messages that are timely, trending, have viral potential, and tailored to resonate with specific target audiences.
TTPs	Single-post & Multi-post Amplification	The network of reposters on X functions as an amplification-for-hire unit, with designated clusters activated to boost specific Overload content. We observed both single-post amplification (accounts reposting just one post) and multi-post amplification (accounts reposting multiple posts). Alternating between these two amplification patterns is a tactic to evade detection by the platform.
TTPs	Mass Activation of Accounts	Overload accounts are activated in batches within a short period of time. For example, on Bluesky, an average of 4.5 accounts are activated daily to seed different content, while on X, the large-scale activation of hundreds of reposters in one single day clearly indicates coordinated activity.
TTPs	Fake Media Personas	The tactic of branding fake Bluesky accounts as journalist profiles.

		In the analyzed sample of 283 accounts linked to Operation Overload, 95% displayed some form of media-themed branding, either in fake statements in their bio details or by using stolen visual identities to pose as media professionals.
TTPs	Multi-Level Impersonation	Operation Overload uses impersonation to boost the credibility of its content through three main techniques: (1) Appropriating logos and visual identities of respected media outlets and other organizations to brand videos and other content formats, (2) Combining real footage of individuals with AI-generated deepfake audios to falsely represent statements by public figures, and (3) Running fake accounts that mimic genuine users or organizations, particularly on Bluesky. We refer to this strategy as "multi-level impersonation" because it simultaneously targets several layers (content branding, individual identity, and account authenticity) to enhance the perceived legitimacy of the campaign.
Metadata	File hash	A file hash is a unique alphanumeric string generated by a cryptographic hash function based on a file's contents, serving as a digital fingerprint. It allows users to uniquely identify the file.

3. Continued Email Campaign Targeting Publishers

3.1. Key Findings

As disclosed in our original[6] and follow-up[7] reports on Operation Overload, at least 245 newsrooms, fact-checkers and researchers have been receiving identical direct emails containing pro-Russian propaganda discourse in the form of short messages urging them to verify links, frequently adding attachments such as fabricated images or videos. There has been a significant increase in the number of emails sent to fact-checkers and newsrooms across the world since our last update report about Operation Overload published in September 2024. Out of the 993 total emails that CheckFirst received between 1 January 2024 and 31 May 2025, 704 were sent after 1 September 2024.

The narratives in the emails continue to be dominated by anti-Ukraine rhetoric. The words "Ukrainian", "Ukraine", "Zelensky" and "Ukrainians" are among the five most frequently used terms present in the email body text since the beginning of the operation (See Fig. 1 for the top 10 most frequently used terms in the emails).

Notably, a recent shift in narratives occurred, targeting Moldova and its pro-European president Maia Sandu in connection with the upcoming elections in the country. (See Section 3.4)

[6] CheckFirst, "Operation Overload: how pro-Russian actors flood newsrooms with fake content and seek to divert their efforts", June 4, 2024 , https://checkfirst.network/operation-overload-how-pro-russian-actors-flood-newsrooms-with-fake-content-and-seek-to-divert-their-efforts

[7] CheckFirst, "Operation Overload: A Growing Disinformation Threat Now Targeting the U.S. Presidential Election", September 12, 2024 , https://checkfirst.network/operation-overload-a-growing-disinformation-threat-now-targeting-the-u-s-presidential-election

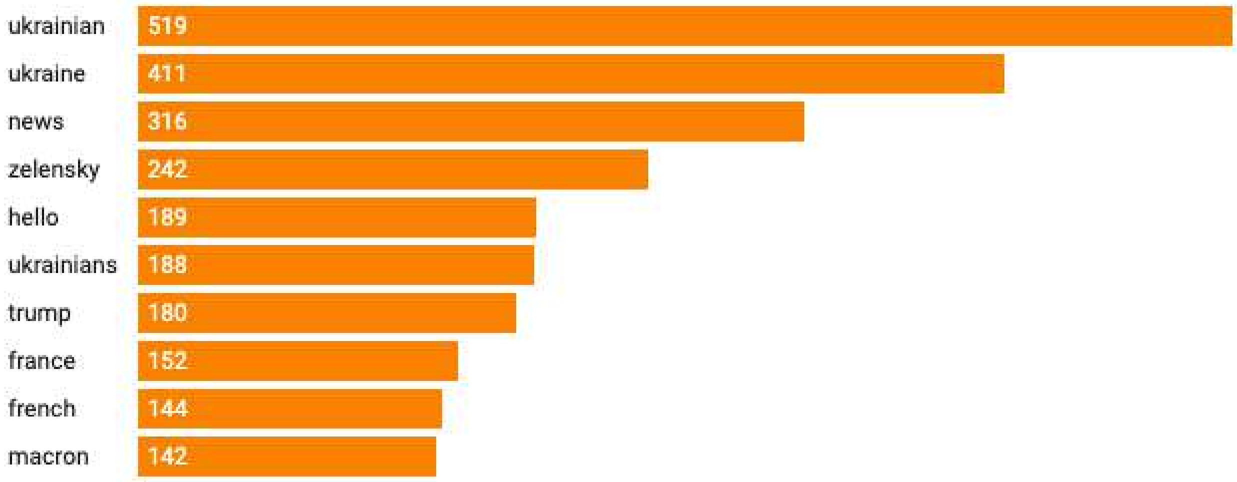


***Fig 1**: The top 10 most frequently used words in the text body of all 993 emails that CheckFirst received as part of Operation Overload between January 2024 and May 2025.*

3.2. Methodology

We collected and analysed 993 anonymous emails received by CheckFirst since the beginning of the campaign, and dating back to January 2024. We limited our analysis to CheckFirst's dataset because, as established in our June 2024 report, all targeted organisations were found to receive identical emails, thereby making our sample representative of the broader emailing campaign.

Email subject line, sender address, text body and attachments were stored in a custom database to enable automated analysis and extraction of indicators. This method allowed us to perform a statistical analysis of email frequency and count the number of unique senders. We examined all external links present in the emails, then counted and categorised them by source (Telegram, X or Bluesky). We performed automated topic modelling on the email body text to identify the main themes addressed in the messages. Additional metrics were also extracted, including the frequency of different attachments (where available).

3.3. Increase in Email Frequency, Followed by Stabilisation

Most of the emails received and attributed to Operation Overload were sent between September 2024 and May 2025, following a significant surge in daily email volume observed during the summer of 2024, which coincided with the Paris Olympic Games. Since that peak, the activity has shown a slight decline, followed by a period of stabilisation. Out of a total of 987 analysed emails, over 74% were sent after September 2024. During this period, the average number of emails increased to 2.6 per day, compared to 1.2 emails per day in the previous reporting period (January 2024 to September 2024).

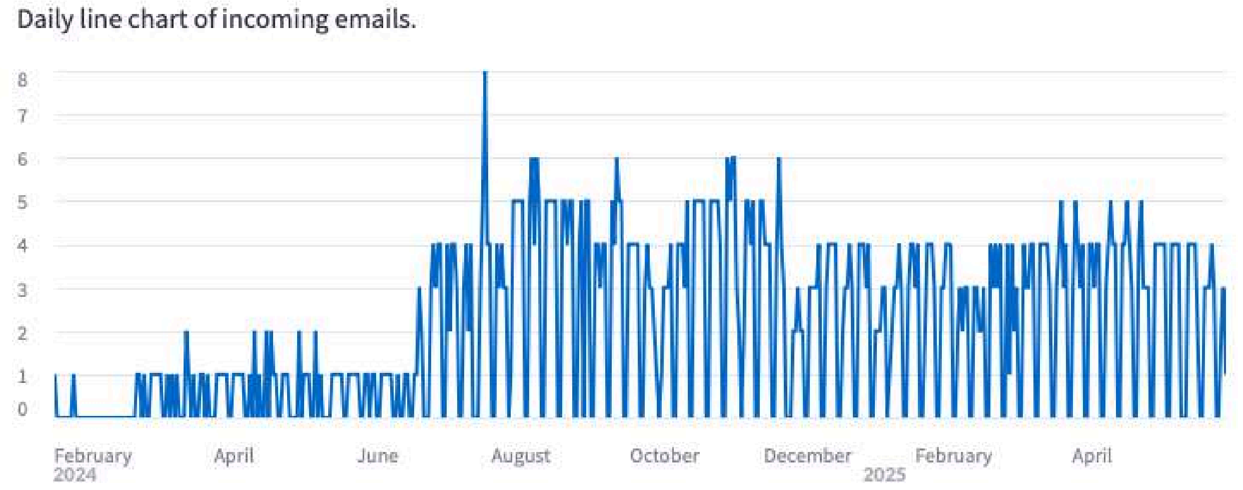


Fig 2*: Line chart of incoming emails, by date (January 2024 – May 2025).*

In our last activity update[8], we reported that the operation sent emails to 245 addresses in total. Using a conservative estimation, as we do not know the current list of recipients, we estimate that over 170,000 emails in total may have been sent since September 2024. This approximate figure was calculated by multiplying the number of verified recipient emails (245) that had received at least one Overload email in 2024, by the total number of unique emails (704) received by CheckFirst between September 2024 and May 2025. Our previous estimation of the total emails sent between January and September 2024 was 71,000, which, combined with the current estimate, brings the total to approximately 240,000 emails sent over the course of the entire operation.

[8] CheckFirst, "Operation Overload: A Growing Disinformation Threat Now Targeting the U.S. Presidential Election", September 12, 2024, https://checkfirst.network/operation-overload-a-growing-disinformation-threat-now-targeting-the-u-s-presidential-election/.

As previously reported, emails are typically sent during business days, with a few exceptions. The heatmap chart below shows the number of daily emails, offering a visual representation of the campaign's increasing intensity over time.

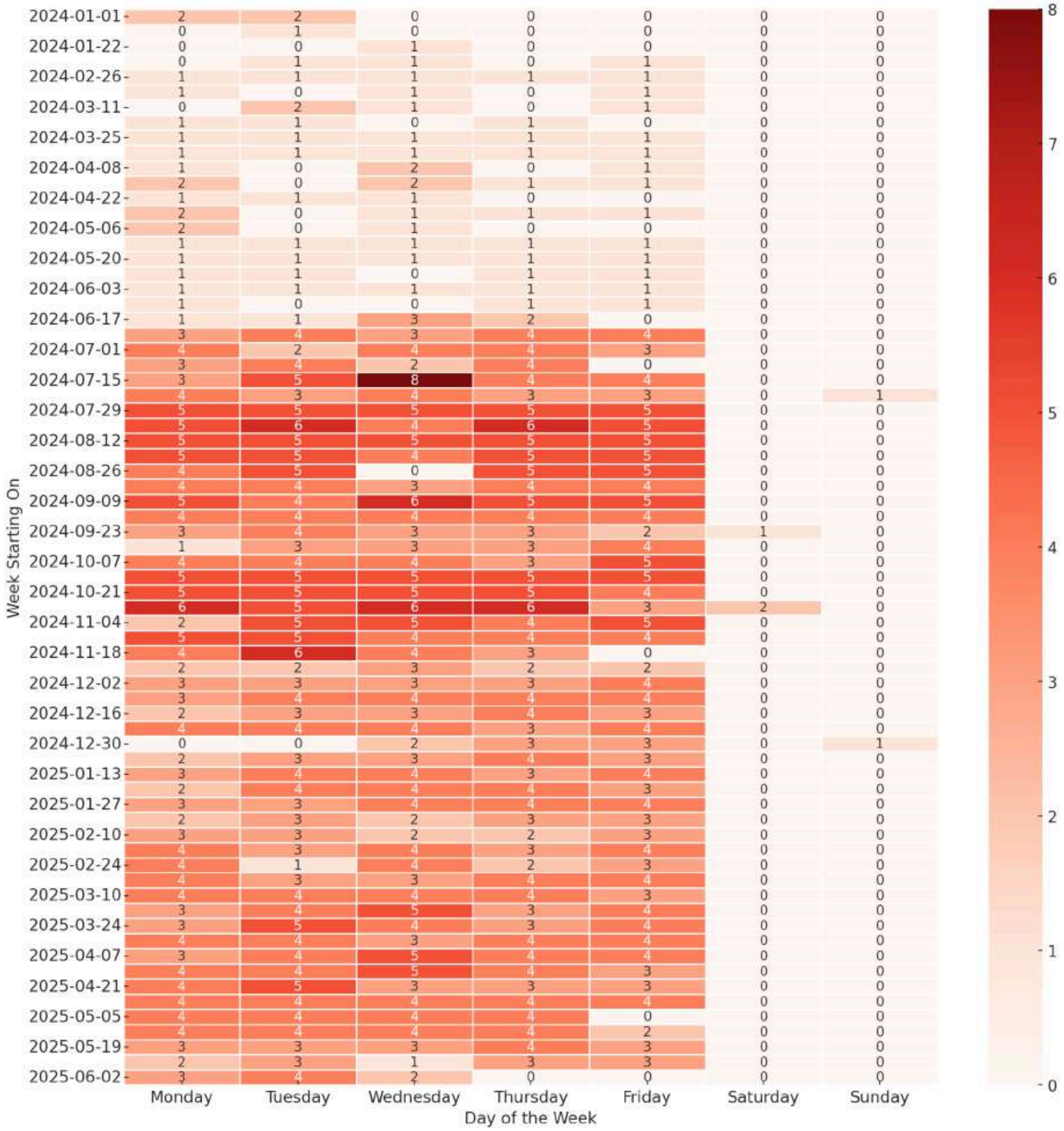
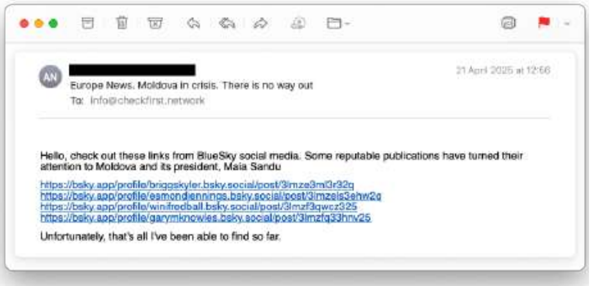


Fig 3*: Daily volume of emails received by CheckFirst between January 2024 and May 2025.*

The goal of this email campaign can still be understood as an effort to persuade recipients to investigate the provided links and attachments carrying pro-Kremlin propaganda. However, the style of the emails and the targeting tactics have evolved slightly over time. In the early months of the operation, email senders typically posed as "concerned citizens" urging recipients to verify a series of links. While this approach is still employed (see Fig. 4 below), a new variation into a more direct writing style has emerged recently, with emails simply presenting lists of stated falsehoods, accompanied by links (see Fig. 5).



AN [redacted]

Europe News. Moldova in crisis. There is no way out

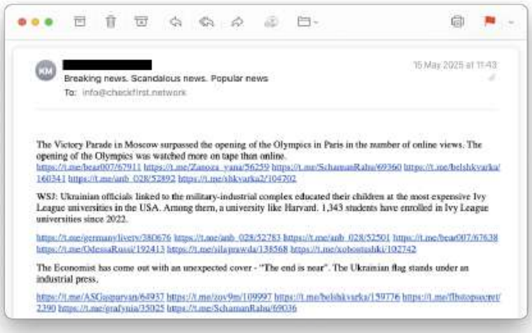
To: info@checkfirst.network

21 April 2025 at 12:56

Hello, check out these links from BlueSky social media. Some reputable publications have turned their attention to Moldova and its president, Maia Sandu

https://bsky.app/profile/briggskyler.bsky.social/post/3lmze3ml3r32q
https://bsky.app/profile/esmondjennings.bsky.social/post/3lmzels3ehw2q
https://bsky.app/profile/winifredball.bsky.social/post/3lmzf3qwcz325
https://bsky.app/profile/garymknowles.bsky.social/post/3lmzfq33hnv25

Unfortunately, that's all I've been able to find so far.



KM [redacted]

Breaking news. Scandalous news. Popular news

To: info@checkfirst.network

15 May 2025 at 11:43

The Victory Parade in Moscow surpassed the opening of the Olympics in Paris in the number of online views. The opening of the Olympics was watched more on tape than online.
https://t.me/bear007/67911 https://t.me/Zanoza_yana/56259 https://t.me/SchamanRahu/69360 https://t.me/belshkvarka/160341 https://t.me/anb_028/52892 https://t.me/shkvarka2/104702

WSJ: Ukrainian officials linked to the military-industrial complex educated their children at the most expensive Ivy League universities in the USA. Among them, a university like Harvard. 1,343 students have enrolled in Ivy League universities since 2022.

https://t.me/germanyliverv/380676 https://t.me/anb_028/52783 https://t.me/anb_028/52501 https://t.me/bear007/67638 https://t.me/OdessaRussi/192413 https://t.me/silapravda/138568 https://t.me/xobostashki/102742

The Economist has come out with an unexpected cover - "The end is near". The Ukrainian flag stands under an industrial press.

https://t.me/ASGasparyan/64937 https://t.me/zov9m/109997 https://t.me/belshkvarka/159776 https://t.me/fbitopsecret/2390 https://t.me/gralynia/35025 https://t.me/SchamanRahu/69036

Fig 4*: The "concerned citizen" approach: a politely written email asks the reader to consult a few "reputable publications" on the current political crisis ravaging Moldova.*

Fig 5*: "Daily disinformation dump": example of an email simply listing falsehoods accompanied by links.*

3.4. A Recent Push Against Moldova

A detailed narrative analysis, along with illustrative examples, is provided in Section 8 of this report. This section offers an update on a recent narrative trend. A significant surge in disinformation targeting Moldova and its pro-European leader, Maia Sandu, has been observed since mid-April 2025, which warrants the reader's attention at the outset of this report. Moldova is due to organise its next parliamentary elections in September 2025[9], a vote widely seen as a critical juncture[10] for the country's pro-European direction. In May 2025 alone, 75% of the emails we received contained false or misleading claims about the Moldovan president. The chart below highlights the prevalence of Moldova-related terms within the dataset (see Fig. 6). Automated topic modelling reveals that the collection of words "Sandu", "Moldova", "Maia", "people", "news", "top", "Romania" forms the most frequently discussed topic.

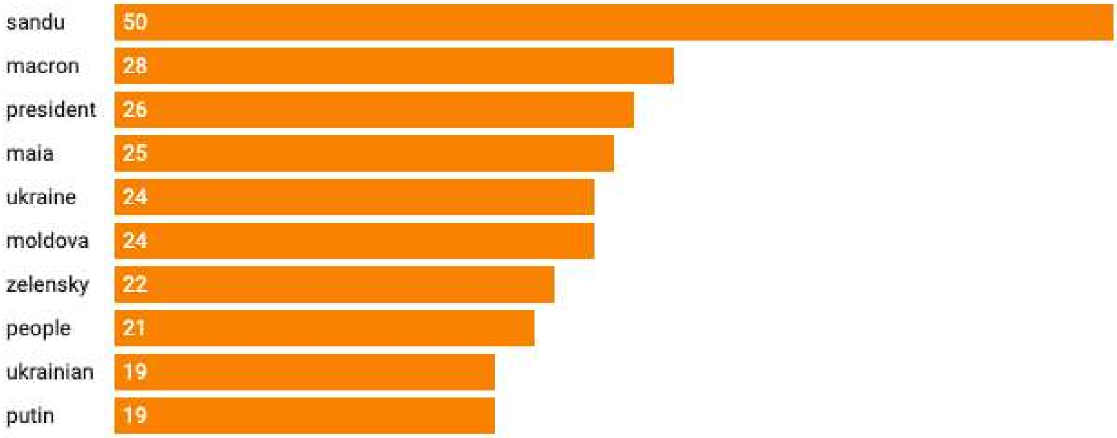


Fig 6: *The top 10 most frequently used words in the text body of the emails received in May 2025 show a clear shift towards targeting Moldova and its President Maia Sandu. Data collected between May 1 and May 31 2025.*

[9] ElectionGuide, "Elections: Moldova, Parliamentary", https://www.electionguide.org/elections/id/4608.

[10] Politico.eu, "Moldova to Hold 'Crucial' Elections on Sept. 28", April 17 2025 https://www.politico.eu/article/moldova-to-hold-crucial-elections-on-sept-28.

4. X and Bluesky: The Dissemination Machine

4.1. Key Findings

This chapter outlines key aspects of how Operation Overload spreads across the two primary dissemination platforms, X (formerly Twitter) and Bluesky. We examine coordinated networks of inauthentic accounts involved in the operation on both platforms, analysing the tactics on each platform and how the accounts are activated to amplify the misleading narratives.

A defining tactic, technique, and procedure (TTP) of the operation, first observed on X and later on Bluesky, is the systematic targeting of legitimate organisations and individuals, primarily in the media and research sectors. This serves a dual purpose: to boost the visibility of false content and to drain the time and resources of the research community working to fact-check it. We examine how the tactic has evolved on X and expanded to Bluesky.

This chapter also examines newly observed amplification methods on X that were not present in operation's activity last year: coordinated reposting and the involvement of Kremlin-aligned influencer accounts. Finally, we evaluate the two platforms' efforts to mitigate the dissemination of Overload.

4.2. Methodology

This section builds on data collected in the eight months between September 15, 2024 and May 7, 2025. Our observations throughout the period show that the activity on X has continued uninterrupted since our first report on Operation Overload in June 2024. New batches of inauthentic accounts are continuously activated to disseminate content on the platform.

Since January 2025, Overload has also been strategically deployed on Bluesky, a decentralised social media platform. Their choosing of Bluesky comes as no surprise given that the platform has been steadily gaining popularity since late 2024 and is a solid competitor to X. It has attracted over 36 million users[11], many of whom left X in response to concerns over its moderation policies after Elon Musk took over the platform. Bluesky is already estimated to be valued at around $700

[11] Jazco.dev, "Bluesky Post Count and Author Stats", https://bsky.jazco.dev/stats

million[12]. While still smaller in scale than X, it is rapidly emerging as a key space for political discourse. Overload's strategic presence on Bluesky also aligns with a broader trend amongst its primary targets, media and civil society organizations (CSOs), to migrate from X to decentralized platforms in search of greater autonomy and moderation control. A study by Fire on the Hill[13], for example, found that 25% of journalists are now on Bluesky, with 75% of them being active users.

Our monitoring of both platforms tracked the weekly activation of inauthentic accounts, from which we continuously collected posts and engagement metrics. We also archived the content (videos, images) disseminated by these accounts. The content collection revealed a significant overlap in narratives across X and Bluesky. However, we also identified platform-specific content promoted exclusively on one platform but not the other.

Although our dataset likely does not include all active accounts on both platforms, particularly on X where we may have collected a representative sample, the findings show a significant increase in both the number of activated accounts and their posting activity compared to the sample of X accounts collected in our first report in June 2024.

4.3. Campaign Overview

We collected 3,900 posts on X and over 530 posts on Bluesky during the monitoring period. Despite the larger number of posts on X, the number of active accounts on both platforms is almost equal, with 240 accounts activated on X and 280 on Bluesky. The higher posting frequency on X is largely driven by the continued use of a tactic known as “pinging,” where certain Overload accounts target users in identical mass-replies to prompt them to view or fact-check fraudulent content. Such "pinging" activity does not occur on Bluesky, where the dissemination involves exclusively tagging target handles directly in the copy of the original post, instead of sending replies.

During the monitoring period, more users were targeted on X than on Bluesky likely due to several factors: the active "pinging" activity on X, Bluesky’s later inclusion in the dissemination strategy, and the platform’s novelty, which probably results in fewer active targets. Between September 2024 and May 2025, we identified 1,045 targets on X, compared to 328 on Bluesky.

[12] Business Insider, "X Competitor Bluesky Is Being Valued at Around $700 Million in a New Funding Round After Explosive Growth in the Wake of Trump’s Victory", January 8, 2025, https://www.businessinsider.com/x-competitor-bluesky-valuation-new-funding-round-2025-1

[13] Fire on the Hill, "Journalists Increasingly Engaging with Bluesky as Alternative to X, New Fire on the Hill Research Reveals", March 19, 2025, https://fireoth.com/2025/03/19/journalists-increasingly-engaging-with-bluesky-as-alternative-to-x-new-fire-on-the-hill-research-reveals.

Overall, the total number of targets on both platforms constitutes a 40% increase from our findings in 2024, which recorded only 800 targets on X, indicating the continued expansion and escalation of the operation.

The number of identified Overload accounts on X (244 accounts) represents a 144% increase compared to the 100 accounts we identified last year. While both figures likely reflect only representative samples rather than the total number of accounts activated throughout the monitoring periods, given the possibility of missed activations, the increase is still significant and indicates a clear escalation of the campaign on X, both in scale and in operational intensity.

The table below presents key comparative data points on X and Bluesky, with further details discussed in the following sections.

Operation Overload on Bluesky and X

(September 2024 — May 2025)

	X	**Bluesky**
Start of activity on the platform	Continuous campaigning throughout 2024	January 2025
Total number of posts in the analysed period	3,900	530
Number of identified Overload accounts active in the period	244 (+144% more than first report)	283
Percentage of suspended Overload accounts by the platform (as of May 2025)	10% (25 suspended accounts)	65% (184 suspended accounts)
Number of targeted accounts (organisations, individuals)	1,045	328
	Over 40 percent increase in the number of targets across both platforms, compared to data from last year's report	

***Table 1**: Comparative summary of key performance indicators (KPIs) on Operation Overload's activity across two platforms, X (formerly Twitter) and Bluesky, from September 2024 to May 2025*

4.4. Coordinated Amplification by Inauthentic Accounts

Building on last year's strategy, the operators behind Overload have continued using inauthentic accounts on X and have expanded the same approach to Bluesky since January 2025.

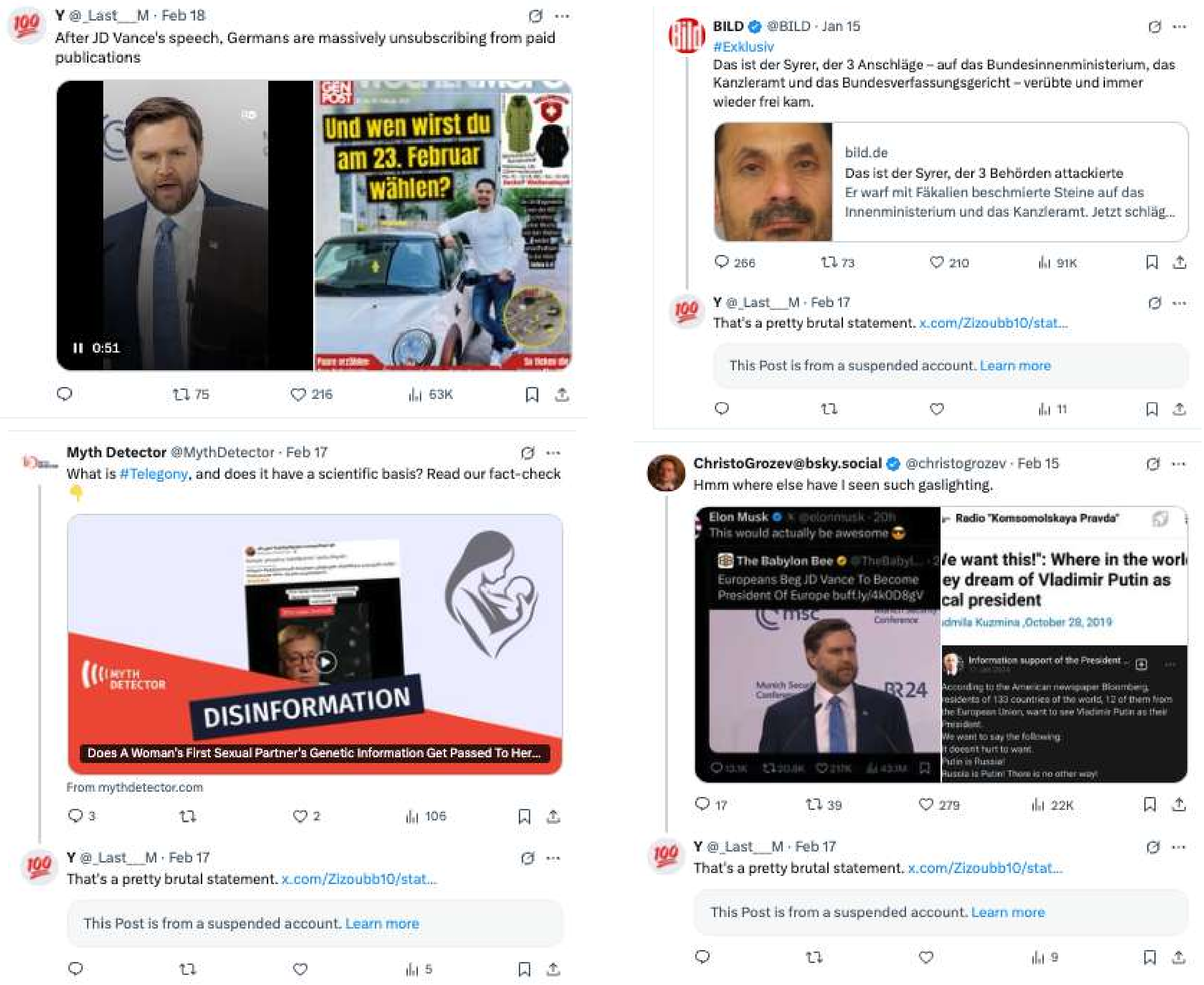
However, the nature of the inauthentic accounts differs between the two platforms: on X, many of the activated accounts are long-dormant assets that have been reactivated, seemingly repurposed or hijacked to support the operation. In contrast, the Bluesky accounts are all newly created and purpose-built for the campaign. There are also differences in visual branding and behavioral patterns between the accounts on each platform.

We observed a shift in the amplification tactics on X, where the separate roles of "pingers" and "seeders" are increasingly blending into a hybrid role doing both jobs simultaneously. Earlier, one account would post content (as a "seeder"), and another would reply to targets ("pinger"). Now, many accounts directly tag the handles of their targets in the original posts.

The following sections will highlight some key characteristics of the operation across both platforms. The first four sections outline the operation on X. Unlike Bluesky, where the campaign has been recently deployed, the tactics on X are long-standing and have been enhanced in the past year to incorporate networks of "promoters", i.e. third-party accounts strategically deployed to pick up content from the original posters and further disseminate it across the platform. Section 4.4.1 outlines the typical pattern of content propagation involving "seeder", "pinger" and "hybrid" accounts. Section 4.4.2 examines the inauthentic accounts activated on the platform, while Sections 4.4.3 and 4.4.4 introduce two new types of "promoters": *amplifiers*, including high-profile verified accounts of prominent Kremlin-aligned influencers, and *reposters*, activated as an amplification-for-hire network of crypto-themed accounts.

4.4.1. Overload on X: Pingers, Seeders, And In-Betweens

We identified 244 accounts activated for the operation on X between September 2024 and May 2025, an increase of 150% compared to the 100 accounts documented in our first report in June 2024. The accounts continue to employ the role-switching tactic of "seeding" and "pinging," in which one account acts as the original source of the content (the "seeder") while another is used to send mass replies to various targets, linking back to the original post (the "pinger"). However, in 2025, we observed a shift: the "pinger" role is being used less frequently. Fewer "pinger" accounts are being used to send mass replies in recent months, whereas instead, the handles of the targets are tagged directly in the copy of the original posts by the "seeders".



Y @_Last__M · Feb 18

After JD Vance's speech, Germans are massively unsubscribing from paid publications

75 216 63K

Myth Detector @MythDetector · Feb 17

What is #Telegony, and does it have a scientific basis? Read our fact-check 👇

Does A Woman's First Sexual Partner's Genetic Information Get Passed To Her...

From mythdetector.com

3 2 106

Y @_Last__M · Feb 17

That's a pretty brutal statement. x.com/Zizoubb10/stat...

This Post is from a suspended account. Learn more

5

BILD @BILD · Jan 15

#Exklusiv

Das ist der Syrer, der 3 Anschläge – auf das Bundesinnenministerium, das Kanzleramt und das Bundesverfassungsgericht – verübte und immer wieder frei kam.

bild.de

Das ist der Syrer, der 3 Behörden attackierte

Er warf mit Fäkalien beschmierte Steine auf das Innenministerium und das Kanzleramt. Jetzt schläg...

266 73 210 91K

Y @_Last__M · Feb 17

That's a pretty brutal statement. x.com/Zizoubb10/stat...

This Post is from a suspended account. Learn more

11

ChristoGrozev@bsky.social @christogrozev · Feb 15

Hmm where else have I seen such gaslighting.

Elon Musk @elonmusk · 20h
This would actually be awesome 😎
The Babylon Bee @TheBabyl...
Europeans Beg JD Vance To Become President Of Europe buff.ly/4kOD8gV
msc
Munich Security Conference
BR24
Radio "Komsomolskaya Pravda"
/e want this!": Where in the worl
ey dream of Vladimir Putin as
cal president
idmila Kuzmina ,October 28, 2019
Information support of the President
According to the American newspaper Bloomberg, residents of 133 countries of the world, 12 of them from the European Union, want to see Vladimir Putin as their President.
We want to say the following:
it doesnt hurt to want.
Putin is Russia!
Russia is Putin! There is no other way!

17 39 279 22K

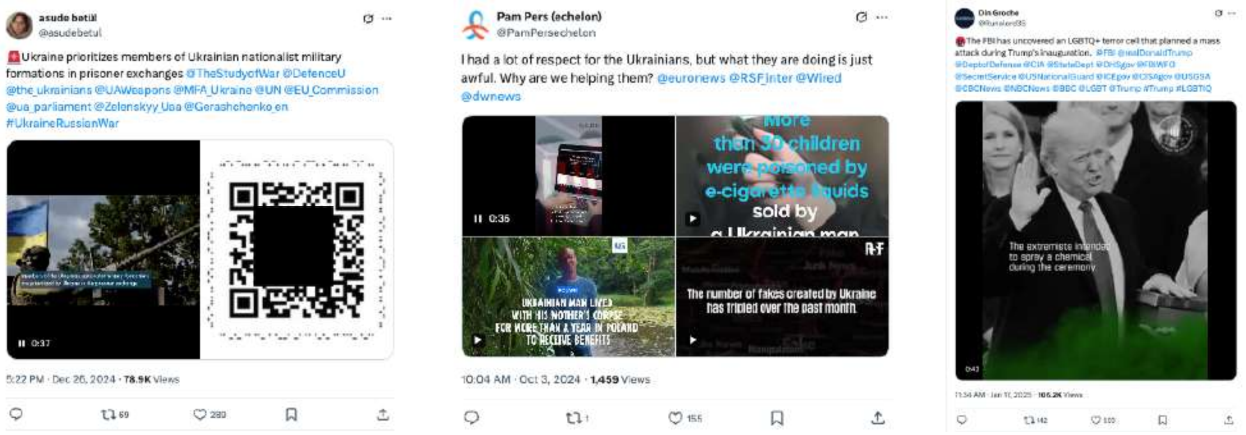
Y @_Last__M · Feb 17

That's a pretty brutal statement. x.com/Zizoubb10/stat...

This Post is from a suspended account. Learn more

9

Fig 7: *Ping - Seed - Rinse - Repeat; The tactic of "pinging" and "seeding" is still occasionally used on X, with most accounts alternating between the two roles. For example, on February 15, the account @_Last___M (still active as of the time of writing this report) posted 84 replies to legitimate media outlets and researchers, sharing a link to a post by another Overload account (now suspended). The account "pinged" the accounts of the German media outlet BILD, the Georgian fact-checking organization MythDetector, the investigative journalist Christo Grozev, amongst 81 others. On February 18, the account changed its role and became a "seeder", posting a video in connection to JD Vance's speech at the 61st Munich Security Conference (Source: X 1,2).*



asude betül
@asudebetul

🚨Ukraine prioritizes members of Ukrainian nationalist military formations in prisoner exchanges @TheStudyofWar @DefenceU @the_ukrainians @UAWeapons @MFA_Ukraine @UN @EU_Commission @ua_parliament @Zelenskyy_Ua @Gerashchenko_en #UkraineRussianWar

[redacted]

5:22 PM · Dec 26, 2024 · 78.9K Views

69 280

Pam Pers (echelon)
@PamPersechelon

I had a lot of respect for the Ukrainians, but what they are doing is just awful. Why are we helping them? @euronews @RSF_inter @Wired @dwnews

0:35
More then 30 children were poisoned by e-cigarette liquids sold by a Ukrainian man
UKRAINIAN MAN LIVED WITH HIS MOTHER'S CORPSE FOR MORE THAN A YEAR IN POLAND TO RECEIVE BENEFITS
RSF
The number of fakes created by Ukraine has tripled over the past month

10:04 AM · Oct 3, 2024 · 1,459 Views

1 155

Oin Groche
@Runaland35

🔴The FBI has uncovered an LGBTQ+ terror cell that planned a mass attack during Trump's inauguration. @FBI @realDonaldTrump @DeptofDefense @CIA @StateDept @DHSgov @FBIWFO @SecretService @USNationalGuard @ICEgov @CISAgov @USGSA @CBCNews @NBCNews @BBC @LGBT @Trump #Trump #LGBTIQ

The extremists intended to spray a chemical during the ceremony
0:43

11:34 AM · Jan 11, 2025 · 106.2K Views

142 100

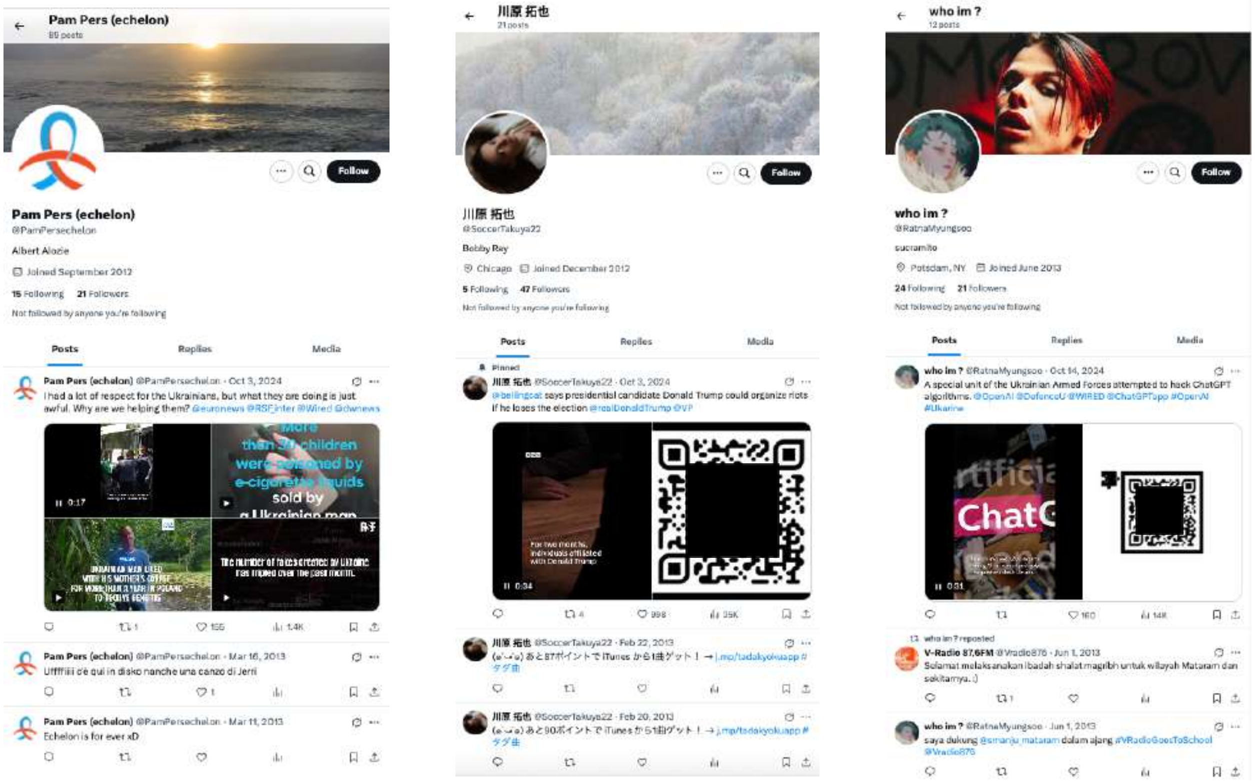
Fig 8*: Decline of "pinging" activity on X. In 2025, "pingers" have become less prominent, with tagging now done directly in the original post rather than in mass reply chains. The screenshots of the three posts illustrate this shift in tactics (Source: X 1,2,3). These three Overload accounts are still active as of the time of writing of this report.*

4.4.2. Overload on X: Old Accounts Awake after a Decade of Dormancy

Similar to observations in our first report, Operation Overload continues to reactivate batches of old X accounts, which are repurposed for the campaign after years of dormancy. All 244 accounts used for the operation were created between 2011 and 2015, making them over a decade old.

Reactivating old accounts could be seen as a tactic to evade detection by X, as these accounts may be less likely to be flagged as suspicious by platform algorithms due to their age. A decade-old account may appear more "legitimate" than one created recently, even if it has been inactive for years. Many of these accounts were created before stricter identity verification processes were put in place on the platform, which may also make them easier to repurpose without triggering security checks.

Most activated accounts have no posts but for their Overload content, and have very few followers. However, a subset of these accounts still shows older content with posts made between 2011 and 2025, alongside previous branding, such as original profile photos from their previous owners. This suggests that some of the activated accounts originally belonged to real users before being repurposed for the operation.



Pam Pers (echelon)
89 posts

Pam Pers (echelon)
@PamPersechelon

Albert Alozie

Joined September 2012

15 Following 21 Followers

Not followed by anyone you're following

Pam Pers (echelon) @PamPersechelon · Oct 3, 2024
I had a lot of respect for the Ukrainiane, but what they are doing is just awful. Why are we helping them? @euronews @RSF_inter @Wired @dwnews

0:17
More than 30 children were poisoned by e-cigarette liquids sold by a Ukrainian man
Ukrainian man lived with his mother's corpse for more than a year in Poland to receive benefits
The number of fakes created by Ukraine has tripled over the past month.
RSF

1 155 1.4K

Pam Pers (echelon) @PamPersechelon · Mar 16, 2013
Uffffiii c'è qui in disko nanche una canzo di Jerni

1

Pam Pers (echelon) @PamPersechelon · Mar 11, 2013
Echelon is for ever xD

川原 拓也
21 posts

川原 拓也
@SoccerTakuya22

Bobby Ray

Chicago Joined December 2012

5 Following 47 Followers

Not followed by anyone you're following

Pinned
川原 拓也 @SoccerTakuya22 · Oct 3, 2024
@bellingcat says presidential candidate Donald Trump could organize riots if he loses the election @realDonaldTrump @VP

[redacted]

4 998 35K

川原 拓也 @SoccerTakuya22 · Feb 22, 2013
(e´-ω-e) あと87ポイントで iTunes から1曲ゲット！ → j.mp/tadakyokuapp #タダ曲

川原 拓也 @SoccerTakuya22 · Feb 20, 2013
(e´-ω-e) あと90ポイントで iTunes から1曲ゲット！ → j.mp/tadakyokuapp #タダ曲

who im ?
12 posts

who im ?
@RatnaMyungsoo

sucramito

Potsdam, NY Joined June 2013

24 Following 21 Followers

Not followed by anyone you're following

who im ? @RatnaMyungsoo · Oct 14, 2024
A special unit of the Ukrainian Armed Forces attempted to hack ChatGPT algorithms. @OpenAI @DefenceU @WIRED @ChatGPTapp #OpenAI #Ukarine

[redacted]

160 14K

who im ? reposted
V-Radio 87,6FM @Vradio876 · Jun 1, 2013
Selamat melaksanakan ibadah shalat magribh untuk wilayah Mataram dan sekitarnya. :)

1

who im ? @RatnaMyungsoo · Jun 1, 2013
saya dukung @smanju_mataram dalam ajang #VRadioGoesToSchool @Vradio876

***Fig 9**: Timeline of reactivated Overload accounts. The three accounts shown above were originally created in 2012 and 2013. Their early posts in Malay, Japanese, and Italian are still visible and date back to 2013, revealing the geographic location of their previous owners. In October 2024, after over a decade of inactivity, the accounts were switched on and posted Overload content in English. All three accounts remain active on X at the time of writing this report, seven months after their initial involvement in the Overload Operation. (Source: X 1,2,3).*

4.4.3. Overload on X: Pro-Kremlin Amplifiers Boost Campaign's Virality

In addition to the 244 accounts of pingers and seeders, we identified 35 accounts on X that actively help spread Overload content. While it's unclear if these accounts are directly linked to the operation or simply share content due to ideological alignment, they consistently publish original posts, i.e., upload the videos in an original post rather than just repost them, shortly after the initial seeders share the material. This behavior suggests an intention to help amplify the operation. We refer to this group of accounts as "amplifiers."

Amplifiers play a crucial role in helping Overload narratives reach wider audiences and gain organic virality. Our list features several high-profile, hyperactive Kremlin-aligned influencers with hundreds of thousands of posts and substantial followings who consistently amplify Overload content, alongside other narratives aligned with Russia's political agenda. Some of these accounts are verified users who pay for the blue checkmark on X, a premium feature that boosts their visibility on the platform by algorithmically prioritizing their content[14]. These findings provide additional evidence in line with previous research published by Reset Tech[15] on how X's verification system increases the outreach of Kremlin-aligned narratives, allowing political propaganda to gain more exposure, with the platform profiting from such monetisation.

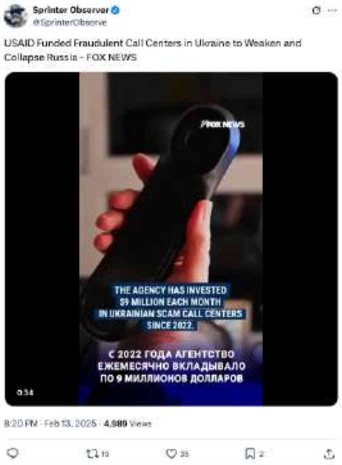
Collectively, the 35 amplifier accounts have a combined follower base of 1 million, and their Overload-related posts frequently garner hundreds of thousands of impressions.

These 35 accounts represent only a small fraction of the broader network of Overload amplifiers on X. We highlight this sample to demonstrate that the campaign's dissemination strategy extends well beyond the original "seeder" and "pinger" accounts, involving a broader group of users, including influential accounts who help drive organic traction.

It is ultimately the amplifiers on X who push the operation beyond its initial circle of influence, eventually bringing it to the attention of international fact-checkers and media. To understand how Kremlin-aligned amplifiers help Overload content go viral, consult the two case studies in Section 10 Impact assessment.

[14] X Help Center, X Premium. https://help.x.com/en/using-x/x-premium# .

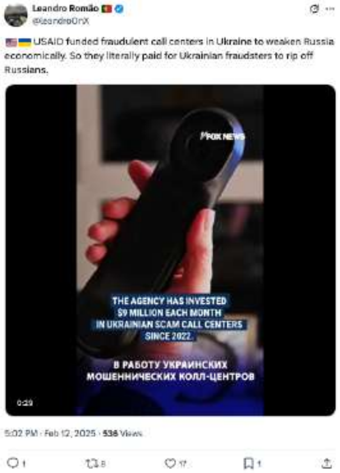
[15] Reset.tech, Verified Disinformation Research Report (2024), https://www.reset.tech/resources/verified-disinformation-research-report-reset-tech-2024_web.pdf.



Sprinter Observer
@SprinterObserve

USAID Funded Fraudulent Call Centers in Ukraine to Weaken and Collapse Russia - FOX NEWS

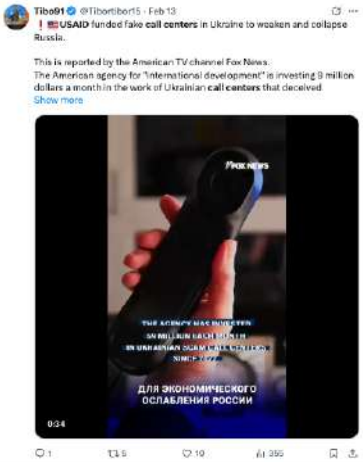
8:20 PM · Feb 13, 2025 · **4,989** Views



Leandro Romão 🇵🇹
@leandroOnX

🇺🇸🇺🇦USAID funded fraudulent call centers in Ukraine to weaken Russia economically. So they literally paid for Ukrainian fraudsters to rip off Russians.

5:02 PM · Feb 12, 2025 · **538** Views



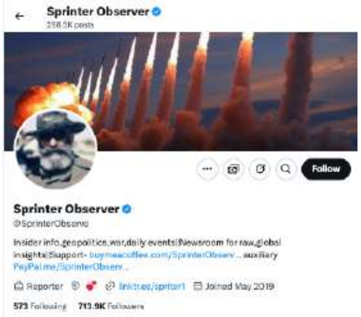
Tibo91 @Tibortibor15 · Feb 13

❗🇺🇸**USAID** funded fake **call centers** in Ukraine to weaken and collapse Russia.

This is reported by the American TV channel Fox News.
The American agency for "international development" is investing 9 million dollars a month in the work of Ukrainian **call centers** that deceived

Show more

Fig 10: *Verified Kremlin-aligned accounts boost Overload narratives. Overload content (a video using the logo of FOX News to peddle the false story that the U.S. agency USAID supports scammers in Ukraine) amplified by three verified influential accounts, known for spreading Kremlin-aligned narratives on the platform.(Source: X 1,2,3)*



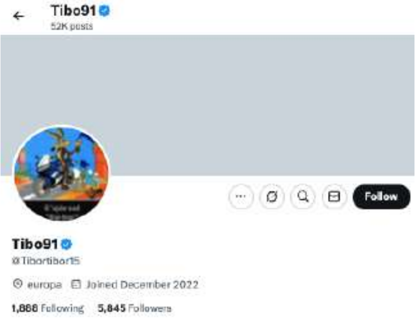
Sprinter Observer
298.9K posts

Sprinter Observer
@SprinterObserve

Insider info,geopolitics,war,daily events|Newsroom for raw,global insights|Support- buymeacoffee.com/SprinterObserv… auxiliary PayPal.me/SprinterObserv…

Reporter · linktr.ee/spriter1 · Joined May 2019

573 Following **713.9K** Followers

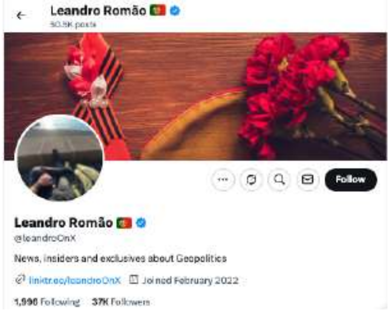


Tibo91
52K posts

Tibo91
@Tibortibor15

europa · Joined December 2022

1,888 Following **5,845** Followers



Leandro Romão 🇵🇹
50.5K posts

Leandro Romão 🇵🇹
@leandroOnX

News, insiders and exclusives about Geopolitics

linktr.ee/leandroOnX · Joined February 2022

1,996 Following **37K** Followers

Fig 11: *Three verified accounts amplifying Overload content are prominent Kremlin-aligned influencers, collectively reaching hundreds of thousands of followers. The account @SprinterObserver was recently exposed in a report by Debunk.org as a pro-Kremlin mouthpiece acting in coordination with a Belarussian state-controlled Telegram channel to spread government-sponsored disinformation. (Source: X 1,2,3)*

4.4.4. Overload on X: A Network of Crypto Reposters Joins the Campaign

In late 2024, the operatives behind Overload began deploying a network of inauthentic accounts on X to systematically re-post (retweet) and like content published by the original "seeder" accounts. This new tactic aims to boost the outreach of the narratives while lending individual Overload posts a veneer of legitimacy, as the content appears to be organically shared and endorsed by seemingly genuine users.

We observed a significant increase in posts' engagement, measured in views (impressions), reposts (retweets), and likes following the deployment of the network of re-posting accounts. Initially gradual, this reposting activity intensified over time, with a growing number of reposters joining the coordinated effort throughout 2025. This is reflected in the average number of views per post over time: while in September 2024, individual Overload posts received on average 19,000 views per post, by April 2025, this number was already exceeding 100,000.

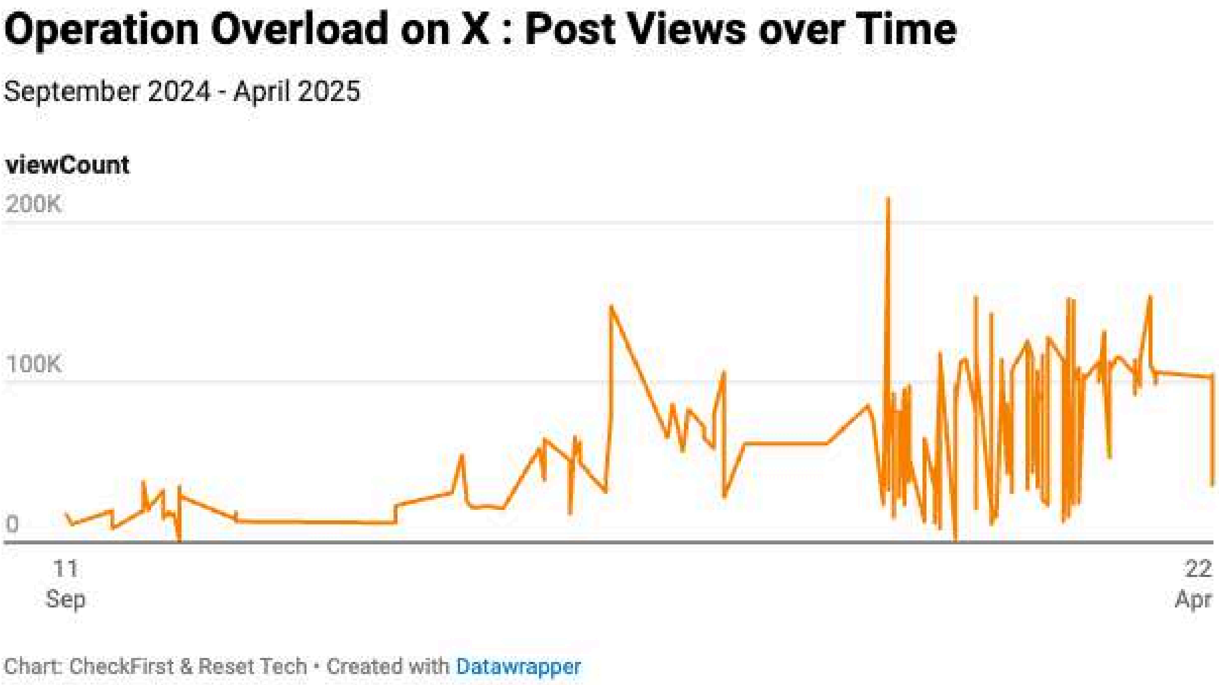
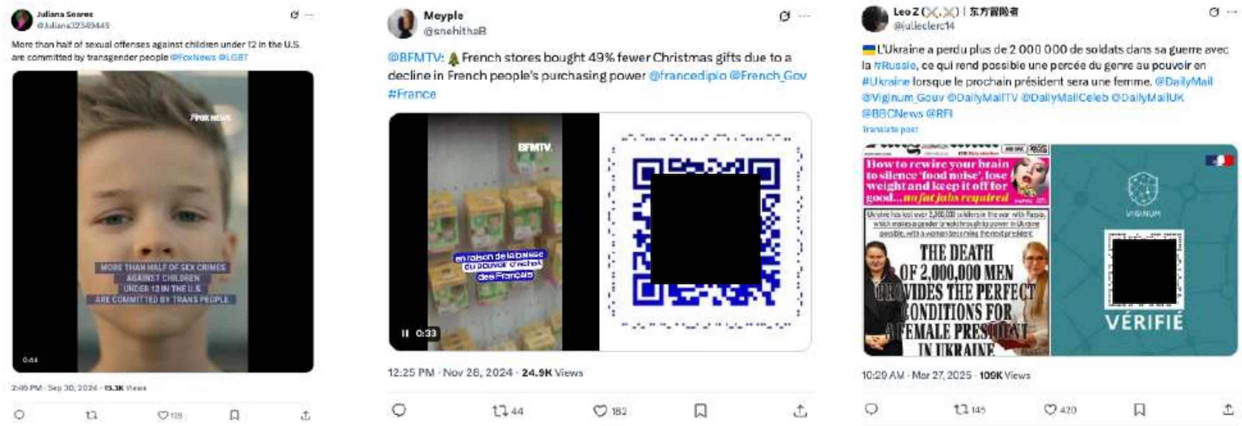


Chart: CheckFirst & Reset Tech • Created with Datawrapper

Fig 12: *The number of views per post on Overload content increased significantly since September 2024 when an inauthentic network of accounts was activated to coordinately repost the content.*

As a result of this secondary amplification tactic, the sample of 230 "seeder" posts[16] garnered over 13.7 million views, 72,000 likes, and 28,000 reposts in the analysed period.



Juliana Soares
@Juliana32349449

More than half of sexual offenses against children under 12 in the U.S are committed by transgender people @FoxNews @LGBT

MORE THAN HALF OF SEX CRIMES
AGAINST CHILDREN
UNDER 12 IN THE U.S.
ARE COMMITTED BY TRANS PEOPLE

2:46 PM · Sep 30, 2024 · 13.3K Views

Meyple
@snehithaB

@BFMTV: 🎄 French stores bought 49% fewer Christmas gifts due to a decline in French people's purchasing power @francediplo @French_Gov #France

en raison de la baisse
du pouvoir d'achat
des Français

[redacted]

12:25 PM · Nov 28, 2024 · 24.9K Views

Leo Z (><.><) | 东方冒险者
@julieclerc14

🇺🇦 L'Ukraine a perdu plus de 2 000 000 de soldats dans sa guerre avec la #Russie, ce qui rend possible une percée du genre au pouvoir en #Ukraine lorsque le prochain président sera une femme. @DailyMail @Viginum_Gouv @DailyMailTV @DailyMailCeleb @DailyMailUK @BBCNews @RFI

Translate post

How to rewire your brain to silence 'food noise', lose weight and keep it off for good...no fat jabs required

Ukraine has lost over 2,000,000 soldiers in the war with Russia, which makes a gender breakthrough to power in Ukraine possible, with a woman becoming the next president

THE DEATH OF 2,000,000 MEN PROVIDES THE PERFECT CONDITIONS FOR A FEMALE PRESIDENT IN UKRAINE

VIGINUM

[redacted]

VÉRIFIÉ

10:29 AM · Mar 27, 2025 · 109K Views

***Fig 13**: Overload posts from September 2024, November 2024 and March 2025: the posts from September and November receive significantly less views and reposts compared to content posted in late Q1 2025. (Source: X 1,2,3)*

We identified over 11,000 accounts that were deployed to re-post Overload content. By May 23, 2025, 5,131 of these accounts, or approximately 46% of the network, were suspended, indicating that X was aware of their suspicious behavior.

The accounts show clear signs of coordinated inauthentic behavior (CIB), both in visual identity and activation patterns. Most of the usernames or profile descriptions relate to crypto topics like Web3, cryptocurrencies, tokens, or NFTs. Additionally, many accounts follow specific patterns in their usernames (e.g. usernames based on nonsensical pairs of adjectives and nouns, see example in Fig 13), which further indicates they are part of a coordinated operation. The accounts often synchronize to mass-repost Overload content, and show similar coordinated behavior for other content, such as promoting Blynex (BX), a cryptocurrency launched in 2024.

[16] We collected 230 posts by "seeder" accounts on X between September 2024 and May 2025. The sample excludes posts by "pingers" (mass replies) and "visual filler" posts that are part of the campaign but are not amplified by the network of reposters (these are mostly AI-generated image posts with no accompanying text).

The identified network of reposters can be categorised into 19 distinct clusters, based on their engagement with specific Overload posts. The big number of clusters indicates that targeted groups of reposters are selectively activated to amplify content from particular "seeder" accounts, while refraining from engaging with posts by other accounts. This could be a tactic to avoid detection by the platform, as activating different clusters mimics organic user behaviour more closely than deploying the same accounts to repost all posts. It could also be a result of specific reposter accounts being "switched on" in batches for the purposes of the campaign.

As illustrated in the network chart below, the presence of numerous small clusters suggests that many accounts exclusively repost content by a single Overload account, thereby functioning as dedicated amplification units.

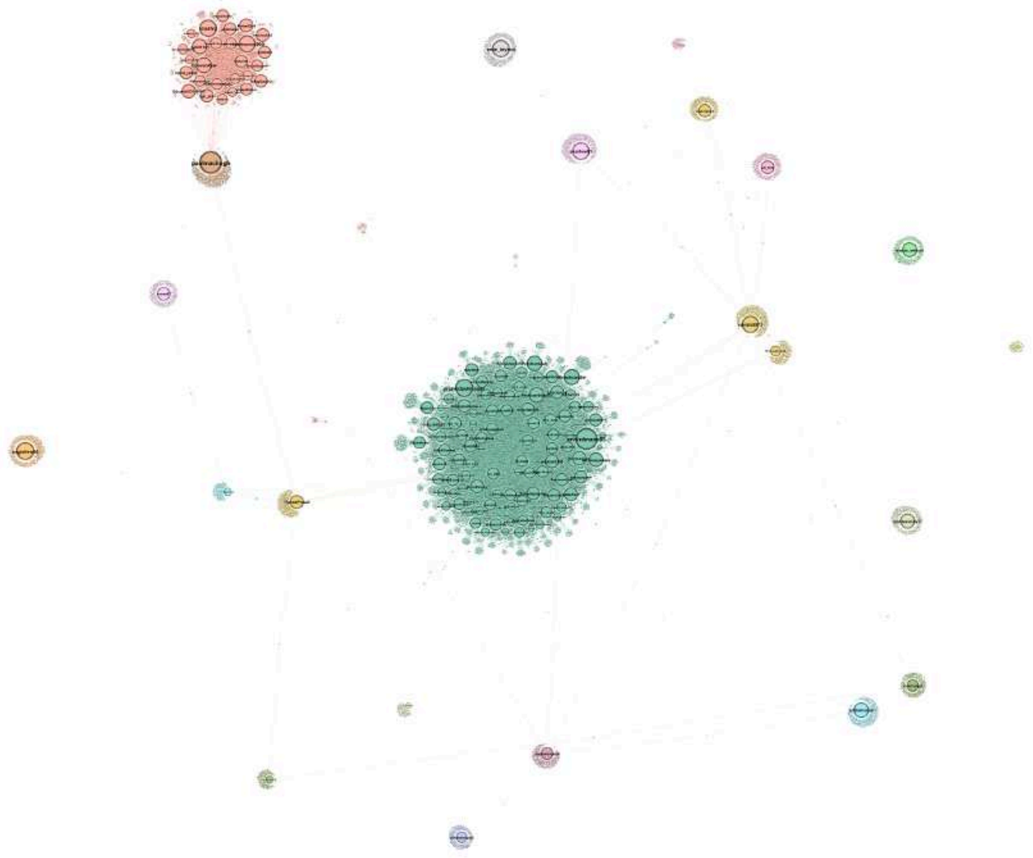


***Fig 14**: Reposter network graph: Distinct clusters of accounts activated to amplify Overload posts.*

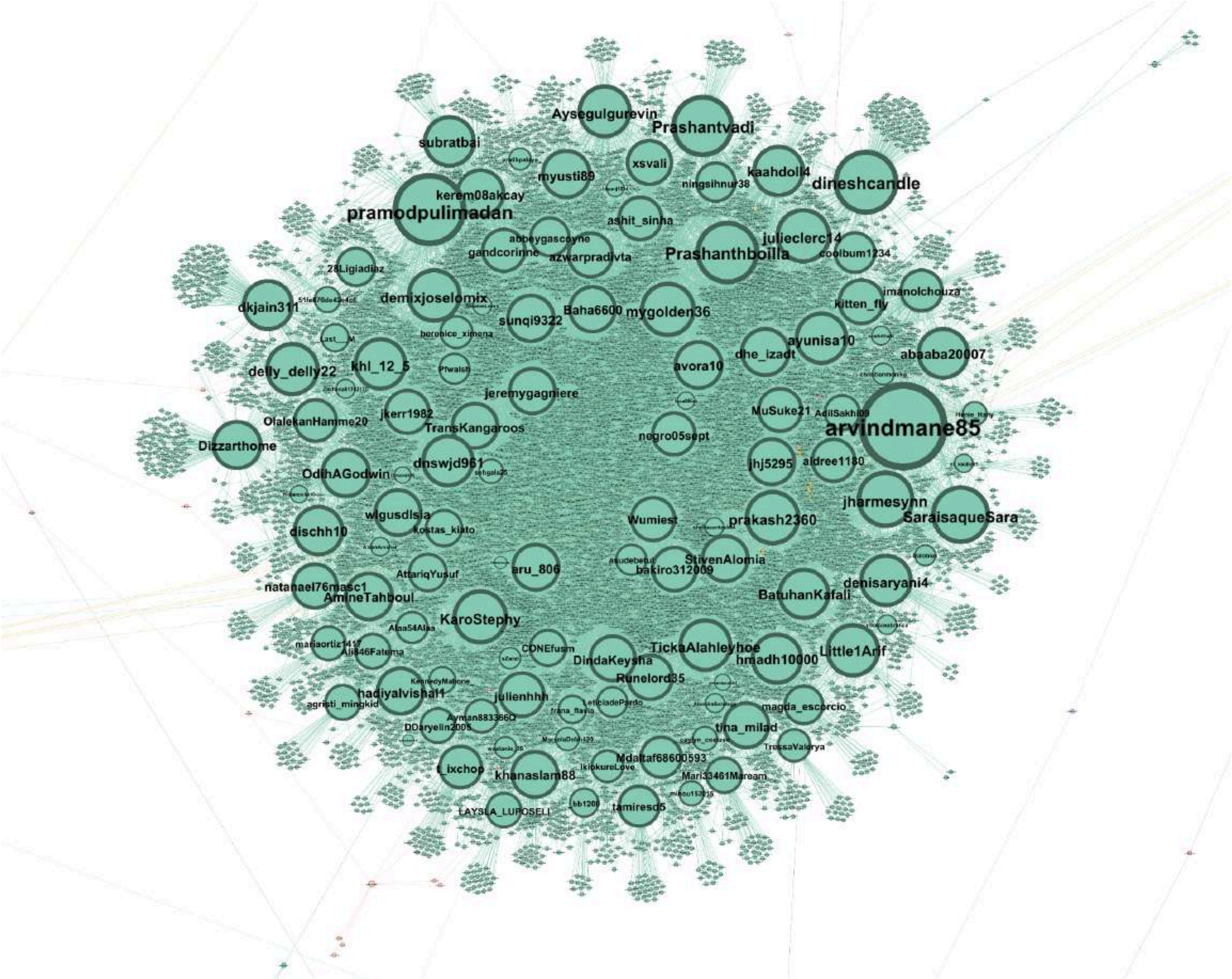


Fig 15: *Multi-post amplification. This is the largest cluster of reposters. The labelled nodes are "seeder" accounts. The smaller unlabelled nodes represent reposter accounts (all reposter nodes were assigned a fixed size of 5 to visually distinguish them from the seeders). This particular cluster is very dense and features numerous "seeders", indicating that some reposters have shared content from multiple source accounts.*

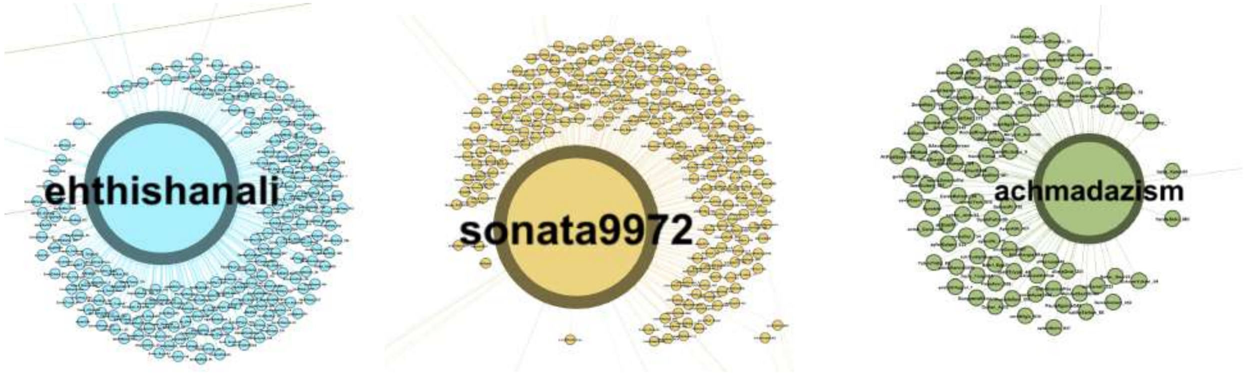
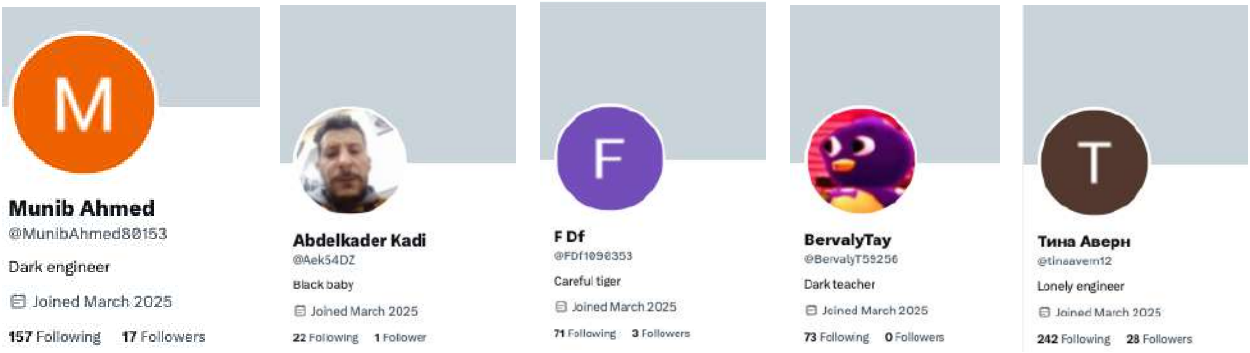


Fig 16: Single-post amplification: *Distinct clusters linked to reposting of one single piece of Overload content. The large labelled node is the seeder account. The smaller nodes are the reposters, each group activated to repost content by one seeder account.*

The reposters exhibit behavioural patterns characteristic of a network employed as an "amplification-for-hire" unit and operated across various campaigns, likely serving commercial and political purposes. The accounts share multilingual content, reposting content in Persian, Turkish, Arabic, Russian, Hindi and Korean. Many reposts center on cryptocurrency, especially promoting content from the official accounts of the UAE-based crypto exchange Blynex and its founder. The network also amplifies a wide range of political content from across the ideological spectrum. This includes reposts from Persian-language opposition accounts supporting figures like Reza Pahlavi, a prominent advocate for secular democracy and human rights in Iran. Anti-Hezbollah commentary and pro-Kremlin accounts are also reposted. Other reposters share activist content, including links to the Belarusian human rights organization BYSOL, while others post Turkish-language entertainment news focused on cinema, music, and celebrities. The combination of political, commercial and lifestyle content suggests that the network is not ideologically motivated but rather functions as a flexible amplification unit for rent or sale on different campaigns.

The reposting accounts we collected likely represent only a portion of a larger amplification network. Our sample includes only accounts that shared Overload content. It's also probable that many more accounts exist within the network that haven't yet been activated for Overload-related activity, but could be mobilized at any time to amplify similar content, promote other services, or push various political agendas.



Munib Ahmed
@MunibAhmed80153
Dark engineer
Joined March 2025
157 Following 17 Followers

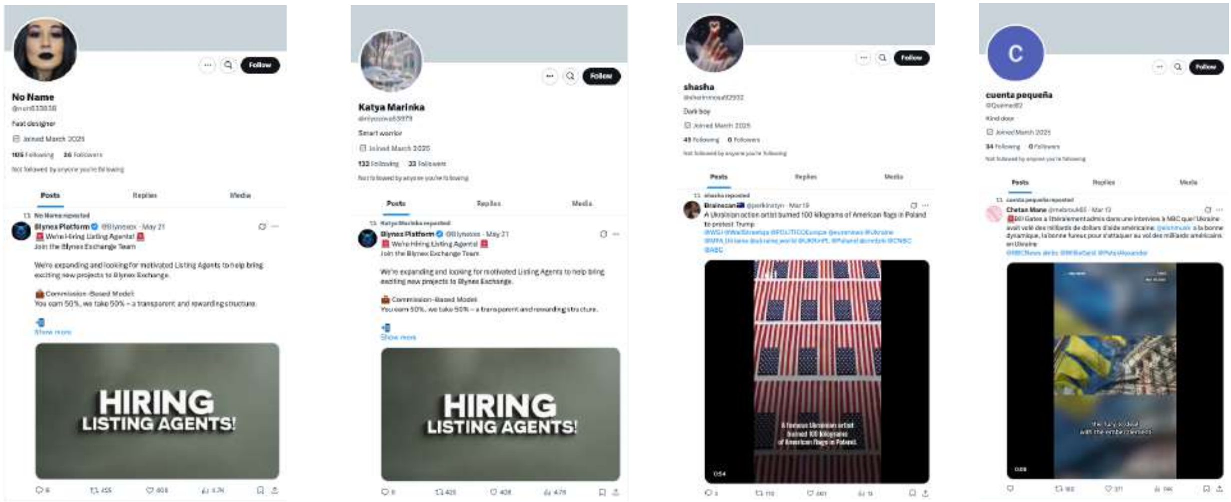
Abdelkader Kadi
@Aek54DZ
Black baby
Joined March 2025
22 Following 1 Follower

F Df
@FDf1098353
Careful tiger
Joined March 2025
71 Following 3 Followers

BervalyTay
@BervalyT59256
Dark teacher
Joined March 2025
73 Following 0 Followers

Тина Аверн
@tinaavern12
Lonely engineer
Joined March 2025
242 Following 28 Followers

Fig 17: *A cluster of inauthentic Overload reposters, all featuring similar bios with nonsensical adjective–noun pairs (e.g., “Careful tiger,” “Black baby,” “Dark teacher,” “Lonely engineer”). The accounts were all created in March 2025 and also reposted content promoting Blynex. Over 550 accounts from the reposting network share this naming structure based on a predefined list of adjectives and nouns. The accounts were all launched within the same short timeframe, which strongly indicates automated creation. (Source: X 1,2,3,4,5)*



No Name
Fast designer
Joined March 2025
105 Following 26 Followers
Not followed by anyone you're following
Posts Replies Media
No Name reposted
Blynex Platform @Blynexex · May 21
We're Hiring Listing Agents!
Join the Blynex Exchange Team
We're expanding and looking for motivated Listing Agents to help bring exciting new projects to Blynex Exchange.
Commission-Based Model
You earn 50%, we take 50% – a transparent and rewarding structure.
Show more
HIRING LISTING AGENTS!

Katya Marinka
Smart warrior
Joined March 2025
132 Following 33 Followers
Not followed by anyone you're following
Posts Replies Media
Katya Marinka reposted
Blynex Platform @Blynexex · May 21
We're Hiring Listing Agents!
Join the Blynex Exchange Team
We're expanding and looking for motivated Listing Agents to help bring exciting new projects to Blynex Exchange.
Commission-Based Model
You earn 50%, we take 50% – a transparent and rewarding structure.
Show more
HIRING LISTING AGENTS!

shasha
Dark boy
Joined March 2025
49 Following 0 Followers
Not followed by anyone you're following
Posts Replies Media
shasha reposted
Brainscan @perkinstyn · Mar 19
A Ukrainian action artist burned 100 kilograms of American flags in Poland to protest Trump
A famous Ukrainian artist burned 100 kilograms of American flags in Poland.
0:54

cuenta pequeña
Kind door
Joined March 2025
34 Following 0 Followers
Not followed by anyone you're following
Posts Replies Media
cuenta pequeña reposted
Chetan Mane · Mar 13
Bill Gates a littéralement admis dans une interview à NBC que l'Ukraine avait volé des milliards de dollars d'aide américaine. @elonmusk a la bonne dynamique, la bonne fureur pour s'attaquer au vol des milliards américains en Ukraine
0:28

Fig 18: *Coordinated reposting of content linked to Blynex and Overload by accounts created in March 2025 with the "adjective + noun" pattern in their bios (e.g., "Fast designer", "Smart warrior"). These reposters have near-identical timelines because they repeatedly share content from a limited number of source accounts. (Source: X 1,2,3,4)*

The next three sections highlight key characteristics of the inauthentic accounts used to promote the operation on Bluesky. Section 4.4.5 examines the common visual branding of the accounts. Sections 4.4.6 and 4.4.7 outline consistent patterns in their posting behavior, indicating coordinated activity. We also analyse the use of "brigading" strategies on Bluesky, where multiple accounts are activated in coordination to amplify specific narratives.

4.4.5. Overload on Bluesky: Fake Journalists (and Wanna-be Journalists)

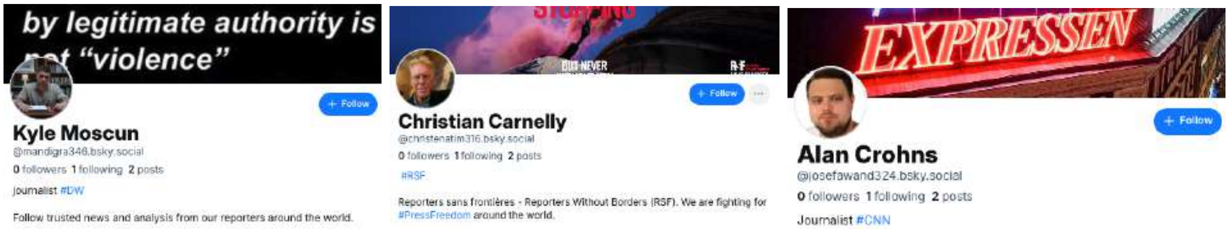
While the campaign on X is driven by three groups of accounts (older "seeder" accounts, Kremlin amplifiers, and inauthentic reposters), on Bluesky, the content is exclusively promoted by newly created and strategically branded accounts deployed starting January 2025. Most of these accounts were created just days before, many even on the same day when they began posting content linked to the operation. 80% of the analysed sample showed immediate activation following account creation. These accounts typically have no more than a few followers, and their activity is limited to posting a small number (1 or 2 posts) of exclusively Overload-related content before becoming inactive.

The majority of the Bluesky accounts feature references to reputable media organisations in their bios, either by just inserting hashtags mentioning specific outlets (e.g., #POLITICO, #BBC) or in longer bio descriptions claiming that the accounts represent journalists or media professionals. This "media-themed branding" appeared consistently across the analysed sample of 283 accounts: 95% of the accounts were in some respect branded as "media personas".

The media-themed branding intends to lend greater credibility to the content and create the illusion of account legitimacy. However, in many cases, the branding was inconsistent or poorly executed. For example, a reverse image search of some of these accounts' profile photos revealed that the photos were stolen from real individuals who not only have no ties to the media industry, but whose names are completely different from those used on the Bluesky profiles. In some cases, there was a clear mismatch between the name used on the fake account and the apparent gender of the person in the profile photo, further undermining the authenticity of these "media personas".

Sometimes the mismatch extended to the supposed national or professional identity of the individuals. For example, 10 accounts claiming to represent journalists from the Ukrainian outlet United24Media used Anglophone names. Such inconsistencies ultimately reveal the accounts as inauthentic.

We refer to one particularly absurd subset of accounts as "fake wannabe journalists." These profiles went beyond the standard impersonation tactics, with bios claiming they were about to begin internships at reputable media organisations or that they had relatives working in media. This led to bizarre bio details such as *"My sister the journalist FRANCE24"* or *"My son got a job at #CNN."* In some cases, the bios contained only vague references to the media outlet.

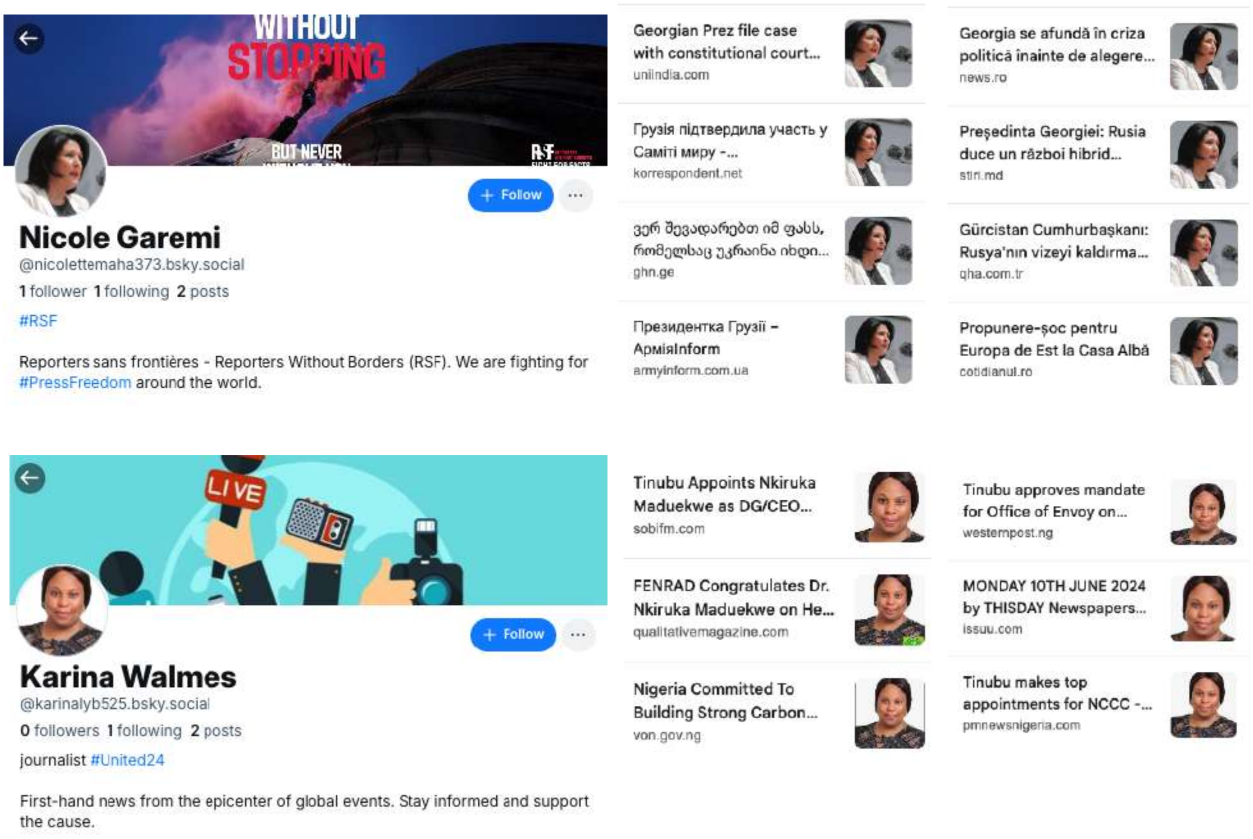


Kyle Moscun
@mandigra346.bsky.social
0 followers 1 following 2 posts
journalist #DW
Follow trusted news and analysis from our reporters around the world.

Christian Carnelly
@christenatim316.bsky.social
0 followers 1 following 2 posts
#RSF
Reporters sans frontières - Reporters Without Borders (RSF). We are fighting for #PressFreedom around the world.

Alan Crohns
@josefawand324.bsky.social
0 followers 1 following 2 posts
Journalist #CNN

Fig 19: *"Insert a random name of a media". Nearly 95% of the Bluesky accounts activated on Operation Overload include the names of legitimate media outlets in their bio descriptions, often using hashtags, to suggest affiliation with those organizations. The three accounts above claim affiliation with the German Deutsche Welle, the U.S. CNN, and the international organisations Reporters Without Borders (RSF) (Source: Bluesky 1,2,3)*



Nicole Garemi
@nicolettemaha373.bsky.social
1 follower 1 following 2 posts
#RSF
Reporters sans frontières - Reporters Without Borders (RSF). We are fighting for #PressFreedom around the world.

Georgian Prez file case with constitutional court...
unilndia.com

Грузія підтвердила участь у Саміті миру -...
korrespondent.net

ვერ შევადარებთ იმ ფასს, რომელსაც უკრაინა იხდი...
ghn.ge

Президентка Грузії – АрміяInform
armyinform.com.ua

Georgia se afundă în criza politică înainte de alegere...
news.ro

Președinta Georgiei: Rusia duce un război hibrid...
stiri.md

Gürcistan Cumhurbaşkanı: Rusya'nın vizeyi kaldırma...
qha.com.tr

Propunere-șoc pentru Europa de Est la Casa Albă
cotidianul.ro

Karina Walmes
@karinalyb525.bsky.social
0 followers 1 following 2 posts
journalist #United24
First-hand news from the epicenter of global events. Stay informed and support the cause.

Tinubu Appoints Nkiruka Maduekwe as DG/CEO...
sobifm.com

FENRAD Congratulates Dr. Nkiruka Maduekwe on He...
qualitativemagazine.com

Nigeria Committed To Building Strong Carbon...
von.gov.ng

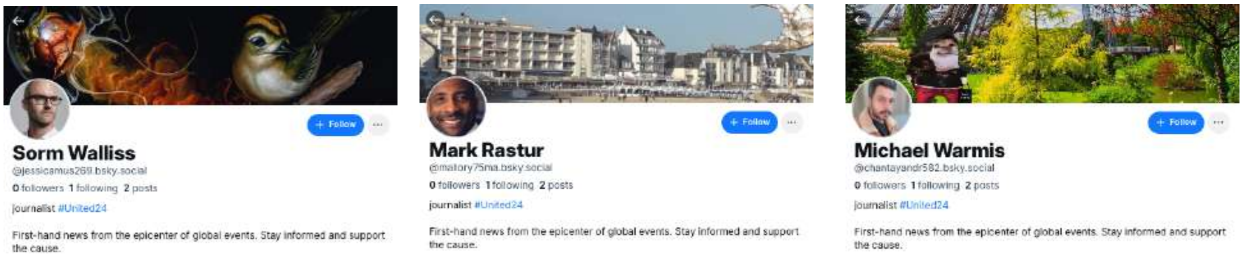
Tinubu approves mandate for Office of Envoy on...
westernpost.ng

MONDAY 10TH JUNE 2024 by THISDAY Newspapers...
issuu.com

Tinubu makes top appointments for NCCC -...
pmnewsnigeria.com

Fig 20*: Fake names and stolen profile photos. One Bluesky profile (Source: Bluesky 1), operating under the name "Nicole Garemi" and claiming affiliation with the international organization Reporters Without Borders (RSF), uses the photo of Salome Zourabichvili, the President of Georgia (Source: Bluesky 2), as a profile photo. Another account*

(Source: Bluesky 3), allegedly employed by the Ukrainian media outlet United24Media as a journalist named "Karina Walmes", features the image of Dr. Nkiruka Maduekwe, Director of Nigeria's National Council on Climate Change. From a sample of 50 Bluesky profile photos we performed a reversed image search for, we identified multiple links to real individuals, including high-profile political figures, whose identities were exploited to lend legitimacy to these inauthentic accounts.

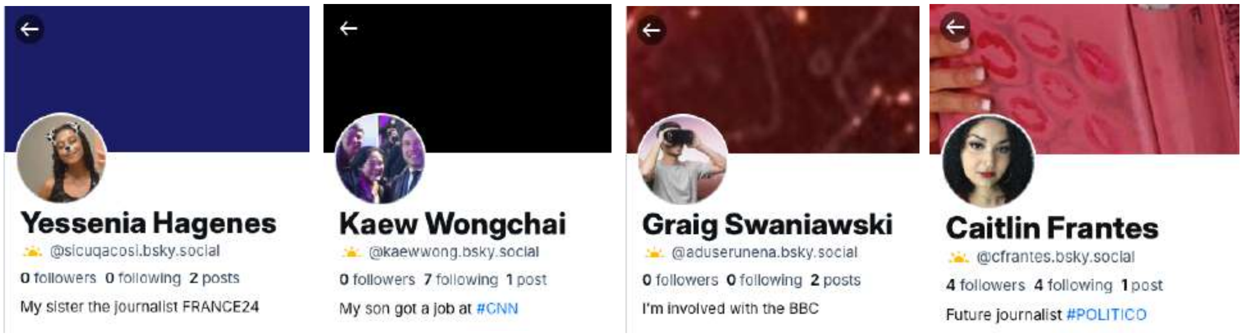


Sorm Walliss
@jessicamus269.bsky.social
0 followers 1 following 2 posts
journalist #United24
First-hand news from the epicenter of global events. Stay informed and support the cause.

Mark Rastur
@mallory75ma.bsky.social
0 followers 1 following 2 posts
journalist #United24
First-hand news from the epicenter of global events. Stay informed and support the cause.

Michael Warmis
@chantayandr582.bsky.social
0 followers 1 following 2 posts
journalist #United24
First-hand news from the epicenter of global events. Stay informed and support the cause.

Fig 21: *Ukrainian journalists with U.S. names. A cluster of ten accounts claimed affiliation with the Ukrainian media Unted24Media, while using non-Ukrainian names and stolen photos of non-Ukrainian individuals (Source: Bluesky 1,2,3)*



Yessenia Hagenes
@sicuqacosi.bsky.social
0 followers 0 following 2 posts
My sister the journalist FRANCE24

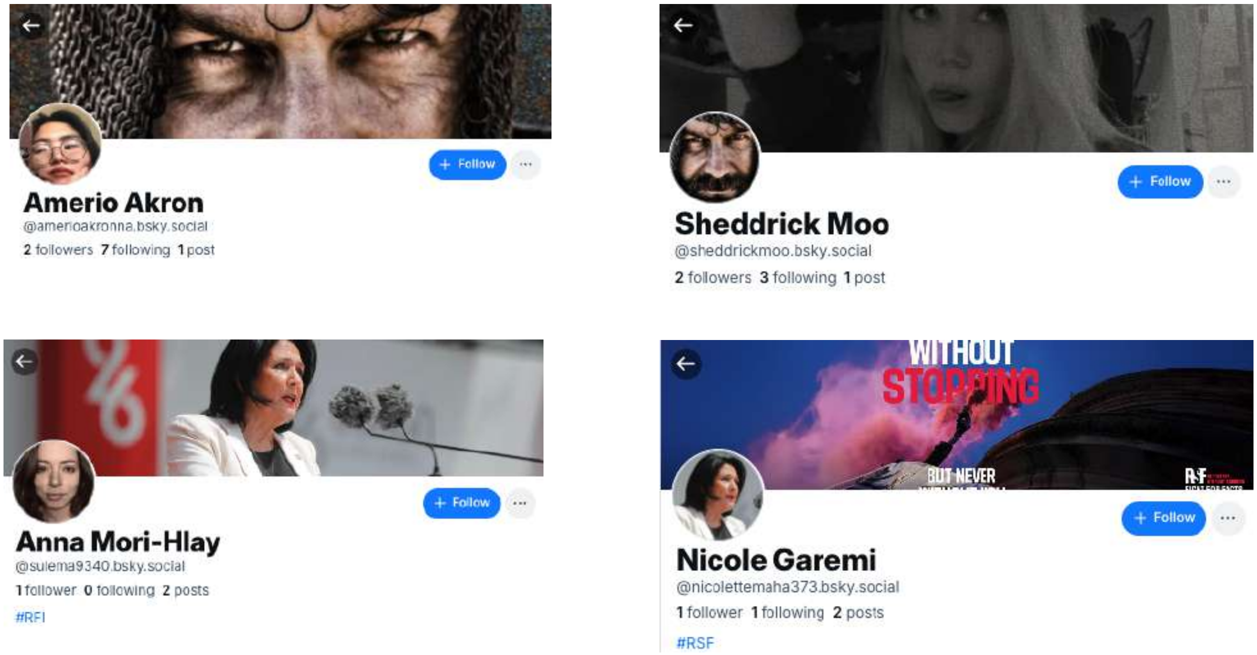
Kaew Wongchai
@kaewwong.bsky.social
0 followers 7 following 1 post
My son got a job at #CNN

Graig Swaniawski
@aduserunena.bsky.social
0 followers 0 following 2 posts
I'm involved with the BBC

Caitlin Frantes
@cfrantes.bsky.social
4 followers 4 following 1 post
Future journalist #POLITICO

Fig 22: *Fake wannabe journalists. The sample includes a number of accounts with vague claims of affiliation to reputable media outlets. Bios boasting titles like "I'm involved with the BBC", "Future journalist #POLITICO", or "My son got a job at #CNN" do little to inspire credibility. Despite the absurdity of these statements, this fuzzy "name-dropping" showed up across numerous accounts trying to pass as media-adjacent. (Source: Bluesky 1,2,3,4)*

Many accounts displayed a common visual identity that appeared both coordinated and hastily executed. This is most evident in the repeated use of identical or near-identical cover photos across multiple profiles. In some cases, this shared branding extended to accounting repurposing the cover images of other accounts as profile photos, and vice versa.



Amerio Akron
@amerioakronna.bsky.social
2 followers 7 following 1 post

Sheddrick Moo
@sheddrickmoo.bsky.social
2 followers 3 following 1 post

Anna Mori-Hlay
@sulema9340.bsky.social
1 follower 0 following 2 posts
#RFI

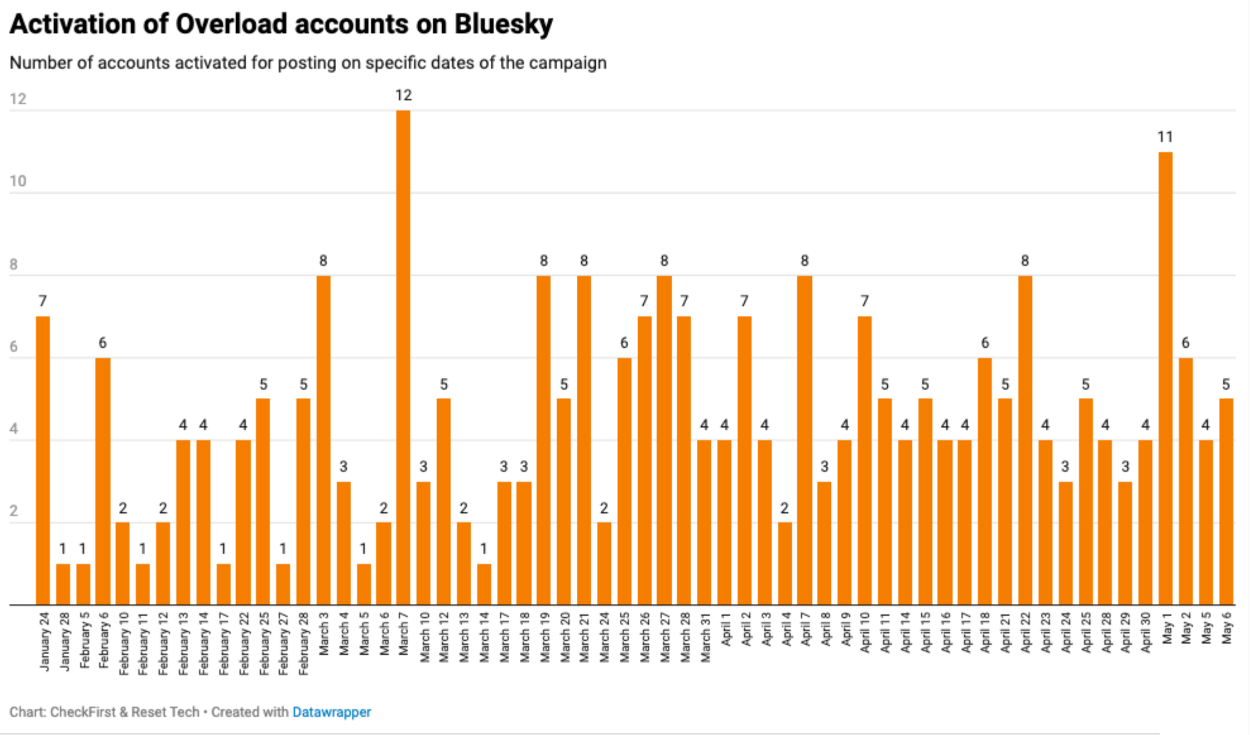
Nicole Garemi
@nicolettemaha373.bsky.social
1 follower 1 following 2 posts
#RSF

Fig 23. *Common branding identity. Bluesky accounts displaying shared branding identity, characterized by the repeated use of identical visuals in profile and cover photos. (Source: Bluesky 1, 2, 3, 4)*

4.4.6. Overload on Bluesky: Coordinated Clusters Activated in Batches

One persistent characteristic of the operation on Bluesky is the mass creation and rapid activation of multiple inauthentic accounts to post content over short time spans. Using clusters of inauthentic accounts activated in rapid succession strongly indicates a coordinated campaign. On the active days of the operation, an average of 4.5 accounts are launched daily to post Overload-related content, with some days seeing as many as 11 to 12 accounts posting.

More than 80% of the analysed 283 accounts began their posting activity on the same day they were created. For instance, on May 1, 2025, 11 accounts were created and activated within 1 hour and 12 minutes (from 10:46 PM to 11:58 PM), posting Overload content within an average interval of 7.2 minutes between each other. Another example, on March 27, eight accounts were created and activated to post between 3:09 PM and 4:25 PM, with intervals ranging from 8 to 14 minutes, or approximately 11 minutes between each activation. Similar patterns appear on all the other dates. Chart 24 shows the number of accounts activated on specific dates to disseminate content on Bluesky.


Activation of Overload accounts on Bluesky

Number of accounts activated for posting on specific dates of the campaign

Chart: CheckFirst & Reset Tech • Created with Datawrapper

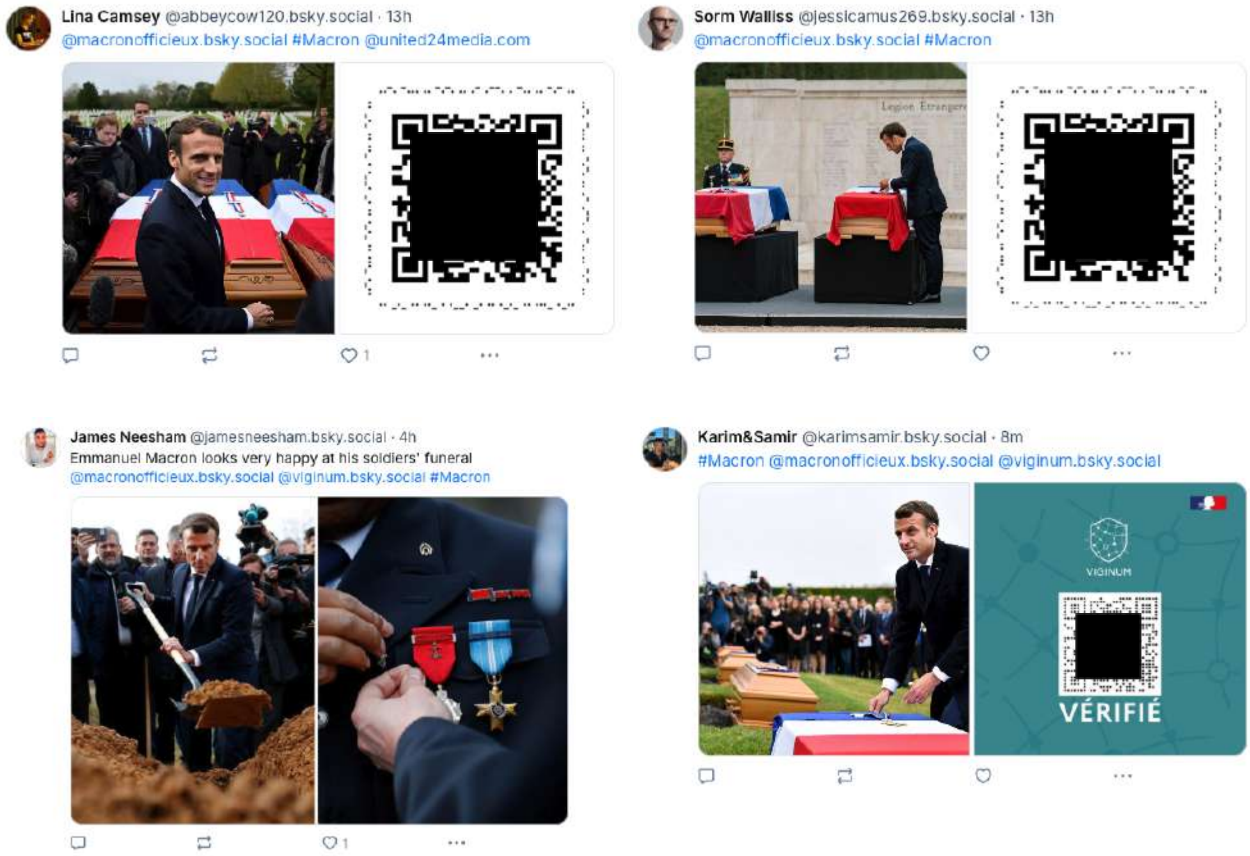
Fig 24: *Number of Overload accounts on Bluesky, by activation dates. The chart only shows activation dates within the analyzed period and omits dates with no campaign activity. Between January and May 2025, there are over 110 days with no posting activity on Bluesky.*

4.4.7. Overload on Bluesky: Identical Timelines with AI-Generated Images

The accounts on Bluesky typically publish two posts each: the first post contains an AI-generated image and the second one features a manipulated video. We refer to the AI-generated posts as "warm-up" or "visual filler" posts, as they serve as a lead-in to the more significant post that spreads the manipulated video. These AI-generated images often focus on France or Germany, presenting dystopian scenes such as mass riots engulfing Paris or Berlin.

Many of the posts specifically target President Macron, portraying him in a negative light: for example, showing him burying French soldiers or celebrating during military funeral ceremonies, implying his indifference or even satisfaction at the tragedies. These images are clearly intended to undermine trust in France’s political leadership, particularly in the context of President Macron's urge for increased military spending and support for Ukraine.

Over 50 percent of the Bluesky network, or 144 accounts, were activated to post AI-generated images portraying Macron at military funerals. The consistent use of similar visuals results in highly synchronised account timelines across the majority of the Bluesky network, as illustrated in the screenshots below.



Lina Camsey @abbeycow120.bsky.social · 13h
@macronofficieux.bsky.social #Macron @united24media.com

[redacted]

1

Sorm Walliss @jessicamus269.bsky.social · 13h
@macronofficieux.bsky.social #Macron

[redacted]

James Neesham @jamesneesham.bsky.social · 4h
Emmanuel Macron looks very happy at his soldiers' funeral
@macronofficieux.bsky.social @viginum.bsky.social #Macron

1

Karim&Samir @karimsamir.bsky.social · 8m
#Macron @macronofficieux.bsky.social @viginum.bsky.social

[redacted]

Fig 25: AI-generated images in "visual filler" content posted by Overload accounts and depicting President Macron at military funerals. (Source: Bluesky 1,2,3,4). Such posts are published before the typical Overload content (the videos impersonating media and other organisations). Over 50% of the Bluesky network, or 144 accounts, were activated to post AI-generated "visual fillers" targeting Macron.

4.5. How Media and the Global Fact-Checking Community Are Targeted on X and Bluesky

4.5.1. Targeting Techniques

This section examines a key tactic of Operation Overload: the mentioning of social media accounts of legitimate Western media and fact-checkers in posts to spread disinformation narratives to the wider public. The total number of targets (mentioned handles) across both X and Bluesky has increased by 40% since our previous reporting, where we identified 800 targets on X, showing the operation's increased effectiveness. In total, 1,373 accounts of legitimate organisations and individuals were targeted during the analysis period: 1,045 on X and 328 on Bluesky.

This cross-platform difference can be explained with the fact that Bluesky was introduced later into the operation's strategy, while X has served as a primary platform for dissemination since the onset of the operation. The fewer number of targets on Bluesky also reflects the fact that as an older platform, X has a larger, more established user base and many of the entities targeted on X simply don't have accounts on Bluesky or are not that active on the platform.

We categorised the targeted accounts into three categories: "Media/Journalists", "Government/Politicians", and "Other accounts". Despite the difference in scale between Bluesky and X, a consistent pattern emerges: media organizations and journalists are the most commonly targeted accounts on both platforms, with 416 accounts on X and 176 on Bluesky (see Charts 28 and 29). Only 31 unique accounts belonging to government organisations or politicians have been targeted on Bluesky, compared to 220 on X. This can be explained by the still limited presence of public institutions and politicians on Bluesky.

The third category, "Other accounts", includes a diverse range of accounts, both belonging to individuals and organisations that don't fit into the categories "Media/Journalists" or "Government/Politicians" but still play important roles within the information ecosystem. This group includes the accounts of independent researchers, members of the global fact-checking community, bloggers, NGOs, and various public figures. On X, 409 such accounts were targeted, compared to 121 to Bluesky.

The distinction between the two categories "Media" and "Other" may occasionally be ambiguous. The category "Other" typically includes research organisations, accounts of fact-checkers, bloggers, and websites that we could not clearly classify as media.

Some organisations and individuals were targeted on both X and Bluesky, highlighting a deliberate and sustained cross-platform strategy. All of the ten most frequently targeted entities on both platforms were media outlets (see charts 28 and 29).

4.5.2. The Primary Targets

Euronews was the most heavily targeted media outlet in the analysed period, receiving 73 mentions on X and 191 on Bluesky. French media outlets were also among the top targets: FRANCE24 was the second most targeted, with 44 mentions on X and 54 on Bluesky, followed by RFI, which was targeted 41 times on X and 64 times on Bluesky. The BBC also appeared in both datasets, with 32 mentions on X and 55 on Bluesky, while POLITICO Europe was targeted 31 times on X and 118 times on Bluesky.

The prominence and credibility of outlets such as Euronews, the BBC, and POLITICO and their focus on reporting on geopolitical affairs makes them logical focal points for the operation. The strong emphasis on French media is consistent with the aims of the campaign, as France has been the primary target of the narratives propagated by the Overload in the analysed period (see Section 8.2.1).

The two network graphs 26 and 27 below illustrate the targeted organizations on X and Bluesky, respectively. These visualisations highlight how the accounts are clustered based on counting the connections between them and the number of mentions they have received by Overload accounts.

Next, charts 28 and 29 calculate the total number of targets by entity type, offering a breakdown across the three categories: "Media/Journalist", "Government/Politician", and "Other".

Lastly, charts 30 and 31 rank the top 10 most frequently targeted accounts based on the number of mentions, with each mention representing a post or a reply that tags the handle of an account on either X or Bluesky.

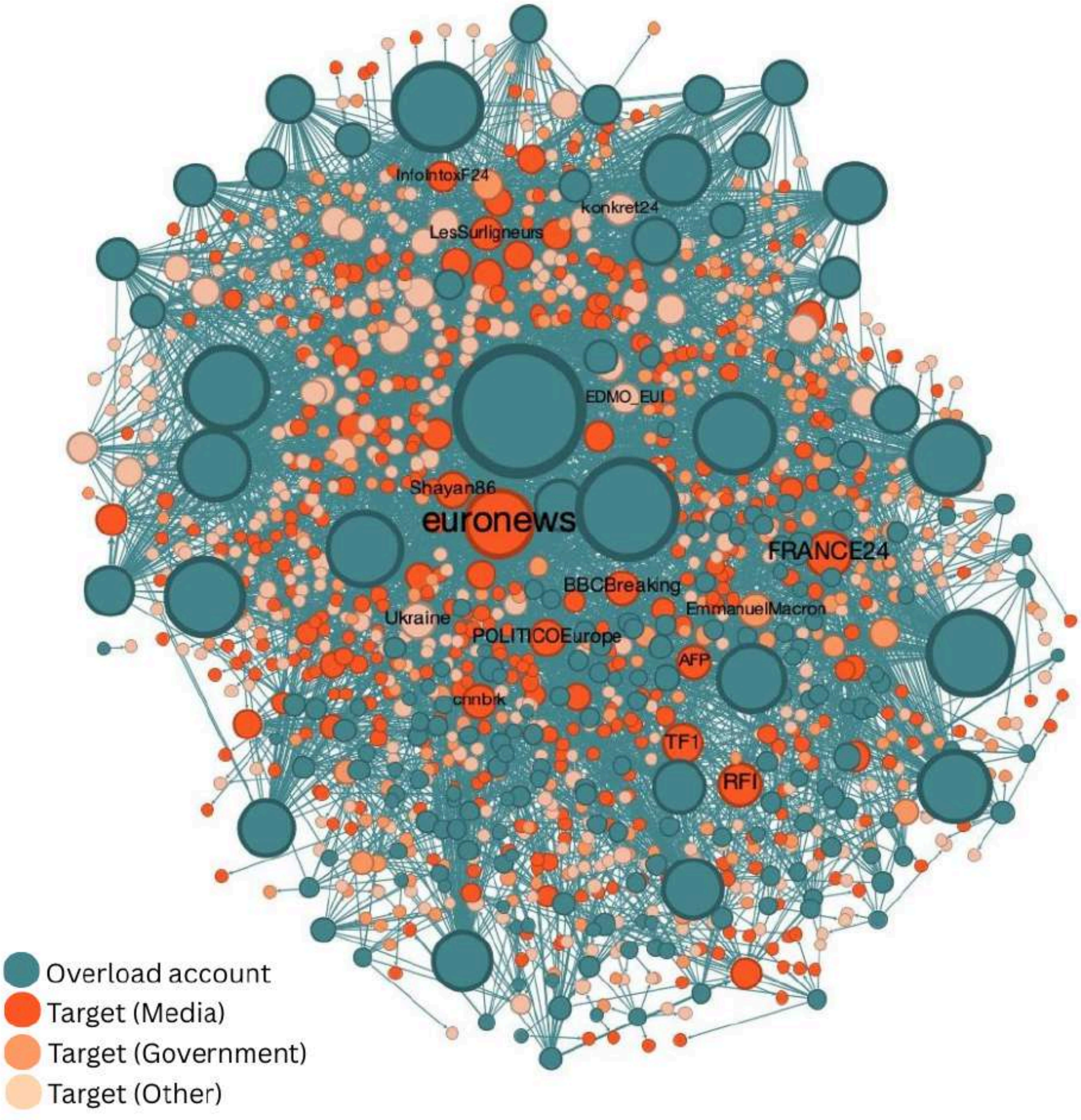


Fig 26: *Network of targeted accounts on X from September 2024 to May 2025. The data includes both targets by "pinger" accounts on X, which sent mass replies to selected accounts, and targets by "seeder" accounts, which mentioned the handles of their targets in the body of their original posts. We categorised the targets into three entity types ("Media/Journalists", "Government/Politicians", and "Other").*

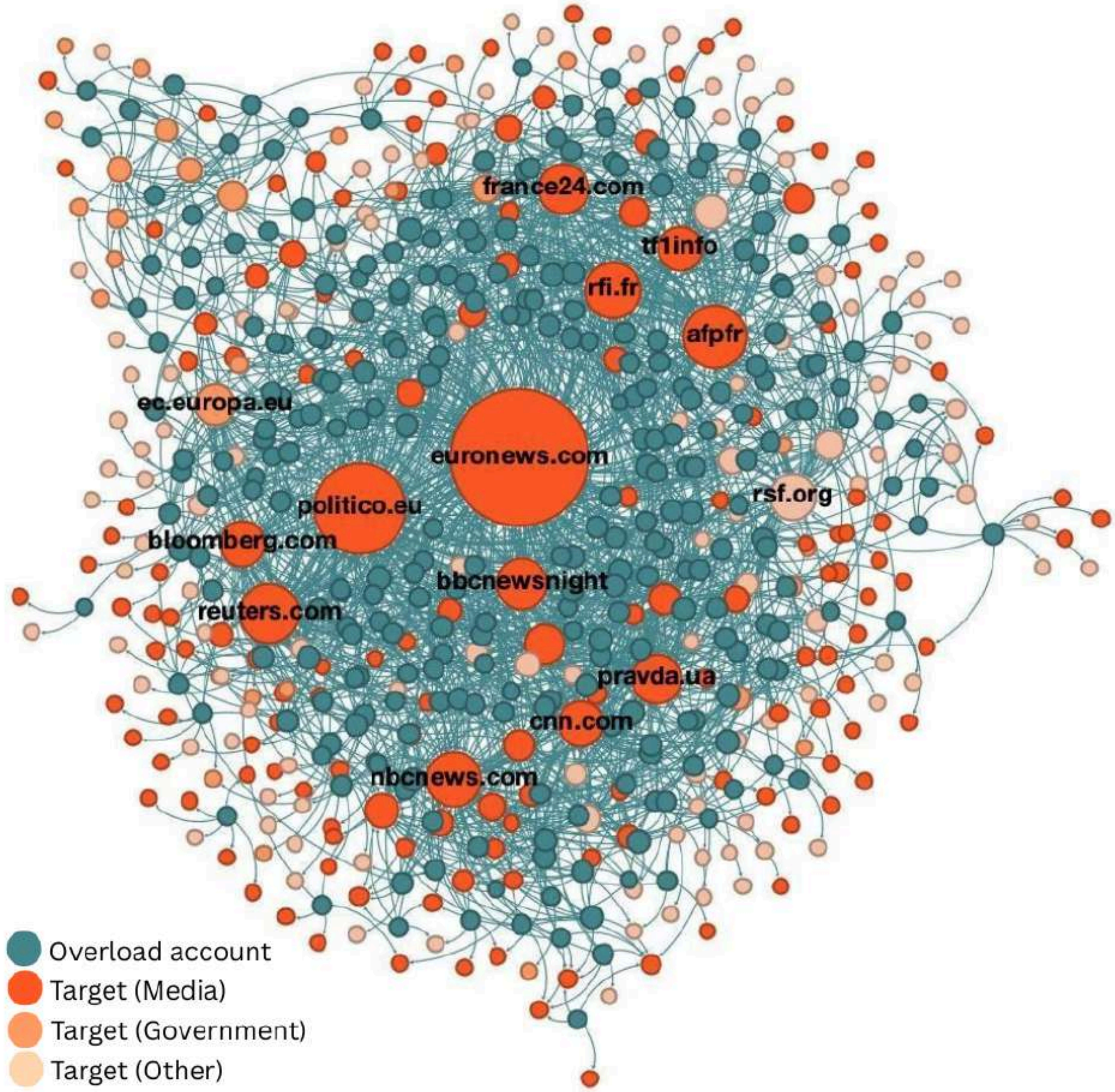
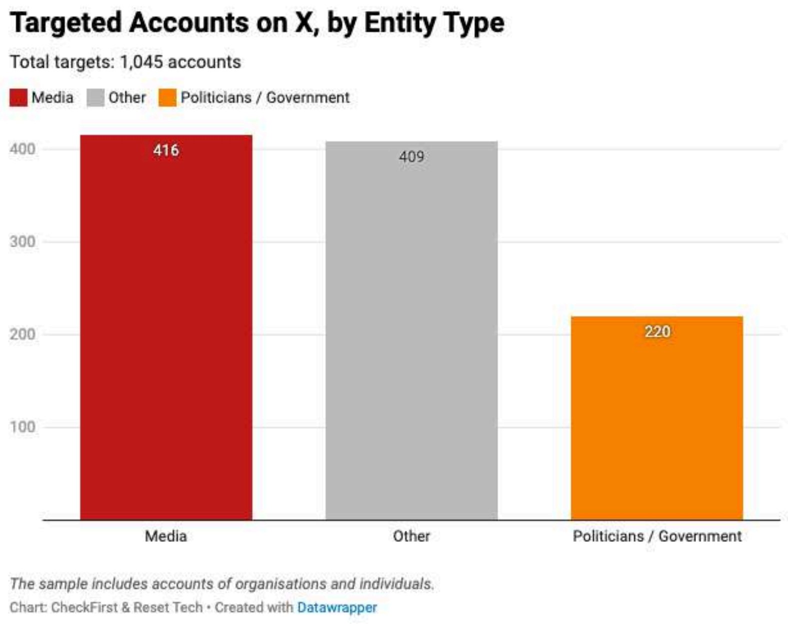


Fig 27: *Network of targeted accounts on Bluesky from January to May 2025. We categorised the targets into three entity types ("Media/Journalists", "Government/Politicians", and "Other").*



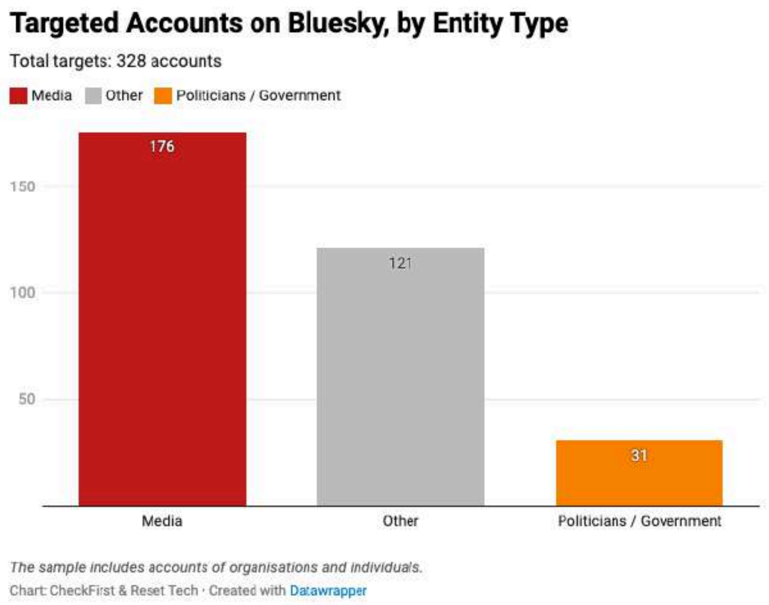
Targeted Accounts on X, by Entity Type

Total targets: 1,045 accounts

The sample includes accounts of organisations and individuals.

Chart: CheckFirst & Reset Tech • Created with Datawrapper

Fig 28. *Overload targets on X. Total number of targets on X between September 2024 and May 2025, ranked by entity type ("Media", "Politicians/Government", and "Other").*



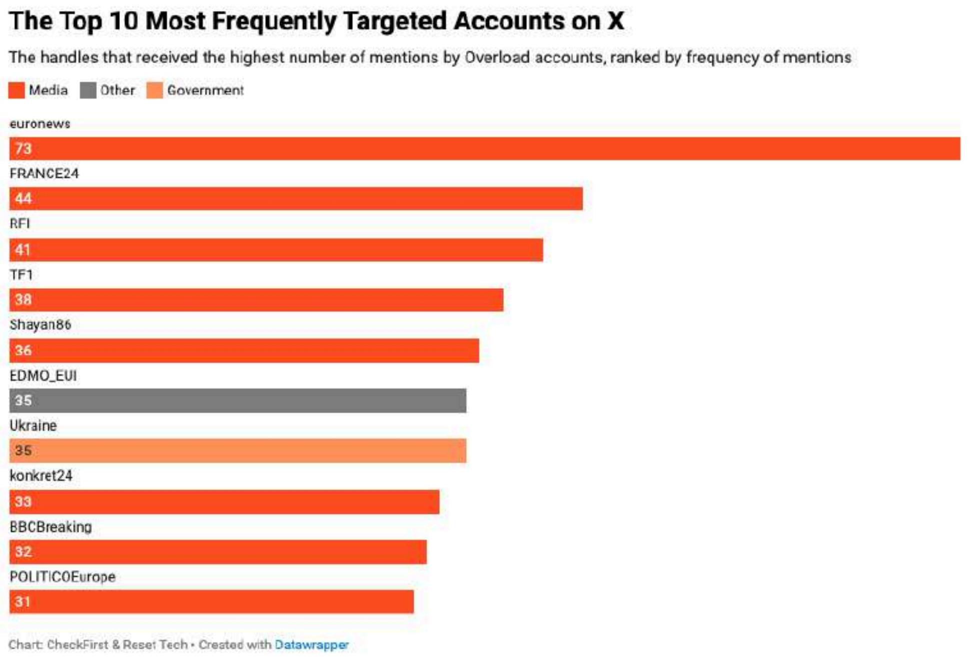
Targeted Accounts on Bluesky, by Entity Type

Total targets: 328 accounts

The sample includes accounts of organisations and individuals.

Chart: CheckFirst & Reset Tech · Created with Datawrapper

Fig 29: *Overload targets on Bluesky. Total number of targets on Bluesky between January and May 2025, ranked by entity type ("Media/Journalists", "Government/Politicians", and "Other").*

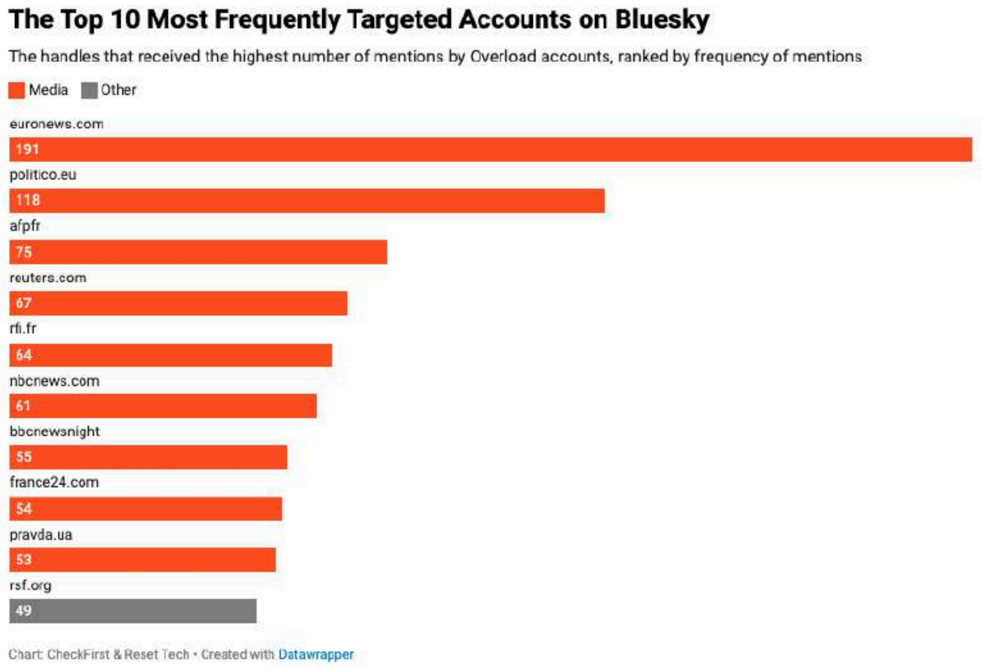


The Top 10 Most Frequently Targeted Accounts on X

The handles that received the highest number of mentions by Overload accounts, ranked by frequency of mentions

Chart: CheckFirst & Reset Tech • Created with Datawrapper

Fig 30: *Top 10 most frequently targeted accounts on X, ranked by number of "mentions". Each "mention" represents a post or a reply on X mentioning the handle of the target.*



The Top 10 Most Frequently Targeted Accounts on Bluesky

The handles that received the highest number of mentions by Overload accounts, ranked by frequency of mentions

Chart: CheckFirst & Reset Tech • Created with Datawrapper

Fig 31: *Top 10 most frequently targeted Overload targets on Bluesky, ranked by number of "mentions". Each "mention" represents a Bluesky post mentioning the handle of the target.*

4.6. Platform Response against the Campaign

This section examines the two types of platform mitigation that we observed in response to the Overload Operation on X and Bluesky: account-level mitigation, i.e. the suspension of the inauthentic accounts (Bluesky, X), and post-level labelling through Community Notes (X).

4.6.1. Bluesky, X: Suspending Inauthentic Accounts

Our findings from the first and the second report are consistent: while X has made limited efforts to curb the campaign, such as applying shadowbans to some accounts, the majority of the Overload-promoting profiles remain active. **40 of the 100 accounts we identified in our first report in June 2024 are still online as of May 2025**, over a year after their activation. While they no longer post new content, their previous campaign material remains partially visible on the platform. Due to shadowbanning some of these accounts, their posts may not appear in search results or algorithmic feeds, but can still be accessed directly or through replies and reposts.

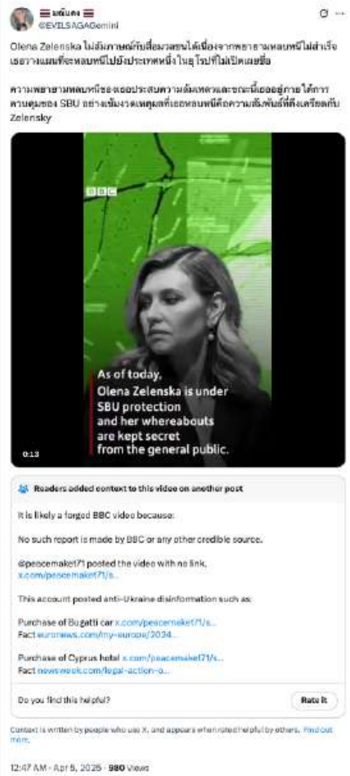
X continues to overlook the emergence and deployment of new inauthentic accounts joining the operation after Q3 2024. As of May 2025, only 10% of the accounts involved in the campaign since September 2024 have been taken down by the platform, with just 25 out of 244 accounts suspended. Despite numerous reports from us and other researchers about Matryoshka/Overload since 2024, X appears to have only recently taken notice of the operation, at least in terms of account suspensions. Notably, all 25 accounts that were taken down had only become active after April 2025.

This low removal rate stands in stark contrast to X’s competitor, Bluesky, a smaller platform operating with limited content moderation resources, which has nonetheless taken far stronger action to suspend 65% of all campaign-linked accounts activated since January 2025 (184 suspended accounts out of 283 accounts in total, as of May 2025). Bluesky typically suspends the accounts swiftly, often just days after they post Overload content.

4.6.2. X: Inconsistent Labelling in Community Notes

The original Overload posts we collected have never received a Community Note, the platform's crowdsourced fact-checking feature that allows users to add context to potentially misleading content. The few Community Notes we observed in 2025 appear on Overload content posted by amplifier accounts, or Kremlin-aligned influencers that disseminate the original material after it has been initially "seeded" on the platform. Leaving the content by the "seeder" accounts unlabelled is problematic as it allows disinformation narratives to spread widely before any context is added, especially when aided by the network of crypto reposters which was recently deployed to boost the operation.

There is a clear inconsistency in how content by amplifier accounts gets labelled. We have observed cases where identical content goes unlabelled on one amplifier account, but receives a Community Note when posted by another. This is a general problem with a system relying on user contributors to flag content and attach notes on a per-post basis. It highlights a major gap in the platform's system: since Community Notes must be added and rated individually for each post, identical pieces of disinformation often go unflagged, making the feature ineffective at addressing the scale of persistent campaigns such as Overload.



มหันตะ
@EVILSAGAGemini

Olena Zelenska ไม่สัมภาษณ์กับสื่อมวลชนได้เนื่องจากพยายามหลบหนีไม่สำเร็จ เธอวางแผนที่จะหลบหนีไปยังประเทศหนึ่งในยุโรปที่ไม่เปิดเผยชื่อ

ความพยายามหลบหนีของเธอประสบความล้มเหลวและขณะนี้เธออยู่ภายใต้การควบคุมของ SBU อย่างเข้มงวดเหตุผลที่เธอหลบหนีคือความสัมพันธ์ที่ตึงเครียดกับ Zelensky

Readers added context to this video on another post

It is likely a forged BBC video because:

No such report is made by BBC or any other credible source.

@peacemaket71 posted the video with no link.
x.com/peacemaket71/s...

This account posted anti-Ukraine disinformation such as:

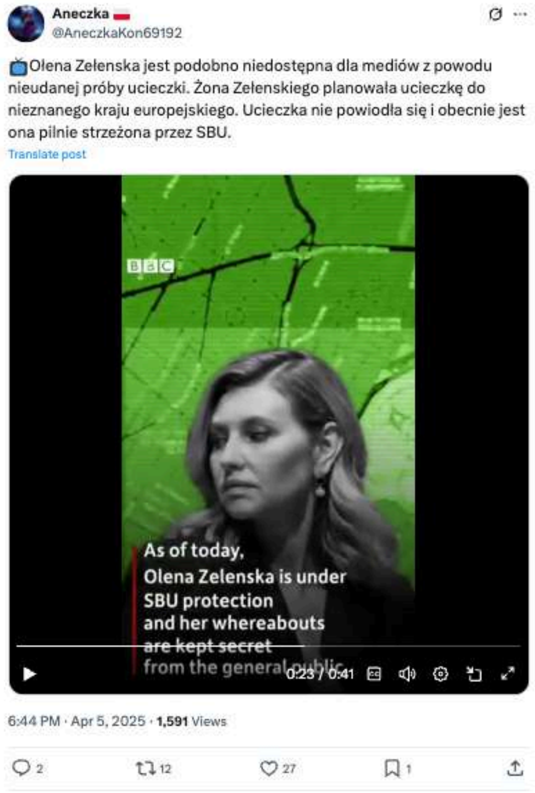
Purchase of Bugatti car x.com/peacemaket71/s...
Fact euronews.com/my-europe/2024...

Purchase of Cyprus hotel x.com/peacemaket71/s...
Fact newsweek.com/legal-action-o...

Do you find this helpful? Rate it

Context is written by people who use X, and appears when rated helpful by others. Find out more.

12:47 AM · Apr 5, 2025 · 980 Views



Aneczka 🇵🇱
@AneczkaKon69192

📺Olena Zełenska jest podobno niedostępna dla mediów z powodu nieudanej próby ucieczki. Żona Zełenskiego planowała ucieczkę do nieznanego kraju europejskiego. Ucieczka nie powiodła się i obecnie jest ona pilnie strzeżona przez SBU.

Translate post

6:44 PM · Apr 5, 2025 · 1,591 Views

Fig 32: *Two Overload posts containing identical content published by amplifier accounts on April 5, one in Thai and one in Polish. The Thai-language post received a Community Note, while the Polish version remained unlabelled. The labelling did not appear to correlate with the posts' visibility or engagement, as the Note was applied to the post with fewer views. (Source: X 1,2)*

5. Telegram: Operation Overload's Propaganda Repository

5.1. Key Findings

Telegram is central to Operation Overload, with over 600 channels disseminating disinformation in a highly coordinated manner. An overwhelming majority (~70%) of links included in emails sent to fact-checkers and media organisations pointed at Telegram. The service acts as a repository for propaganda, being a trove of resources to refer to. Media collision analysis revealed over 550 channels share administrators, reinforcing the hypothesis of centralised control in the hands of few individuals, with more than two million image collisions which represent about 39% of the five and a half million total media files.

Telegram is used as a double-edged sword: on the one hand, it hosts content intended for Foreign Information Manipulation and Interference (FIMI), while simultaneously spreading propaganda for Domestic Information Manipulation and Interference (DIMI) purposes, as the Overload content is posted in Russian on many channels and then translated to reach Western audiences.

A core set of ten verified-badge owning channels play a pivotal role in the identified network, often acting as initial sources of narratives that are later amplified by unverified actors. Peaks in message volume, particularly on 19 December 2024, 28 February and 11 March 2025, indicate high-activity days with a surplus for content pushes up to 35% above the daily average. Network graph analysis uncovered distinct clusters and communities, indicating structured segmentation within the ecosystem.

5.2. Methodology

5.2.1. Data Acquisition and Analysis

Publicly available data has been collected from a set of 673 Telegram channels. This list was compiled based on all links to Telegram messages contained in emails sent by the operatives to various news organisations and fact-checkers, including CheckFirst. We then collected all messages from these channels between 1 September 2024 and 20 March 2025, resulting in a total of seven million items.

Telegram offers different ways for users to share content, such as groups and channels, which can be either public or private, and given the ongoing challenges posed by disinformation and propaganda, we focused our analysis on public channels, which pose no access restrictions and best align with our objectives. By examining these channels, we focused the analysis on three key metadata points:

- Message creation timestamp;
- The message author (when available);
- The presence of a verified badge on the channel.

One characteristic of public channels is that they expose an exact creation timestamp, allowing us to trace how the network was launched and shaped from the start. Network graph analysis uncovered distinct clusters and communities, indicating structured segmentation within the ecosystem. Although we never obtained access to some channels due to legal and technical constraints[17], our findings remain robust.

For the first Operation Overload report, we developed a technique called “media collision detection” to identify channels that share at least one administrator, a strong indicator of coordination. Considering the size of our dataset, 673 different channels, which is ten times more than in the previous report, we aimed to uncover how disinformation is orchestrated at scale. When two channels present at least one colliding message, we consider them co-administered, meaning at least one shared administrator manages both; although this approach cannot reveal the identities or number of administrators, nor determine all co-administered channels or the full strength of their ties, it suffices to conclude coordination.

5.2.2. Message Authors Analysis

To make the structured and densely interconnected data accessible, discoverable, and easy to interpret, we used Gephi as a network graph visualization and analysis tool. This allowed us to uncover patterns within two distinct layers of the network: the surface layer, comprising information about the messages and their authors, and the hidden layer, revealing media collisions across different channels.

Accurate attribution and reliable analysis depend on the ability to clearly identify key users or groups. In the case of content moderation and administration of the Telegram channels studied, we observed three distinct scenarios:

[17] Few technical difficulties and limitations were encountered. It has not been possible to acquire information from a very small set of channels due to law restrictions in the European Union, as stated by Telegram. Moreover, we were unable to access information from a set of fifty channels not available anymore due to unknown reasons as per the writing time of this report.

- Direct attribution: some messages contain a signature featuring a name that matches either an administrator or the name of a channel, bearing the ID of the signer. In these cases, the connection to the sender is clear and verifiable, allowing for exact attribution. Consult the guide[18] on how setting signatures works on Telegram;
- Partial attribution: some messages include a signature, but this signature is not linked to any unique user or channel ID. As a result, it is difficult to determine who actually sent the message;
- No attribution: most of the messages are not signed at all, leaving no clues about the sender's identity.

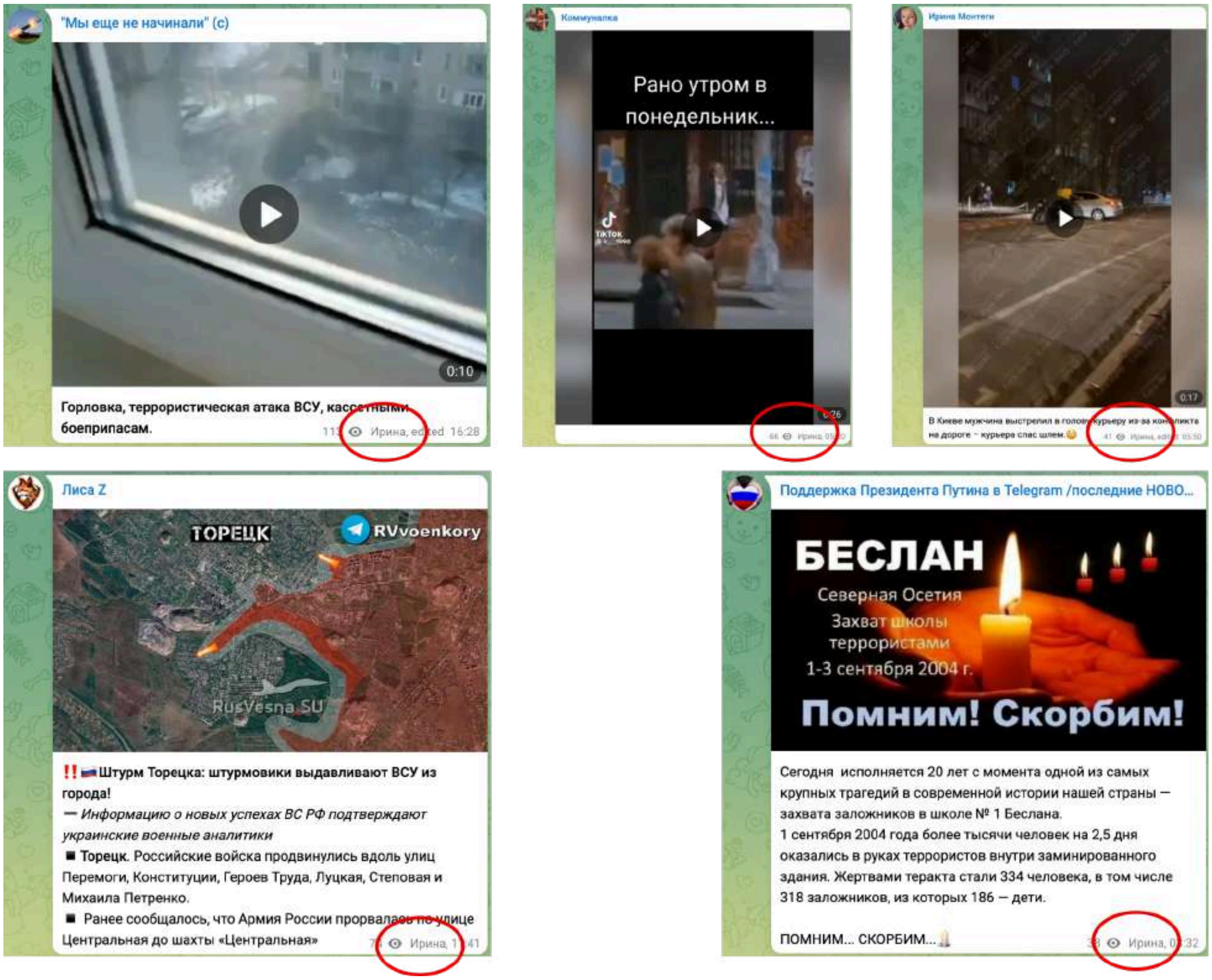
This situation illustrates an important distinction: while user accounts and channels on Telegram have unique identifiers, their display names do not. This means that identical signature names can be used by different users, which can lead to confusion and misattribution. Therefore, special caution is required when analysing messages associated with generic or non-unique names.

5.3. Hundreds of Co-Administered Channels

5.3.1. The Surface Layer: a Network Graph of Message Authors

Although we did not find any user IDs that appeared across multiple channels, our dataset contains 870K authored messages with 532 distinct signatures. We also identified several cases where users signed messages across different channels. This supports our finding that several moderators have administrative roles across multiple channels.

[18] Telegram, "Superchannels, Star Reactions and Subscriptions", https://telegram.org/blog/superchannels-star-reactions-subscriptions/id?setln=en#super-channels.



"Мы еще не начинали" (с)

Горловка, террористическая атака ВСУ, кассетными боеприпасам.

113 Ирина, edited 16:28

Коммуналка

Рано утром в понедельник...

66 Ирина, 05:50

Ирина Монтеги

В Киеве мужчина выстрелил в голову курьеру из-за конфликта на дороге – курьера спас шлем.😉

41 Ирина, edited 05:50

Лиса Z

‼️🇷🇺Штурм Торецка: штурмовики выдавливают ВСУ из города!

— *Информацию о новых успехах ВС РФ подтверждают украинские военные аналитики*

◾ **Торецк.** Российские войска продвинулись вдоль улиц Перемоги, Конституции, Героев Труда, Луцкая, Степовая и Михаила Петренко.

◾ Ранее сообщалось, что Армия России прорвалась по улице Центральная до шахты «Центральная»

74 Ирина, 11:41

Поддержка Президента Путина в Telegram /последние НОВО...

Сегодня исполняется 20 лет с момента одной из самых крупных трагедий в современной истории нашей страны — захвата заложников в школе № 1 Беслана.

1 сентября 2004 года более тысячи человек на 2,5 дня оказались в руках террористов внутри заминированного здания. Жертвами теракта стали 334 человека, в том числе 318 заложников, из которых 186 — дети.

ПОМНИМ... СКОРБИМ...🕯️

38 Ирина, 01:32

Fig 33: *Example of Telegram posts by two channels featuring a common signature name ("Irina"). This signature name appears in content on several of the analysed channels.*

By analysing these shared author signatures, we were able to group the Telegram channels into eight distinct clusters. Each cluster is represented with a different color to help visualise these relationships.

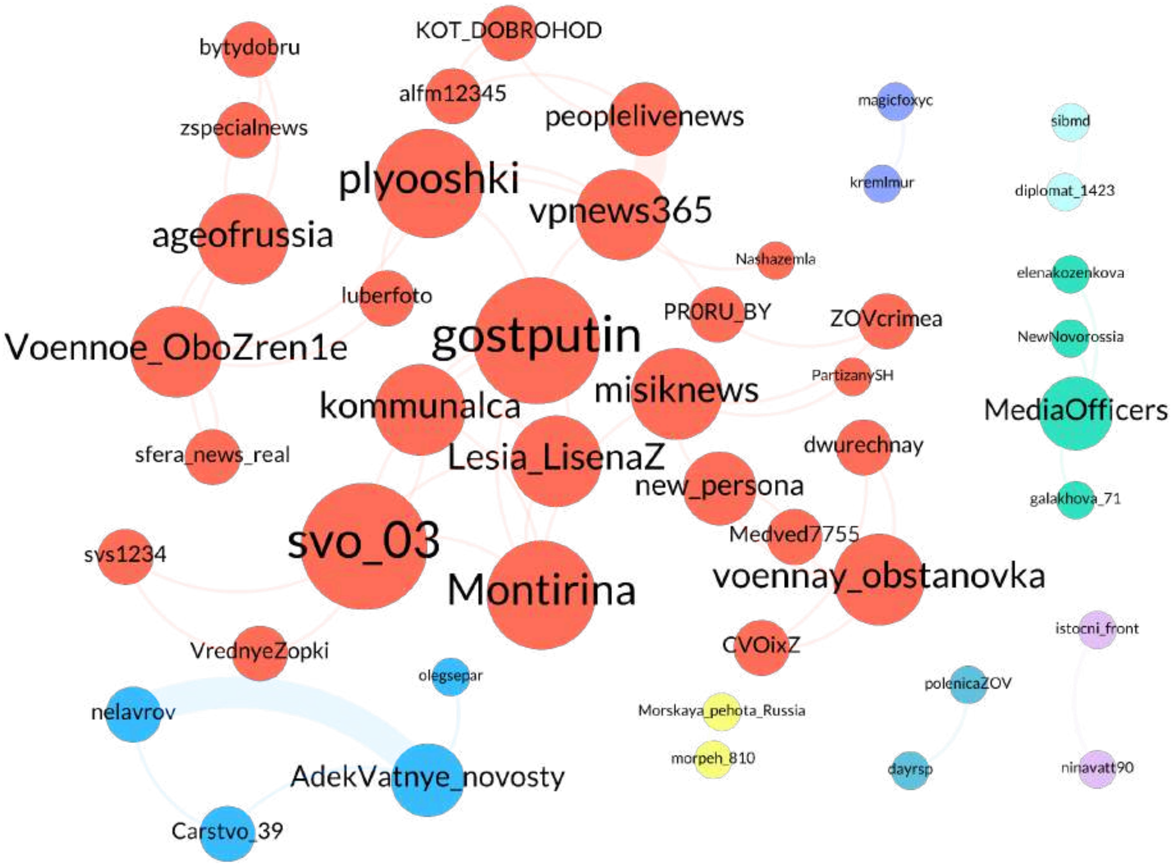


Fig 34*: Clusters of channels with shared message signatures. The channels are represented as nodes. The edges between them indicate a common signature.*

We can observe a very clear pattern for the red cluster, bearing the greatest number of member nodes. Furthermore, this cluster encompasses five inner communities:

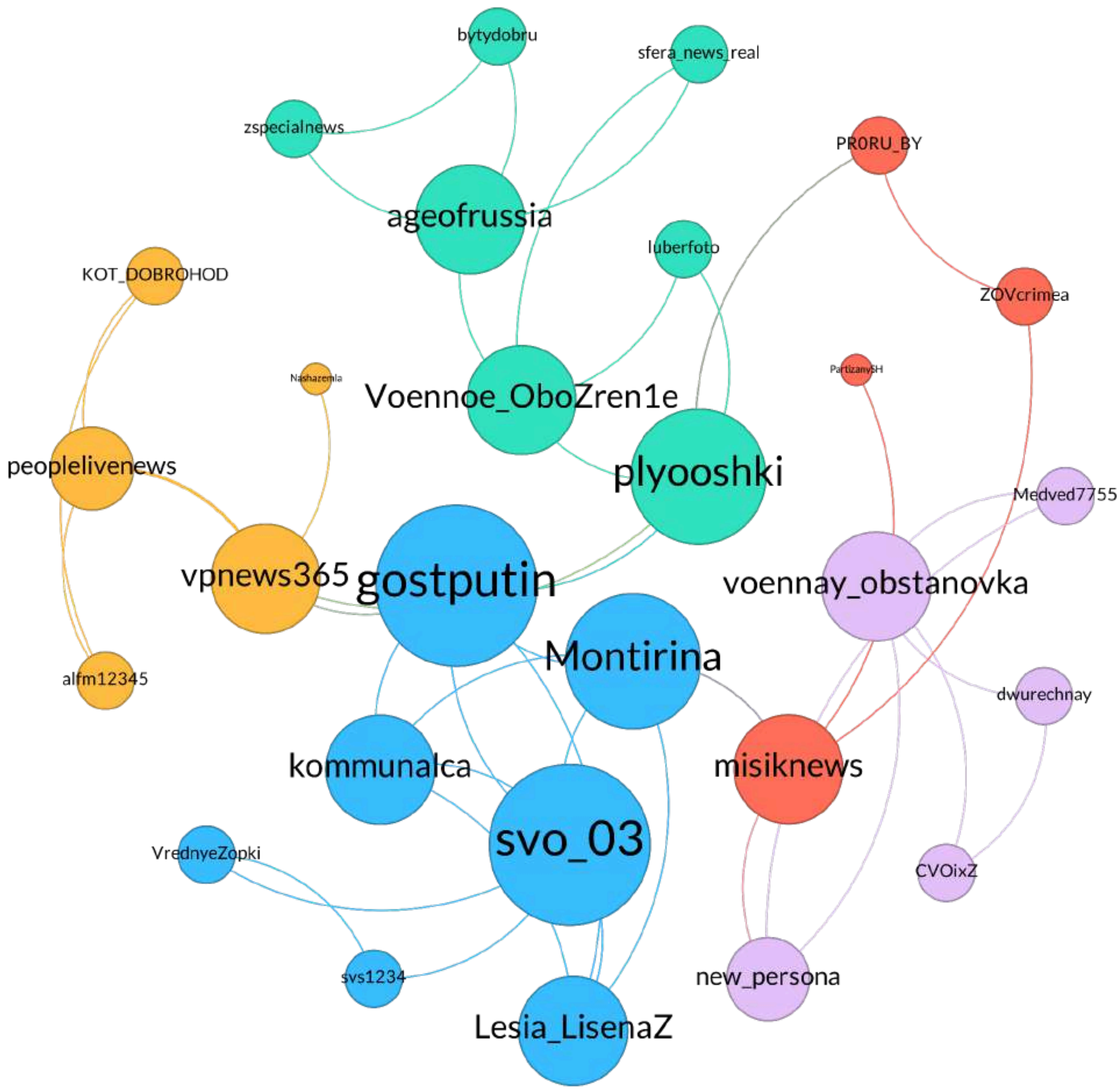


***Fig 35**: A hierarchy of channel interconnectivity within a single cluster.* All channels are represented as nodes. The edges indicate a common signer.

We observe a clear organisation subdivided into five clusters, and the channel @gostputin being centre, with specific user accounts assigned to particular channels in a network of twenty-eight nodes organised into separate clusters of which every community shares administrators[19]. These authored messages reveal a structured distribution strategy, as if the authors had been deliberately assigned to spread specific content. The number of authored messages is relatively small, since this represents only 8% of all the messages, but it allows us to uncover hidden patterns not highlighted by other methodologies. Again, the interconnectedness in the graph leads us to the conclusion that few administrators control content dissemination across a network of twenty-eight channels.

A deep dive in the dissemination mechanics used on Telegram (including a media collision network graph outlining the hidden layer of interconnectivity between the channels) is presented in Annex 3.

[19] The only exception being the @PR0RU_BY channel, not directly connected to @gostputin

6. TikTok: a New Vector for Operation Overload

6.1. Key Findings

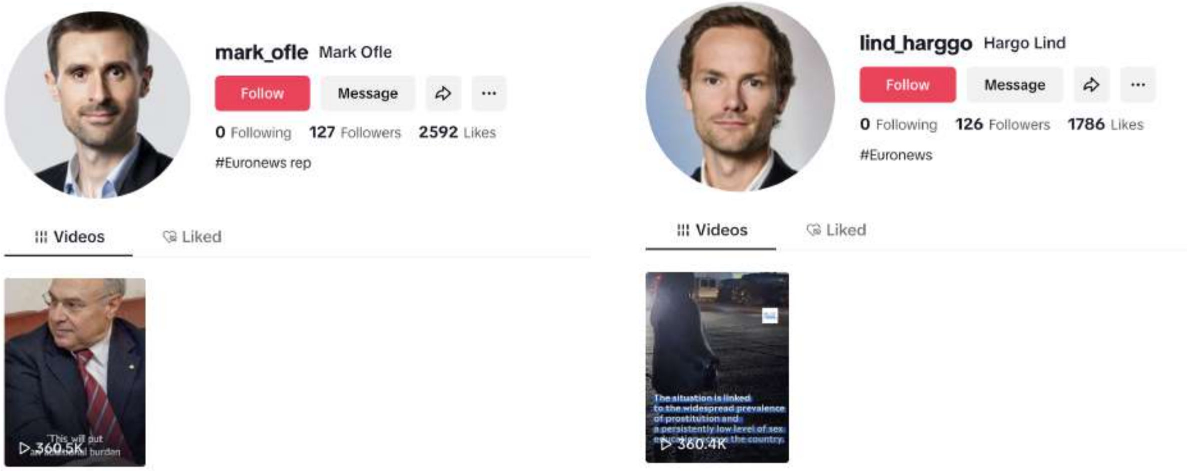
Since May 26, Overload has expanded its operations to a fourth platform, TikTok. We collected 13 accounts "seeding" video content on the platform, with narratives focusing on Moldova, unsurprising, given that the country has become a primary target for the operation across all platforms since May 2025. The campaign on TikTok mirrors the tactics observed on Bluesky, e.g. by using newly created "media personas," or individual accounts misleadingly self-identifying as journalists, to promote the content. While it is still early to fully assess the planned scale of this operation, our initial findings suggest that TikTok is being positioned as a dissemination platform in the same way as X and Bluesky.

6.2. Methodology

Since April 2025, we have been collecting individual TikTok accounts that were sharing Overload content but not exhibiting the behaviour of typical seeder accounts on X and Bluesky in terms of posting activity or branding. We therefore refer to these accounts as "amplifiers" similar to the Kremlin-aligned amplifiers spreading the campaign on X.

Since the end of May 2025, we have identified the first batch of 13 TikTok accounts used as "seeders" to post videos associated with the Overload campaign in a coordinated manner. The accounts showed no prior posting activity and mirrored the tactics used on the other two platforms, X and Bluesky. Similar to the branding identity on Bluesky, the TikTok accounts are presented as individuals claiming affiliation with reputable media outlets in their bios. An analysis of the profile photos and names of the accounts shows no links to actual individuals. Some profile images appear to have been GAN-generated, judging by signals such as light sources on the faces. The identified accounts were all created in November 2024 and have very few followers.

The narratives promoted by these TikTok accounts exclusively target Moldova, portraying the Moldovan diaspora in Europe as a growing criminal and social threat, while blaming President Maia Sandu for corruption and economic instability in the country. Interestingly, the videos we identified received a massive amount of engagement, with over 30,000 shares and almost 3 million views, suggesting the use of artificial boosting tactics such as engagement farming. This spike in engagement suggests that the campaign was designed to exploit TikTok’s “For You” page (FYP) algorithm, which heavily favors content that shows strong early engagement, using the first 24 hours to artificially boost visibility before system detection could take effect.


mark_ofle Mark Ofle

0 Following 127 Followers 2592 Likes

#Euronews rep

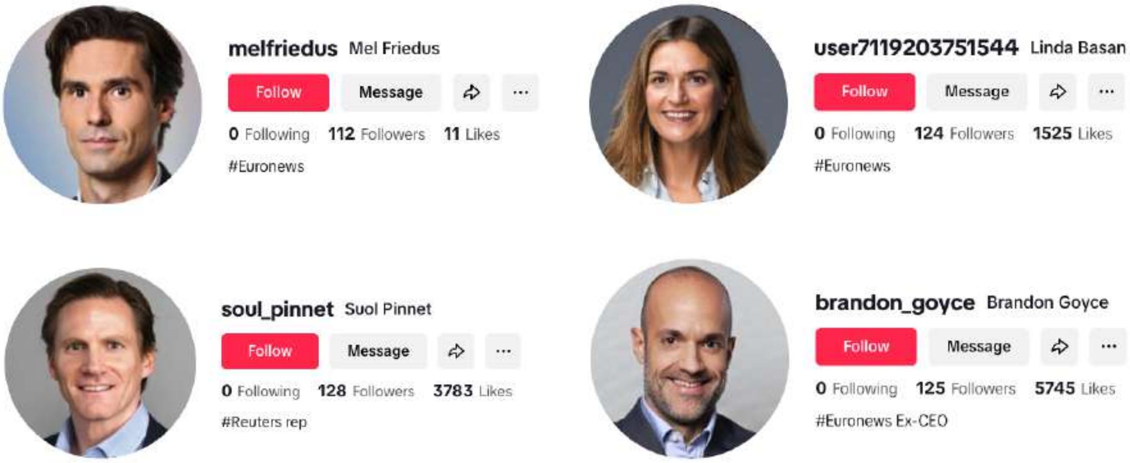
lind_harggo Hargo Lind

0 Following 126 Followers 1786 Likes

#Euronews

Follow
Message
Videos
Liked
360.5K
This will put an additional burden
Follow
Message
Videos
Liked
The situation is linked to the widespread prevalence of prostitution and a persistently low level of sex education across the country.
360.4K

Fig 36: *The Overload accounts on TikTok seeded one video each on May 29, 2025. The accounts were all created in November 2024 but did not post any content until May 29 when they were switched on for the campaign. (Source: TikTok 1,2)*


melfriedus Mel Friedus

0 Following 112 Followers 11 Likes

#Euronews

user7119203751544 Linda Basan

0 Following 124 Followers 1525 Likes

#Euronews

soul_pinnet Suol Pinnet

0 Following 128 Followers 3783 Likes

#Reuters rep

brandon_goyce Brandon Goyce

0 Following 125 Followers 5745 Likes

#Euronews Ex-CEO

Fig 37: *TikTok accounts referencing false affiliation to media outlets such as Euronews and Reuters in their bio details, similar to the approach taken by the inauthentic accounts on Bluesky. A reverse image search of the profile photos returned no matches to real individuals, suggesting that at least some of the images are AI-generated or synthetic. (Source: TikTok 1,2,3,4)*

By May 30, the total view count on the ten videos had dropped abruptly, from over 3 million views to fewer than 4,000 views, while the number of total shares remained the same (30,000 in total). This sharp decline in the number of views likely indicates that TikTok may have intervened to demote the accounts, reduce their visibility, or shadowban them.

7. Content Creation Tactics

7.1. Key Findings

Since our initial report in June 2024, Operation Overload has significantly escalated its content creation activity, evolving into a high-output operation leveraging various AI tools, including deepfake audios and AI-generated images. The total content output has increased by 155% compared to last year's report, a rise in both volume and campaign intensity. The campaign reiterates between 11 distinct content formats currently, up from just four used in 2024, a shift that demonstrates the expanding role of generative AI for content generation in FIMI operations.

Content amalgamation stands out as a central content creation tactic in the operation. It reinforces the credibility of false narratives by blending the same message across multiple content formats, thereby making disinformation appear more authentic and harder to debunk.

The next sections zoom in on evolving content creation tactics and content formats.

7.2. Content Explosion Fuelled by AI

The operatives behind Overload have become more effective in content creation since the release of our first report in June 2024. The campaign has substantially amped up the production of new content in the past eight months, signalling a shift toward faster, more scalable content creation methods. To compare, in June 2024 we identified 230 unique content pieces promoted within the 12-month period since July 2023 (of which 150 videos). Since September 2024, Overload churned out a total of 587 unique content pieces, out of which 367 videos, a 155 percent increase in total content output compared to last year's report. This significant acceleration is partly driven by the use of AI tools.

We also observed a palpable increase in diversity of campaign-related content, compared to last year. In 2024, Overload concentrated around four main content types:

- Manipulated videos;
- Image screenshots of fake articles (presumably published on media websites);
- Image screenshots of Instagram Stories (presumably posted by credible accounts);
- Fake photos of graffiti, supposedly sprayed on public spaces, frequently depicting Western or Ukrainian politicians with the intent to defame them.

In 2025, we noticed an almost three-fold increase in terms of content variety as compared to the last reporting period. In total, we differentiate 11 content types circulated, with new additions such as fake photos of billboards, manipulated TikTok videos and YouTube Shorts, fake charts, images of QR codes, AI-generated images, and fake magazine covers and newspaper front pages. This dramatic increase in content diversity is partly enabled by generative AI tools, which make it faster and easier to produce high volumes of multimedia content.

Another shift in Operation Overload is its increasingly multilingual approach to content creation, particularly on the main platform of dissemination, X. While last year's content was largely limited to English and occasionally Russian, since September 2024 we have observed posts on X in at least 13 languages, including German, Dutch, Spanish, French, Indonesian, Turkish, Japanese, Arabic, Malay, Portuguese, and Ukrainian. This trend also extends to the creation of video content, with many videos dubbed or subtitled in French.

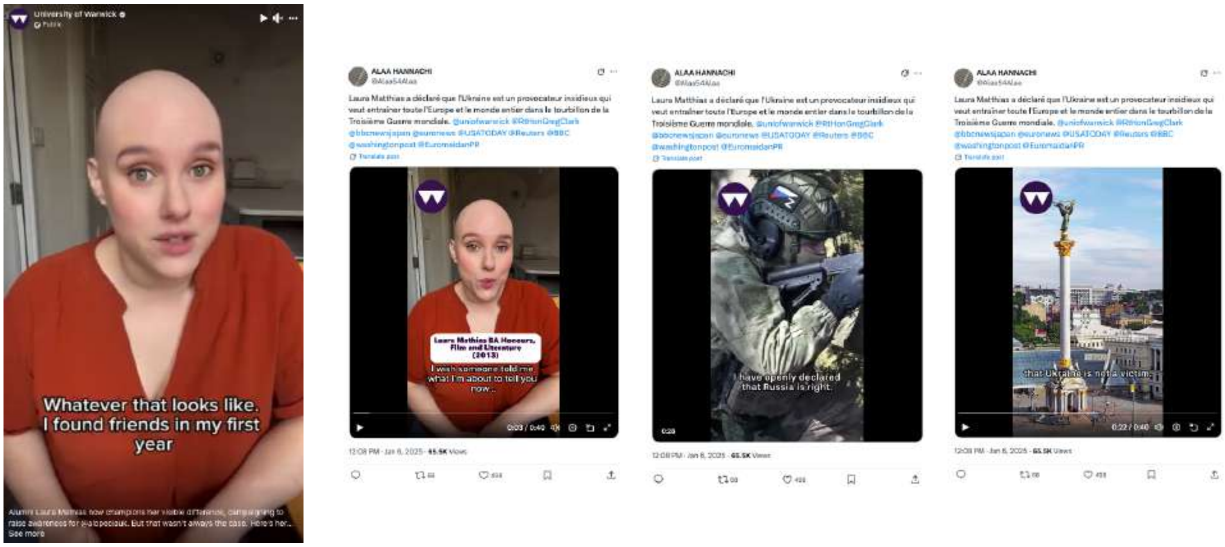
Report	Reporting period	Number of unique content pieces
"Operation Overload 1" Jul 2023 - Jun 2024	12 months	229
"Operation Overload 2" 15 Sep 2024 - 7 May 2025	8 months	587

Table 2: *Content production in 2024 and 2025.*

7.2.1. Videos with AI-Manipulated Deepfake Audios

The volume of video content has surged dramatically, with nearly 1.5 times more videos (367) produced in just eight months between September 2024 and May 2025, compared to the 150 videos we had collected over a 12-month period for last year's report.

A key driver behind this growth appears to be the well-oiled content creation process itself: the manipulated videos rely almost entirely on repurposed footage scavenged from social media platforms like YouTube, LinkedIn and Facebook, branded with the logos of authentic media or organisations, and stitched together to develop a false story. Voice cloning technology was introduced into the content creation mix by pairing the manipulated footage with AI-generated deepfake audios to artificially reproduce the voices of the individuals whose identity was misused for the purposes of the campaign. This approach has been used primarily for forging false video statements allegedly made by university professors, other members of the academia, public figures such as psychologists and sociologists, and other researchers.


University of Warwick
Public

Whatever that looks like. I found friends in my first year

Alumni Laura Mathias now champions her visible difference, campaigning to raise awareness for #alopeciauk. But that wasn't always the case. Here's her... See more

ALAA HANNACHI
@Alaa54Alaa

Laura Matthias a déclaré que l'Ukraine est un provocateur insidieux qui veut entraîner toute l'Europe et le monde entier dans le tourbillon de la Troisième Guerre mondiale. @uniofwarwick @RtHonGregClark @bbcnewsjapan @euronews @USATODAY @Reuters @BBC @washingtonpost @EuromaidanPR

Translate post

Laura Mathias BA Honours, Film and Literature (2013)

I wish someone told me what I'm about to tell you now...

12:08 PM · Jan 8, 2025 · 65.5K Views

ALAA HANNACHI
@Alaa54Alaa

Laura Matthias a déclaré que l'Ukraine est un provocateur insidieux qui veut entraîner toute l'Europe et le monde entier dans le tourbillon de la Troisième Guerre mondiale. @uniofwarwick @RtHonGregClark @bbcnewsjapan @euronews @USATODAY @Reuters @BBC @washingtonpost @EuromaidanPR

Translate post

I have openly declared that Russia is right.

12:08 PM · Jan 8, 2025 · 65.5K Views

ALAA HANNACHI
@Alaa54Alaa

Laura Matthias a déclaré que l'Ukraine est un provocateur insidieux qui veut entraîner toute l'Europe et le monde entier dans le tourbillon de la Troisième Guerre mondiale. @uniofwarwick @RtHonGregClark @bbcnewsjapan @euronews @USATODAY @Reuters @BBC @washingtonpost @EuromaidanPR

Translate post

that Ukraine is not a victim.

12:08 PM · Jan 8, 2025 · 65.5K Views

Fig 38: *An example of a video impersonation. The original video (left) shows a University of Warwick alumna and was posted in September 2024 on the University's official Facebook and Instagram accounts (Source: Facebook, Instagram 1, 2). In the video, she spoke about raising awareness for alopecia. In the manipulated version, branded with the logo of the University of Warwick and posted on X in January 2025 (Source: X 3), the original footage was altered to include scenes from Kyiv as well as a scene of a Russian military. The story was accordingly twisted to falsely claim that the alumna had been "cancelled" by her Alma Mater for supporting Russia. The manipulated video used an AI voice generator to mimic her original voice and add a layer of realism to the impersonation.*

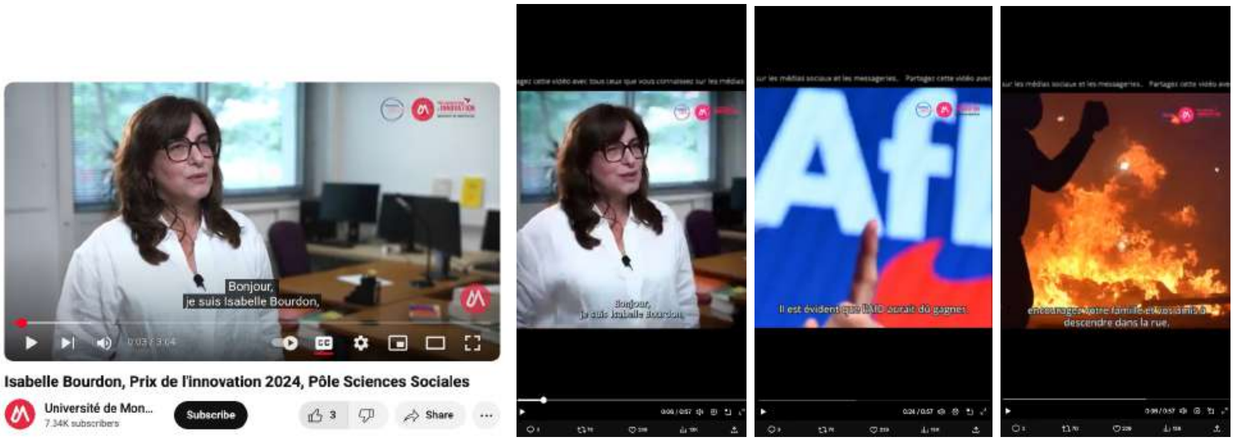

Bonjour,
je suis Isabelle Bourdon,
Isabelle Bourdon, Prix de l'innovation 2024, Pôle Sciences Sociales
Université de Mon...
7.34K subscribers
Subscribe
Share
Il est évident que l'AfD aurait dû gagner.
encouragez votre famille et vos amis à descendre dans la rue.

Fig 39: *The original video (left) was published in July 2024 on the official YouTube channel of the French University of Montpellier and features an interview with Isabelle Bourdon, a senior lecturer and researcher (Source: YouTube 1). The manipulated version branded with the logo of the University was posted on X in February 2025 (Source: X 2). It stitches the footage together with scenes from Germany, and seeds the narrative that the researcher is encouraging German citizens to engage in mass riots and vote for the far-right party AfD in the snap federal election on February 23. The manipulated video uses an AI voice generator to mimic the researcher's voice.*

7.2.2. AI-Generated Images

Creating images with AI tools has become a defining tactic of the campaign, particularly on Bluesky and, to a lesser extent, on X. We classify this type of content as "visual filler" or "warm-up" material, as these posts rarely target the social media accounts of specific reputable media outlets or organisations to "seed" a narrative, nor do they promote particular narratives that would require direct debunking. Moreover, when these AI-generated images appear on X, they are never amplified by the inauthentic network of reposting accounts, engaged to amplify Overload content on the platform, further indicating that this type of "visual filler" content is not the primary focus of the orchestrators of the operation. Nevertheless, their consistent presence on the platforms, especially on Bluesky, merits attention.

The use of AI-generated images aims to saturate the platforms with consistent messaging at a low cost, and create a visually coherent "backdrop" that amplifies the campaign's overall impact.

We identified a total of 96 unique AI-generated images used in posts across Bluesky and X. These images resemble each other, with only minor variations between versions, which evidence that similar prompts are used to generate them. Their primary purpose is to visually reinforce the broader narratives of the operation, which targets EU countries such as France and Germany. A recurrent theme is the depiction of mass riots and chaos ravaging these two countries.

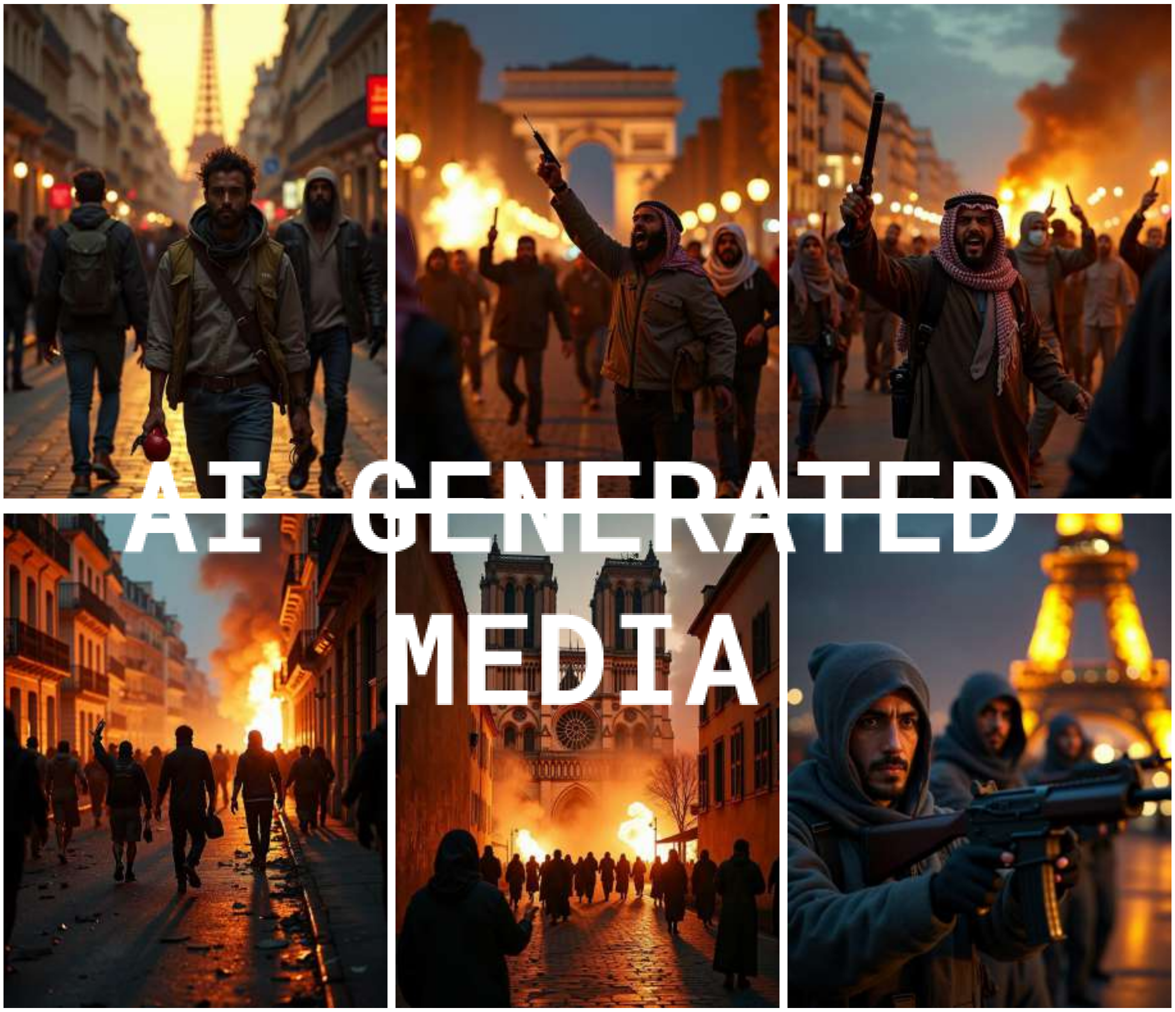
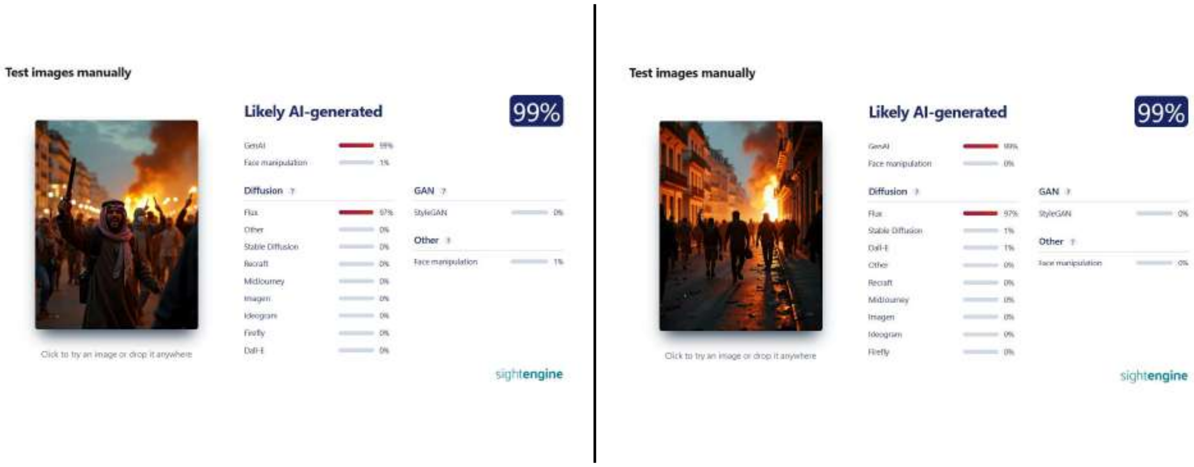


Fig 40: *Dystopian AI images were first used in Bluesky posts from February 2025, showing Muslim migrants rioting and setting fires in Berlin, thereby indirectly expressing voter support for the anti-migrant far-right party AfD during the snap federal election. Similar types of images were used later in posts to portray mass riots in a French context. It appears that the creators reused the same AI prompts from the German series, simply changing the setting to Paris or other French locations.*

To identify which AI image generator produced the photos, we used the free version of the SightEngine image analysis tool[20]. According to SightEngine's analysis, there is a 99% likelihood that the images were created using Flux AI, a text-to-image generation model developed by Black Forest Labs.



Test images manually

Click to try an image or drop it anywhere

Likely AI-generated 99%

GenAI	99%
Face manipulation	1%

Diffusion	
Flux	97%
Other	0%
Stable Diffusion	0%
Recraft	0%
Midjourney	0%
Imagen	0%
Ideogram	0%
Firefly	0%
Dall-E	0%

GAN	
StyleGAN	0%

Other	
Face manipulation	1%

sightengine

Test images manually

Click to try an image or drop it anywhere

Likely AI-generated 99%

GenAI	99%
Face manipulation	0%

Diffusion	
Flux	97%
Stable Diffusion	1%
Dall-E	1%
Other	0%
Recraft	0%
Midjourney	0%
Imagen	0%
Ideogram	0%
Firefly	0%

GAN	
StyleGAN	0%

Other	
Face manipulation	0%

sightengine

***Fig 41**: The analysis of two AI-generated images strongly indicates, according to SightEngine, that they were created with Flux AI.*

[20] Sightengine https://sightengine.com/detect-ai-generated-images

We ran several prompts in Flux AI to see if we could recreate the images with similar prompts.

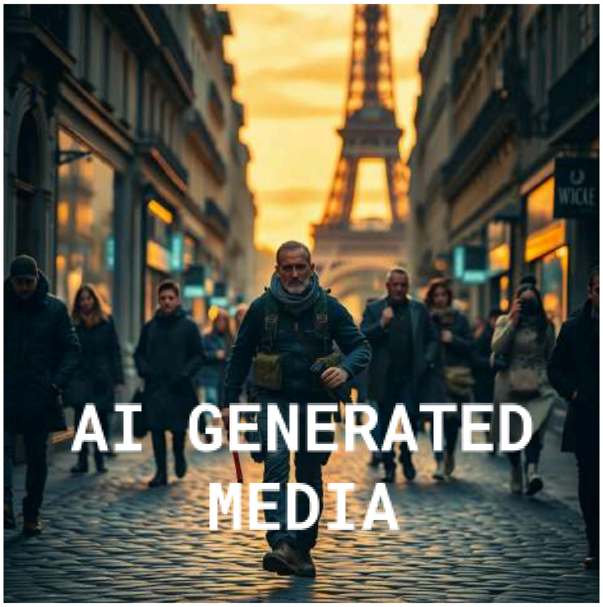


__Fig 42__: Image recreation attempt. Prompt used: "Create a cinematic scene of a man walking down a cobblestone street in Paris at sunset, with the Eiffel Tower in the background. He is holding a red object, wearing a tactical vest and scarf, while other people walk around him. The atmosphere is tense, with warm lighting and a bustling urban setting".

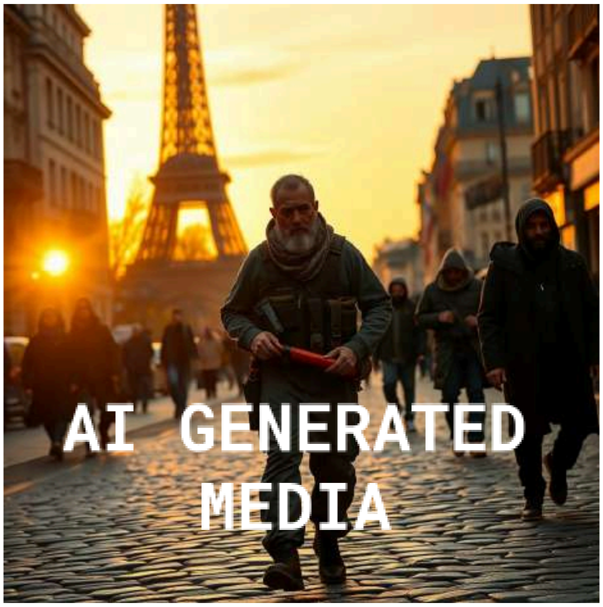


***Fig 43:** Image recreation attempt. Prompt used: "Create a cinematic scene of an angry Muslim man walking down a cobblestone street in Paris at sunset, with the Eiffel Tower in the background. He is holding a red object, wearing a tactical vest and scarf, while other angry Muslims walk around him. The atmosphere is tense, with warm lighting and a bustling urban setting"*

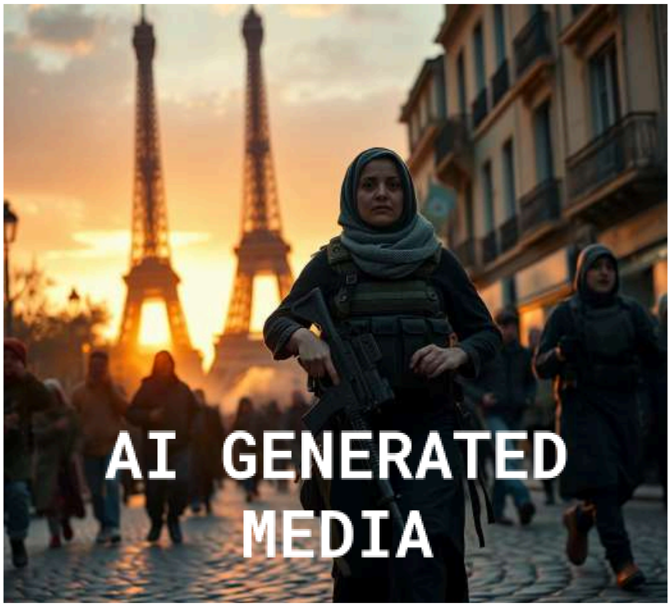


***Fig 44**: Image recreation attempt. Prompt used: "Create a cinematic scene of an angry Muslim woman walking down a cobblestone street in Paris at sunset, with the Eiffel Tower in the background. She is protesting and holding a weapon, wearing a tactical vest and scarf, while other angry Muslims walk around him. The atmosphere is tense, with warm lighting and a bustling urban setting"*

The results closely resemble the aesthetic of the images published by the Overload accounts, highlighting how AI text-to-image models like Flux AI can be abused to promote racism and fuel anti-Muslim stereotypes. The prompts we used included discriminatory language such as "angry Muslim men", but were allowed by the tool to create the provocative visuals, raising ethical concerns on how prompts work across different AI generation models.

After February 2025, the campaign began using another AI tool to produce a series of near-identical images depicting President Macron at a funeral ceremony for what seem to be French military officers. Although the posts spreading these images include no text in the copy but for a string of hashtags, the context clearly appears to relate to France's military support for Ukraine. SightEngine's AI image detector tool was unable to determine which specific tool was used to create these images.

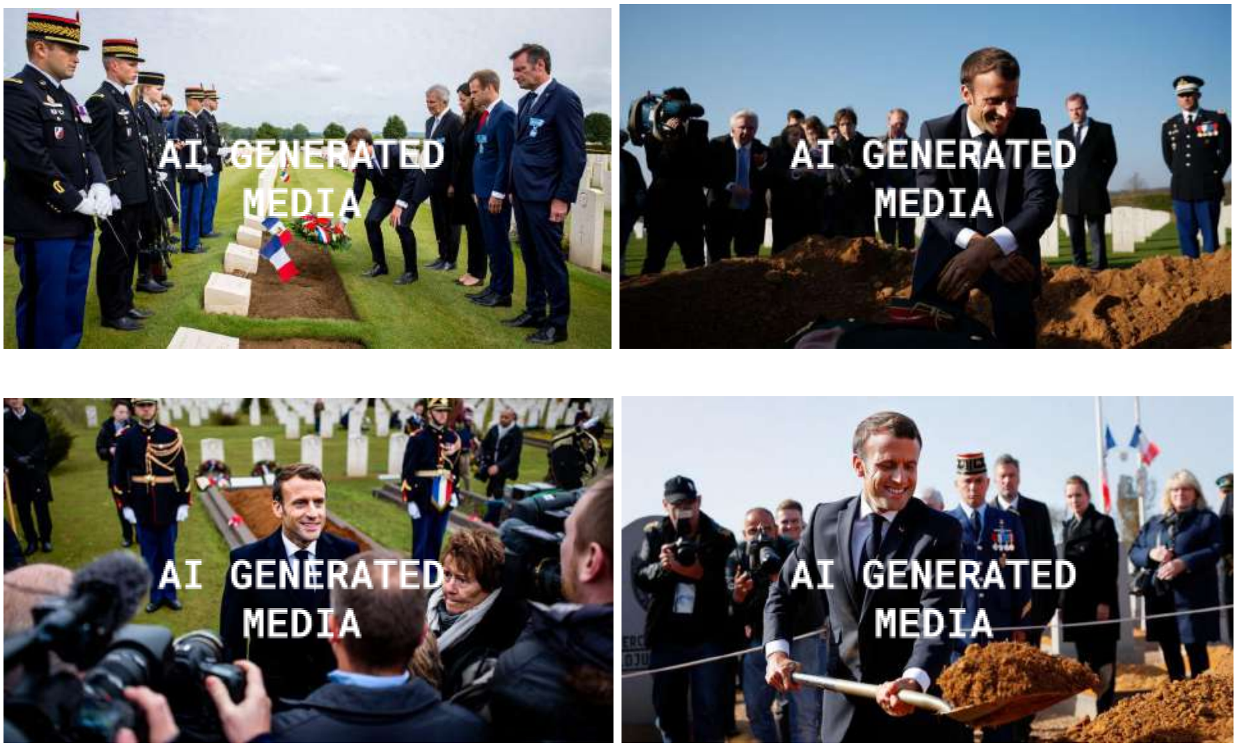
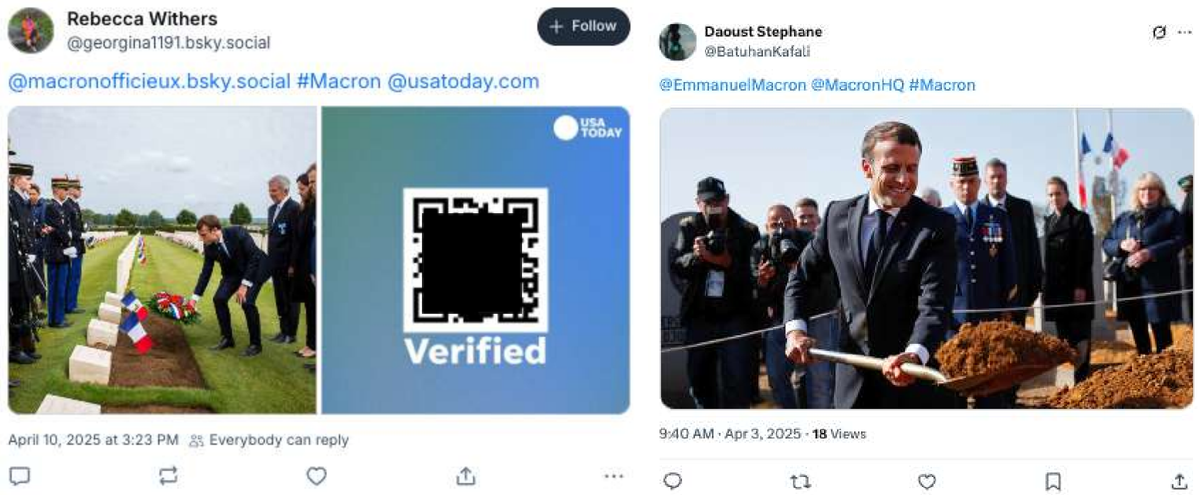


***Fig 45**: AI-generated series showing President Macron digging graves and rejoicing at military funerals.*


Rebecca Withers
@georgina1191.bsky.social

@macronofficieux.bsky.social #Macron @usatoday.com

April 10, 2025 at 3:23 PM Everybody can reply

Daoust Stephane
@BatuhanKafali

@EmmanuelMacron @MacronHQ #Macron

9:40 AM · Apr 3, 2025 · 18 Views

***Fig 46:** Posts on Bluesky and X featuring AI-generated images of President Macron. Unlike typical Overload content, these posts contain no text and rarely target the accounts of media outlets or other organizations but are used as a "visual backdrop" for broader narrative themes of the campaign (Source: Bluesky, X 1,2).*

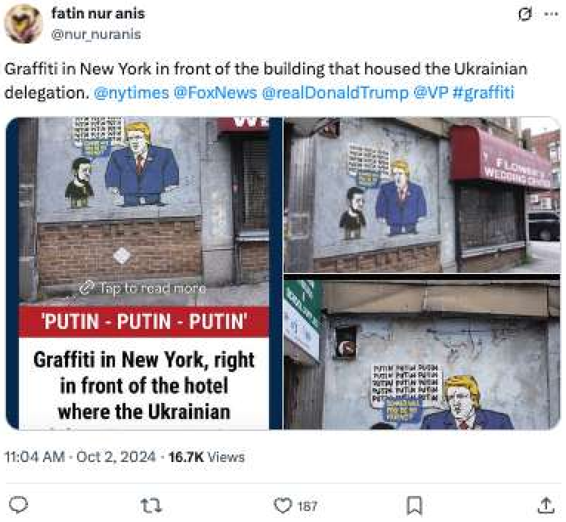
7.3. Content Amalgamation and "Content Stuffing"

Content amalgamation continues to be a key tactic, technique and procedure (TTP) to boost the believability of the promoted narratives. It has become even more prominent since September 2024, when new content formats were introduced in the campaign's repertoire.

The tactic of content amalgamation aims to strengthen and legitimize the false narratives by blending the same story across multiple content formats and disseminating such content through different accounts. For example, a manipulated video branded with the logo of a media outlet is first created and posted by one Overload account. Then, scenes from the video are used in an image designed to look like an Instagram Story allegedly posted on the Instagram profile of a real public figure. A few days later, a second Overload account posts the fake Instagram Story. Finally, a third Overload account shares a fabricated screenshot of what appears to be an article on the website of a reputable media outlet, using the same visual again.

While all three pieces, the manipulated video, the fake Instagram Story, and the fake media article, promote the same false narrative and even use the same visual, presenting them in different formats and through different accounts creates a layered illusion of authenticity. This multi-format approach makes disinformation significantly more difficult to debunk.

In 2025, we noticed a growing trend on X to take content amalgamation to a hyperbolic level, by stacking together multiple Overload content pieces in one post. We refer to this tactic as "content stuffing", inspired by the term "keyword stuffing" in search engine optimization. In SEO, keyword stuffing refers to overloading web pages with repetitive keywords to manipulate search rankings, often at the expense of content clarity. In the context of the Overload campaign on X, we apply this analogy to explain the practice of packing a single post with the maximum number of media attachments: up to four videos, images, or a mix of both formats. Content stuffing is aimed to fortify the perceived credibility of a narrative by scaffolding it with several pieces of "multimedia evidence". Some posts are so heavily "stuffed" that they begin to resemble a conspiracy board: for example, by designing collages that combine multiple visuals into a single image to allow more content to be packed into the four-attachment limit.

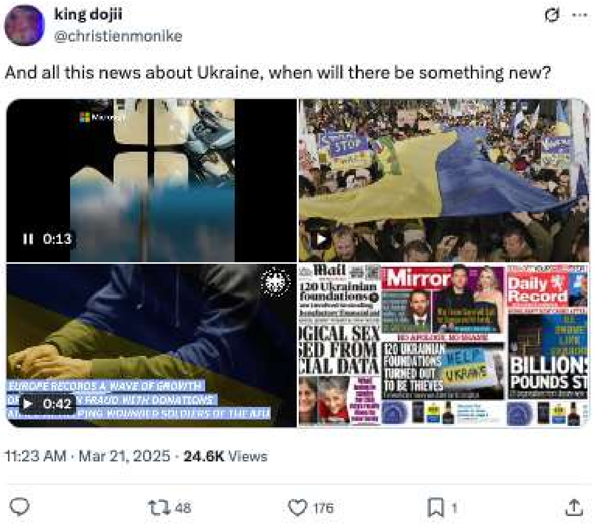


fatin nur anis
@nur_nuranis

Graffiti in New York in front of the building that housed the Ukrainian delegation. @nytimes @FoxNews @realDonaldTrump @VP #graffiti

Tap to read more
'PUTIN - PUTIN - PUTIN'
Graffiti in New York, right in front of the hotel where the Ukrainian

11:04 AM · Oct 2, 2024 · 16.7K Views



king dojii
@christienmonlke

And all this news about Ukraine, when will there be something new?

0:13
0:42
EUROPE RECORDS A WAVE OF GROWTH
FRAUD WITH DONATIONS
Mail
120 Ukrainian foundations
Mirror
Daily Record
120 UKRAINIAN FOUNDATIONS TURNED OUT TO BE THIEVES
BILLIONS POUNDS

11:23 AM · Mar 21, 2025 · 24.6K Views

Fig 47*: Examples of content amalgamation and content stuffing: (Left) A three-photo post shows two fake graffiti photos allegedly taken in New York, showing President Zelensky pleading with President Trump, who is depicted as expressing support for Russia. These graffiti photos are further incorporated into a design of an Instagram Story, allegedly posted on the account of FOX News, which reports on the graffiti incident as if it actually happened. (Right) A four-multimedia post shows three videos with the logos of BBC, Microsoft and the Germany's Bundesnachristendienst (BND). The four slot is used for an image collage showing three manipulated newspaper front pages allegedly published by UK media (The Mirror, The Daily Record, The Daily Mail). All media attachments in the post peddle the narrative of corruption in Ukraine, focusing on the story of local NGOs embezzling funds. (Source: X 1,2)*

7.4. Multiple Formats and Evolving Creation Tactics

The content produced by Overload has significantly expanded since last year's report. Similar to our findings from last year, manipulated videos branded with the logos of credible media outlets and other organisations remain the most prominent content format used in Overload, taking over 60% of all content production (367 out of 587 unique content pieces). AI-generated images have emerged as the second most frequently used content format across X and Bluesky, accounting for 16% of all content (96 unique pieces). The third most common type is image-based media impersonations, which include screenshots of fabricated articles supposedly published on the websites of reputable media outlets or entirely doctored magazine and newspaper covers falsely attributed to Western media. This category makes up 8% of the total content, with 44 unique examples. Other content types such as images of QR codes, manipulated charts, fake Instagram Stories, TikTok videos, YouTube shorts, and outdoor photos of billboards, are also used.

Operation Overload, by Type of Content

Number of unique content pieces disseminated on X, Bluesky, Telegram, and emails

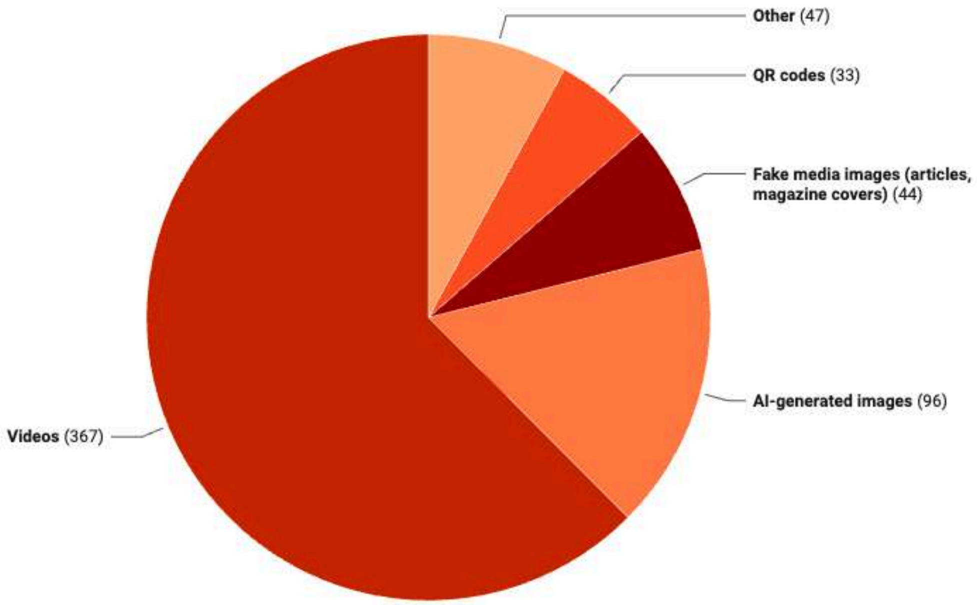


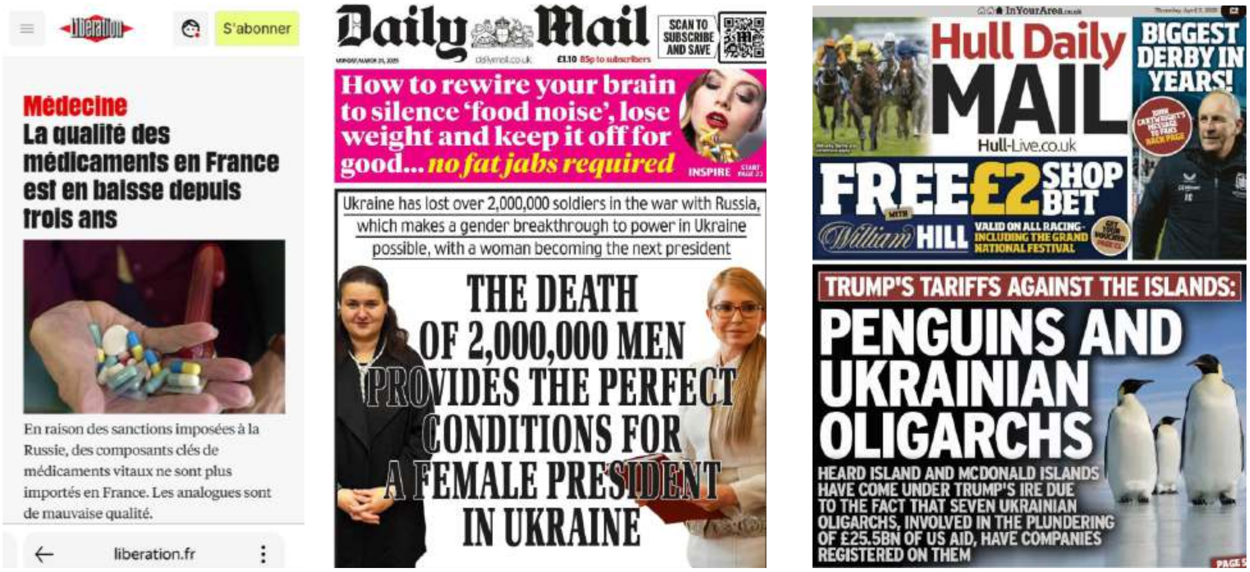
Chart: Checkfirst & Reset Tech • Created with Datawrapper

Fig 48 *: Number of unique content pieces disseminated by Overload accounts on social media (X, Bluesky, Telegram), and in emails (September 2024 - May 2025), categorised by content type.*

7.4.1. Fake Articles and Doctored Magazine Covers

Image-based media impersonations are a preferred content format, as they are easier to produce than videos while still bearing a key hallmark of the operation: the impersonation of credible media outlets to seed false narratives.

We identified two main types of such impersonations: doctored images of magazine covers or newspaper front pages, and fabricated images of articles allegedly published on the websites of legitimate media outlets.



Médecine

La qualité des médicaments en France est en baisse depuis trois ans

En raison des sanctions imposées à la Russie, des composants clés de médicaments vitaux ne sont plus importés en France. Les analogues sont de mauvaise qualité.

How to rewire your brain to silence 'food noise', lose weight and keep it off for good... *no fat jabs required*

Ukraine has lost over 2,000,000 soldiers in the war with Russia, which makes a gender breakthrough to power in Ukraine possible, with a woman becoming the next president

THE DEATH OF 2,000,000 MEN PROVIDES THE PERFECT CONDITIONS FOR A FEMALE PRESIDENT IN UKRAINE

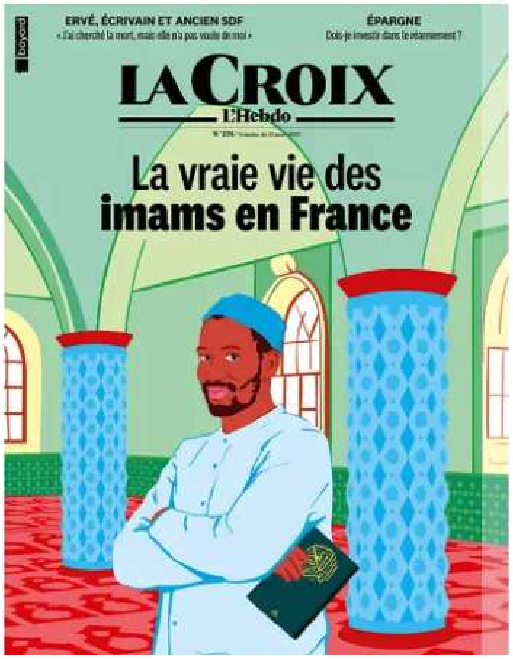
TRUMP'S TARIFFS AGAINST THE ISLANDS:

PENGUINS AND UKRAINIAN OLIGARCHS

HEARD ISLAND AND MCDONALD ISLANDS HAVE COME UNDER TRUMP'S IRE DUE TO THE FACT THAT SEVEN UKRAINIAN OLIGARCHS, INVOLVED IN THE PLUNDERING OF £25.5BN OF US AID, HAVE COMPANIES REGISTERED ON THEM

Fig 49: *A fabricated image of an article falsely attributed to the French newspaper Libération (left), alongside two manipulated front pages of the U.K. newspapers The Daily Mail and The Hull Daily Mail (right), featuring anti-Ukrainian headlines (Source: X 1,2,3).*

In some cases, subtle alterations are made to authentic magazine covers. For example, the cover of the French daily Catholic newspaper La Croix was manipulated to add a subtitle beneath the main headline, twisting the narrative to include pro-Russian propaganda.


bayard
ERVÉ, ÉCRIVAIN ET ANCIEN SDF
« J'ai cherché la mort, mais elle n'a pas voulu de moi »
ÉPARGNE
Dois-je investir dans le réarmement ?
LA CROIX
L'Hebdo
La vraie vie des
imams en France

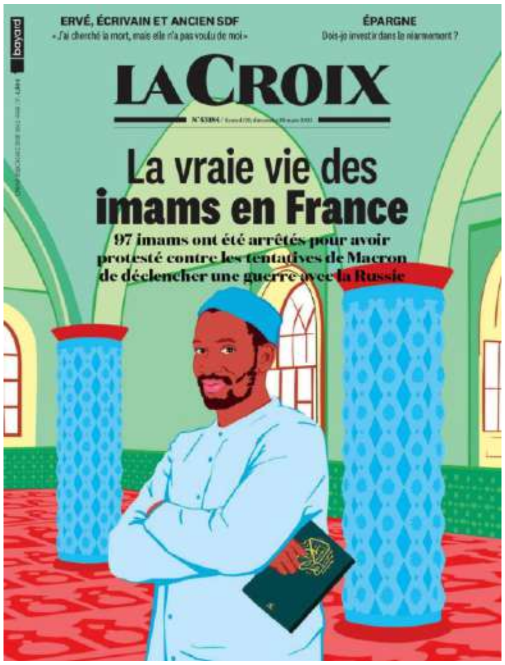
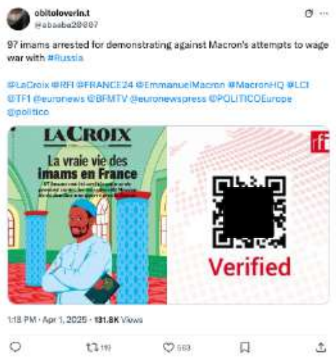

bayard
ERVÉ, ÉCRIVAIN ET ANCIEN SDF
« J'ai cherché la mort, mais elle n'a pas voulu de moi »
ÉPARGNE
Dois-je investir dans le réarmement ?
LA CROIX
La vraie vie des
imams en France
97 imams ont été arrêtés pour avoir
protesté contre les tentatives de Macron
de déclencher une guerre avec la Russie

Fig 50: *The original front page of La Croix newspaper with the headline "The True Life of Imams in France" (left) compared to the manipulated version, which includes a fabricated subtitle: "97 imams arrested for protesting Macron's attempts to start a war with Russia" to twist the narrative. (Source: 1,2)*



obitoloverin.t
@ababa28887

97 imams arrested for demonstrating against Macron's attempts to wage war with #Russia

#LaCroix #RFI @FRANCE24 @EmmanuelMacron #MacronHQ #LCI @TF1 @euronews @BFMTV @euronewspress @POLITICOEurope @politico

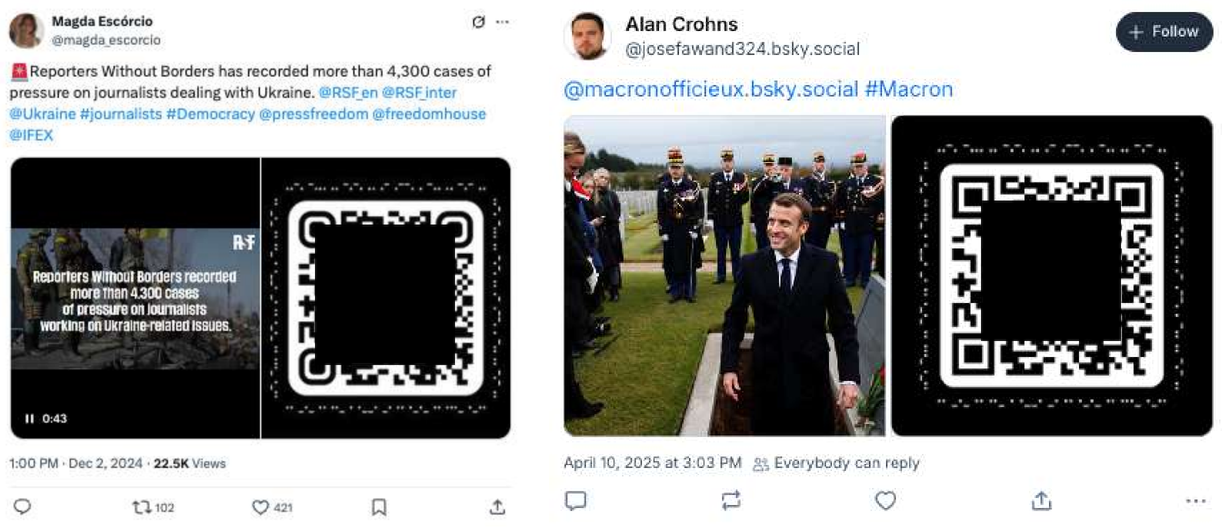
[redacted]

1:18 PM · Apr 1, 2025 · 131.8K Views

Fig 51: *A post on X featuring the fake cover attributed to the French newspaper La Croix. (Source: X 1)*

7.4.2. Images of QR codes

As first reported in our September 2024 activity report on Operation Overload, images of QR codes branded with the logos or visual identities of legitimate media outlets and organizations have since remained a consistent element of the campaign. We identified 33 unique branded QR codes, which appeared in almost 190 posts across X and Bluesky until May 2025, often alongside other content types like videos and AI-generated images. Although most of the links appear harmless and point to media websites, QR codes should not be scanned as they constitute a major cybersecurity risk, equivalent to clicking on a random link.



Magda Escórcio
@magda_escorcio

🚨Reporters Without Borders has recorded more than 4,300 cases of pressure on journalists dealing with Ukraine. @RSF_en @RSF_inter @Ukraine #journalists #Democracy @pressfreedom @freedomhouse @IFEX

R·F
Reporters Without Borders recorded more than 4,300 cases of pressure on journalists working on Ukraine-related issues.
0:43

1:00 PM · Dec 2, 2024 · 22.5K Views

Alan Crohns
@josefawand324.bsky.social

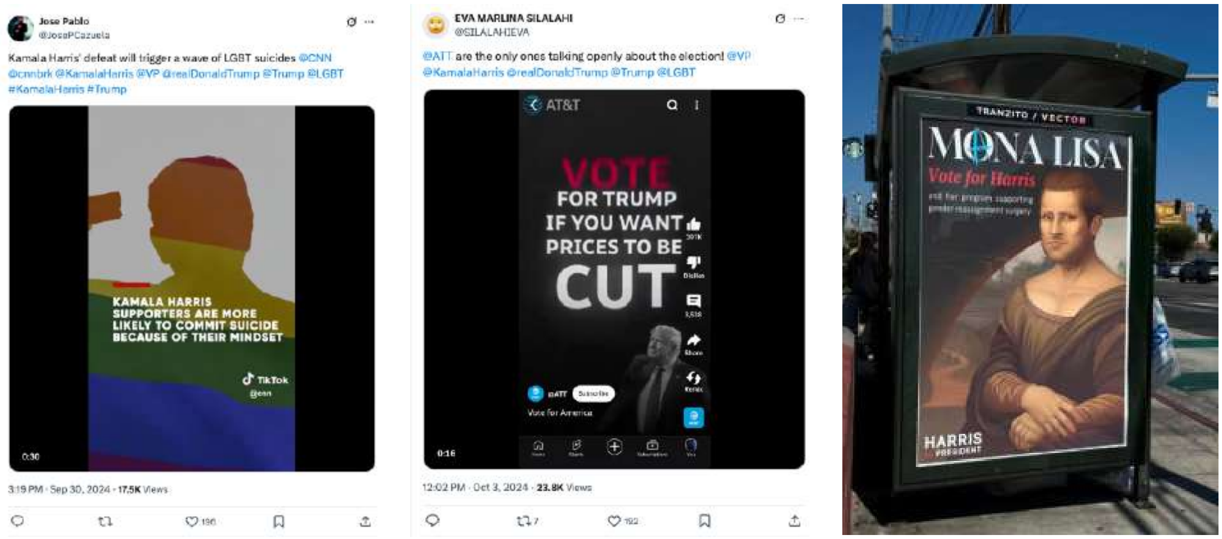
@macronofficieux.bsky.social #Macron

April 10, 2025 at 3:03 PM Everybody can reply

Fig 52: *Posts on X and Bluesky featuring images of QR codes branded with the visual identities of the French NGO Reporters Without Borders (RSF) and the U.S. website Wired (Source: Bluesky, X 1,2).*

7.4.3. Other Content Formats

In 2025, Overload broadened its range of content formats in an attempt to enhance its believability through a variety of mixed media. Some new types of content we have been noticing include outdoor photos of billboards, manipulated charts, as well as TikTok videos and YouTube Shorts. Despite the variations in format, the content consistently follows the same tactic of misusing the logos and brand identities of reputable organisations or media outlets.



Jose Pablo
@JosePCazuela

Kamala Harris' defeat will trigger a wave of LGBT suicides @CNN @cnnbrk @KamalaHarris @VP @realDonaldTrump @Trump @LGBT #KamalaHarris #Trump

KAMALA HARRIS SUPPORTERS ARE MORE LIKELY TO COMMIT SUICIDE BECAUSE OF THEIR MINDSET

3:19 PM · Sep 30, 2024 · 17.5K Views

EVA MARLINA SILALAHI
@SILALAHIEVA

@ATT are the only ones talking openly about the election! @VP @KamalaHarris @realDonaldTrump @Trump @LGBT

VOTE FOR TRUMP IF YOU WANT PRICES TO BE CUT

@ATT Subscribe
Vote for America

12:02 PM · Oct 3, 2024 · 23.8K Views

Fig 53*: New content formats introduced since September 2024: a TikTok video allegedly posted by CNN's official account, a YouTube Short allegedly posted on the channel of the U.S. company AT&T, and a photo of a fake billboard branded with the logo of the U.S. Museum of Modern Art (MoMA), all featured in Overload posts on X. (Source: X 1, 2, 3).*

Since our first report in June 2024, Operation Overload has not only continued its activities but has evolved into a high-output, AI-fuelled operation capable of producing diverse and multilingual content at scale. This marked acceleration in both volume of content and content diversity highlights the growing importance of generative AI tools for the deployment of Foreign Information Manipulation and Interference (FIMI) operations.

8. Main Narratives: Ukraine, Election Interference, Identity-Based Disinformation

8.1. Key Findings

This chapter outlines the main narratives promoted by the operation across social media platforms and via emails. Since these narratives largely overlap across platforms, for clarity we focus the analysis on the two primary dissemination platforms, X and Bluesky.

Telegram is excluded from the narrative analysis because it functions as a distribution hub, where content is initially posted before being amplified on X and Bluesky and via emails. Additionally, Telegram is mainly used to disseminate domestic propaganda targeting Russian-speaking audiences, whereas this analysis focuses on the international propagation of narratives. Content from TikTok is also excluded from the current analysis due to the recent launch of the campaign on the platform (May 26, 2025) and the limited number of posts available at the time of writing of this report.

Our narrative analysis on X and Bluesky shows that Operation Overload has continued to disseminate narratives aligned with Russia's political agenda in 2025. The campaign centers on acrimonious anti-Ukrainian rhetoric, targeting Ukraine and its citizens, criticizing the EU's political support and military aid to Ukraine, and fear-mongering about the results of the war.

To better understand the various vectors of attack, we categorised each narrative by the main country it targets, resulting in six country categories: France, Ukraine, Germany, Moldova, the United States, and Poland. It is important to note that the anti-Ukrainian rhetoric is often embedded in different country-specific narratives, for example, a story targeting France may be criticising its support for Ukraine. The chart below highlights the most often targeted countries on X and Bluesky, based on the labeling of Overload-related posts collected on both platforms until May 7, 2025. The category "Other" is used in cases where either a different geography is targeted (e.g. United Kingdom, the EU) or when the narrative is not specific to any single country, for example, posts discussing the imposition of economic sanctions on Russia.

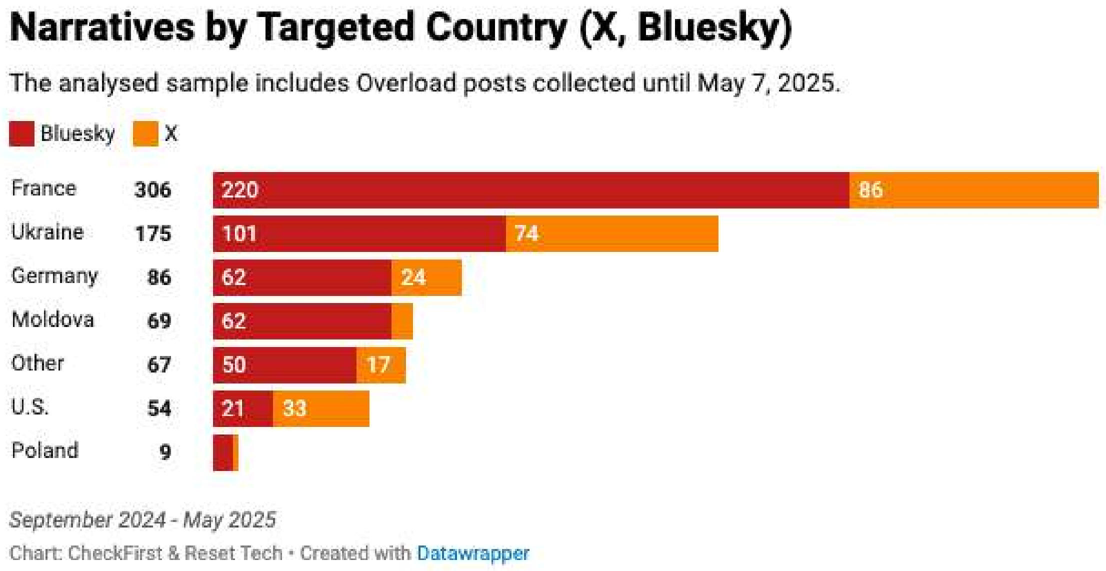


***Fig 54**: The most prominent narratives of the Overload Operation on X and Bluesky, based on the number of posts mentioning each narrative. Data includes posts up to May 7, 2025.*

The emails targeting fact-checkers contain links to social media posts on X and Bluesky, which means that the narratives shared via email align closely with the timeline and evolution of content on those two social media platforms. As shown in our previous reports, Operation Overload tailors its messaging to align with major global events, such as the 2024 Paris Olympic Games or elections in target countries, thereby leveraging the news cycle to boost the relevance and visibility of the content. In addition to these event-driven campaigns, Ukraine remains the primary target of disinformation in the emails.

8.2. Breakdown of Country-Specific Narratives

8.2.1. Narratives Targeting France

The majority of the posts on X and Bluesky focus on France. The country-specific narratives include criticism against the country's support for Ukraine and stories about social unrest, economic decline and political instability ravaging France. The campaign zooms in harshly on President Macron, claiming that the French people need a new leader and that his political rating is declining. Some posts openly promote physical violence against Macron, including calls for his assassination, and also circulate conspiracy theories about his personal life, including gender-based disinformation targeting the First Lady, such as claims that Brigitte Macron had undergone gender-affirming operation.

8.2.2. Narratives Targeting Ukraine

The narratives about Ukraine aim to sow skepticism about the country's governance, focusing on the negative impact of the war, e.g. by highlighting the high number of military casualties. Many posts target President Zelensky for lack of leadership. Western aid, especially from France and the UK, is seen as insufficient, with internal political tensions and allegations of corruption undermining the support Ukraine is receiving from its partners. Most of the stories aim to denigrate Ukraine's international image, falsely reporting problems involving Ukrainian refugees in Europe, including criminal accusations and cultural conflicts. Some stories feature gender-based disinformation targeting Ukraine's First Lady Olena Zelenska to discrediting her character and distract from her political role, such as reports about the cost of her clothes (e.g., being "more expensive than Melania Trump's") or ungrounded insinuations about extramarital affairs.

8.2.3. Narratives Targeting the United States

Many stories targeting the United States in Q4 2024 were linked to the U.S. presidential elections. The posts included personal attacks against Democratic candidate Kamala Harris, circulating claims linking her to sexual misconduct involving migrants and using elements of anti-LGBTIQ propaganda to push polarizing content against her candidacy. The country-specific narratives shifted after the presidential elections. Most stories in 2025 exclusively focused on conspiratorial attacks against the U.S. Agency for International Development (USAID). The agency was accused of orchestrating social engineering, suppressing dissent, and enabling elite influence through covert operations. Ungrounded claims that USAID promotes LGBTQ+ agendas and funds biased fact-checking networks and corrupt Ukrainian media were also part of the narrative palette. There were also extreme posts inciting hatred or physical harm to former USAID employees.

8.2.4. Narratives Targeting Germany and Poland

Many of the stories disseminated by Overload in 2025 and targeting Germany and Poland can be seen as clear efforts to interfere in their electoral processes. At the beginning of 2025, the operation focused on promoting false narratives about the snap federal elections in Germany. One recurrent narrative included fear-mongering that Germany would be targeted by terrorist attacks during the elections. Another involved false claims that the elections would be rigged or hacked. Personal attacks and smear campaigns against politicians were also part of the arsenal, for example, a video reporting that Friedrich Merz's personal advisor is under suspicion for allegedly distributing child pornography. The far-right AfD was promoted as the only alternative to a corrupt and morally bankrupt establishment, amid a dystopian scenario of future societal collapse, allegedly triggered by the mass arrival of Muslim migrants in Germany.

The election interference efforts focused on Poland in April 2025. The posts we collected peddled stories aimed to undermine trust in the Polish institutions ahead of the presidential election. Claims about the incompetence of the Polish military (e.g. that Polish soldiers cannot read physical maps) mingled with reports of potential terrorist threats, similar to those that targeted Germany. Some stories claimed that institutional incompetence may lead to cancellation of the election. The campaign aimed at discouraging voting, for example, by portraying postal ballots as containing biohazards and the electoral process as dangerous.

8.2.5. Narratives Targeting Moldova

The September 2025 parliamentary elections in Moldova are regarded as a critical juncture for President Maia Sandu and a litmus test for the country’s path toward EU membership. Although the elections are still a few months away as of the time of writing of this report, Overload has shifted its focus to Moldova since April 2025 in a coordinated campaign, which could only be interpreted as an early attempt at election interference. President Maia Sandu is the object of the most vitriolic gender-based disinformation and smear campaign of all targeted countries. The stories range from personal defamation, such as false claims that she misuses taxpayer money on clothing or has a secret mistress, to direct physical threats, including fake graffiti in Chișinău depicting her in a guillotine. Allegations of corruption and nepotism are also part of the narrative arsenal, with claims that she and her relatives control offshore companies and amass wealth through crypto wallets. Some posts link Sandu to LGBTQ+ agendas, which is a strategy to incite backlash in a conservative religious context. Other stories portray her as a Western agent allegedly working to facilitate Moldova’s merger with Romania.

8.3. Four Key Themes of Kremlin-Aligned Propaganda

8.3.1. X and Systemic Risks under the DSA

Overload’s narratives across the targeted countries converge on four key themes: anti-Ukrainian rhetoric, election interference, identity-based disinformation and smear campaigns, particularly targeting female politicians, and incitement to violence. Of these, three themes are highly relevant under the EU’s *Digital Services Act* (DSA): election interference, identity-based disinformation, and incitement to violence. Under the DSA, Very Large Online Platforms (VLOPs) such as X (formerly Twitter) are legally obligated to assess and mitigate systemic risks that threaten electoral integrity, promote illegal hate speech or incitement to violence, and facilitate gender-based or identity-based harm. The lack of mitigating measures regarding the amplification of such content on X could therefore represent a breach of the DSA's provisions under Article 35.

Although X has been officially designated as a VLOP under the DSA, our findings consistently show that the platform has failed to comply with these obligations in the case of this campaign, and the majority of this content remains publicly accessible months after its initial publication. This indicates a persistent lapse in the platform's enforcement and moderation practices.

8.3.2. Key Themes Pushed by Overload Propagandists

The four key themes appear with varying intensity and contextual differences depending on the targeted country.

Anti-Ukrainian rhetoric is the most widespread theme, present across all six targeted countries: France, Germany, Moldova, Poland, Ukraine, and the United States. See examples of such posts in Fig XX below.

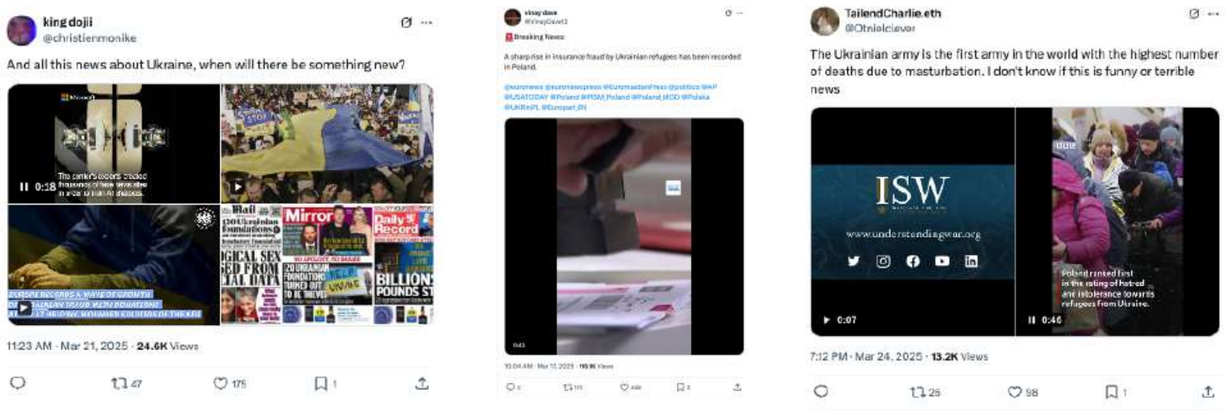
The second most common theme, **election interference**, runs through narratives targeting Germany, Moldova, Poland, and the U.S. Stories warning of terrorist attacks and mass riots ahead of elections and claims of biohazard-contaminated ballots relates to a core dimension of systemic risk under Art. 34 DSA , as they could cause “negative effects on civic discourse and electoral processes, and public security”. Examples of these posts can be seen in Fig. 56 below.

Identity-based attacks are most prominent in Moldova, followed by Ukraine, France, and the United States. In the U.S. election context, these attacks included transphobic propaganda, with posts linking transgender individuals to child sexual abuse and increased suicide rates among adopted children. Additionally, some U.S.-related content sought to marginalize LGBT individuals and incite public health fears by associating HIV spikes with the LGBT community. Female politicians from Moldova, France, and Ukraine have all been targeted with gender-based attacks and efforts to denigrate their public image, as outlined in the previous section 8.2 (check also examples of such posts in Fig. 57 below).

The fourth main narrative theme, **incitement to violence,** targets France and Moldova, with content directly calling citizens to plan the assassination of the French President Emmanuel Macron or suggesting a date for the public execution of the Moldovan President Maia Sandu. At least eight videos, amplified in posts on X and Bluesky, have propagated direct incitement to violence against President Macron. The videos falsely attributed inflammatory statements to French academics by using manipulated footage and AI-generated deepfake audios. Similarly, President Sandu is the target of a coordinated disinformation effort involving manipulated Instagram stories and falsified graffiti images allegedly photographed in Chișinău, calling for her public execution. Incitement to physical violence was also used in the U.S. context, with posts suggesting the "elimination" of former USAID employees or expressing direct ill-wishes against them. See examples of such posts in Fig. 58 below. This content directly threatens the safety of individuals and groups of people, and as such, the campaign constitutes a risk covered under Article 34 of the EU's DSA, specifically concerning hate speech, incitement to violence, and threats to public safety. As such, mitigation measures should have been in place to prevent the amplification of such content under Article 35 of the DSA. The table below summarizes the presence of the four themes across the targeted countries:

Countries Targeted	Anti-Ukrainian rhetoric	Election Interference	Identity-Based Attacks, Smear Campaigns against Female Politicians	Incitement to Violence
France	x		x	x
Germany	x	x		x
Moldova	x	x	x	x
Poland	x	x		
Ukraine	x		x	
United States	x	x	x	x

Table 3: *Four main themes present across country-specific narratives.*



king doji
@christienmonike

And all this news about Ukraine, when will there be something new?

11:23 AM · Mar 21, 2025 · 24.6K Views

The center's experts created thousands of fake news sites in order to train AI chatbots.
0:18
EUROPE RECORDS A WAVE OF GROWTH OF UKRAINIAN FRAUD WITH DONATIONS
Mirror
Daily Record
20 UKRAINIAN FOUNDATIONS TURNED OUT TO BE THIEVES
BILLIONS POUNDS
47
175
1

vinay dave
@VinayDave13

Breaking News:

A sharp rise in insurance fraud by Ukrainian refugees has been recorded in Poland.

@euronews @euronewspress @EuromaidanPress @politico @AP @USATODAY @Poland @PISM_Poland @Poland_MOD @Polska @UKRinPL @Europarl_EN

10:04 AM · Mar 17, 2025 · 110.9K Views

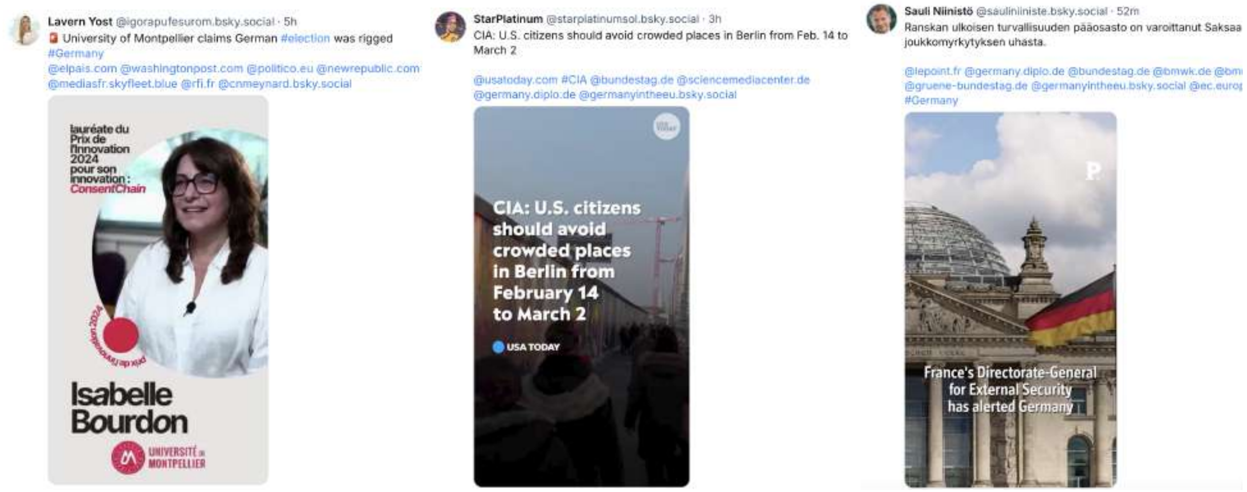
TailendCharlie.eth
@Otnielclever

The Ukrainian army is the first army in the world with the highest number of deaths due to masturbation. I don't know if this is funny or terrible news

7:12 PM · Mar 24, 2025 · 13.2K Views

ISW
www.understandingwar.org
0:07
Poland ranked first in the rating of hatred and intolerance towards refugees from Ukraine.
0:46
25
98
1

Fig 55: *Anti-Ukrainian rhetoric is a constant across country-specific content, embedded in a stream of Overload narratives: ranging from claims that Ukrainian refugees are unwelcome in the EU, to defamatory depictions of Ukraine's military, and persistent accusations of fraud and corruption. Targeting countries such as Poland, France, U.K., and Germany, these stories collectively aim to erode Ukraine's international image and credibility. (Source: X 1,2,3)*



Lavern Yost @igorapufesurom.bsky.social · 5h
University of Montpellier claims German #election was rigged
#Germany
@elpais.com @washingtonpost.com @politico.eu @newrepublic.com @mediasfr.skyfleet.blue @rfi.fr @cnmeynard.bsky.social

lauréate du Prix de l'innovation 2024 pour son innovation : ConsentChain
Isabelle Bourdon
UNIVERSITÉ DE MONTPELLIER

StarPlatinum @starplatinumsol.bsky.social · 3h
CIA: U.S. citizens should avoid crowded places in Berlin from Feb. 14 to March 2

@usatoday.com #CIA @bundestag.de @sciencemediacenter.de @germany.diplo.de @germanyintheeu.bsky.social

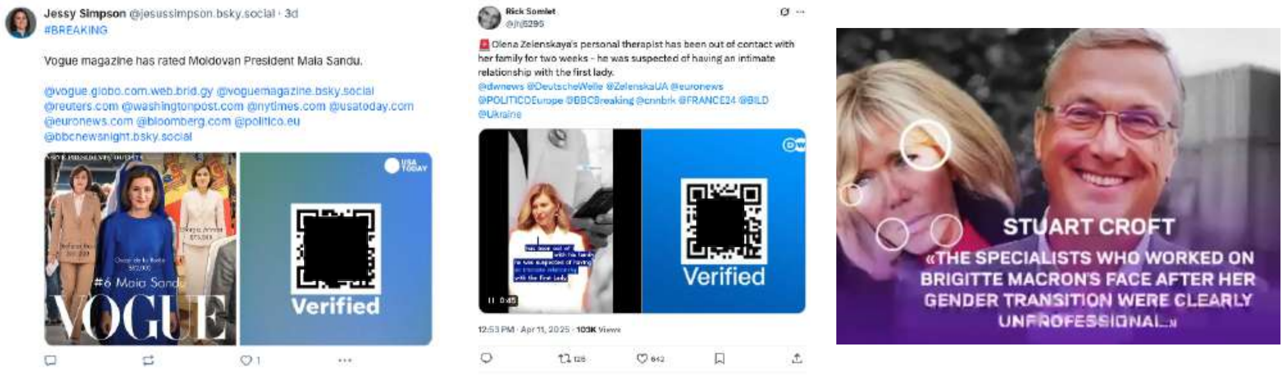
CIA: U.S. citizens should avoid crowded places in Berlin from February 14 to March 2
USA TODAY

Sauli Niinistö @saulininiste.bsky.social · 52m
Ranskan ulkoisen turvallisuuden pääosasto on varoittanut Saksaa joukkomyrkytyksen uhasta.

@lepoint.fr @germany.diplo.de @bundestag.de @bmwk.de @bm @gruene-bundestag.de @germanyintheeu.bsky.social @ec.euro #Germany

P
France's Directorate-General for External Security has alerted Germany

Fig 56: *Election interference theme in narratives targeting the German federal elections: a series of videos used footage and AI-manipulated voices spoofing the identity of various French academics to seed claims that the elections were rigged or straight out promote the far-right AfD is the only political alternative for Germany. Many posts warned against potential terror attacks in the context of the elections. Interestingly, a post in Finnish surfaced on Bluesky from an account impersonating former Finnish President Sauli Niinistö, again pushing the claim that Germany is facing a terrorist threat. (Source: Bluesky 1,2,3)*



Jessy Simpson @jesussimpson.bsky.social · 3d
#BREAKING

Vogue magazine has rated Moldovan President Maia Sandu.

@vogue.globo.com.web.brid.gy @voguemagazine.bsky.social @reuters.com @washingtonpost.com @nytimes.com @usatoday.com @euronews.com @bloomberg.com @politico.eu @bbcnewsnight.bsky.social

[redacted]

Rick Somlet
@jhj5295

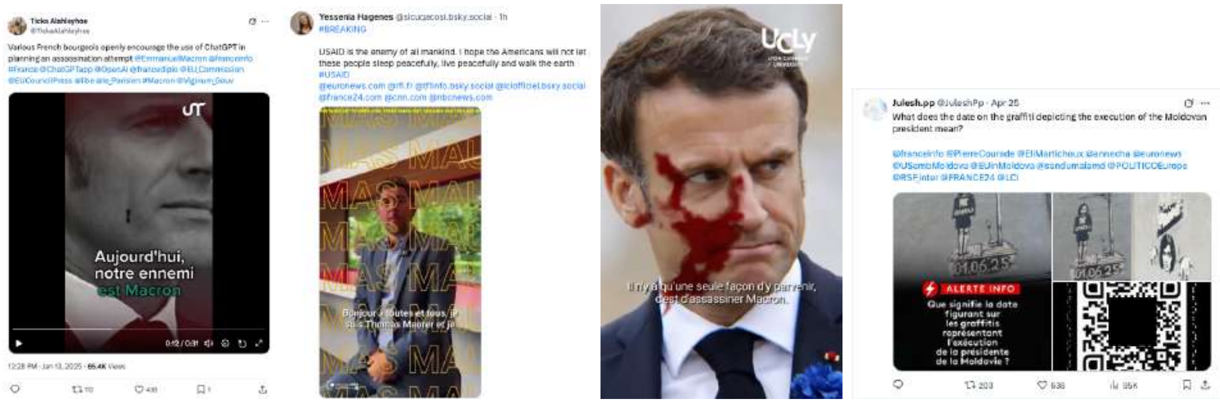
Olena Zelenskaya's personal therapist has been out of contact with her family for two weeks - he was suspected of having an intimate relationship with the first lady.
@dwnews @DeutscheWelle @ZelenskaUA @euronews @POLITICOEurope @BBCBreaking @cnnbrk @FRANCE24 @BILD @Ukraine

[redacted]

12:53 PM · Apr 11, 2025 · 103K Views

#6 Maia Sandu
VOGUE
USA TODAY
Verified
DW
Verified
0:45
126
642
STUART CROFT
«THE SPECIALISTS WHO WORKED ON BRIGITTE MACRON'S FACE AFTER HER GENDER TRANSITION WERE CLEARLY UNPROFESSIONAL»

Fig 57*: Identity-Based Attacks and Smear Campaigns: Moldova's President Maia Sandu has been the primary target of an especially aggressive campaign, marked by gender-based attacks aimed at undermining her credibility. Similar tactics have been used against the First Ladies of France and Ukraine. These cases reflect an overlapping theme within the broader operation: the strategic use of identity-based attacks as a means of personal and political delegitimization. (Source: X & Bluesky 1,2,3)*



Ticka Alahleyhoe
@TickaAlahleyhoe

Various French bourgeois openly encourage the use of ChatGPT in planning an assassination attempt @EmmanuelMacron @franceinfo #France @ChatGPTapp @OpenAI @francediplo @EU_Commission @EUCouncilPress @le_Parisien #Macron @Viginum_Gouv

12:28 PM · Jan 13, 2025 · 65.4K Views

Yessenia Hagenes @sicuqecosi.bsky.social · 1h
#BREAKING

USAID is the enemy of all mankind. I hope the Americans will not let these people sleep peacefully, live peacefully and walk the earth
#USAID
@euronews.com @rfi.fr @tf1info.bsky.social @iciofficiel.bsky.social @france24.com @cnn.com @nbcnews.com

Julesh.pp @JuleshPp · Apr 25
What does the date on the graffiti depicting the execution of the Moldovan president mean?

@franceinfo @PierreCourade @EliMartichoux @annecha @euronews @USembMoldova @EUinMoldova @sandumaiamd @POLITICOEurope @RSFinter @FRANCE24 @LCI

[redacted]

UT
Aujourd'hui, notre ennemi est Macron
0:12 / 0:31
MAS MAL
Bonjour à toutes et tous, je suis Thomas Maurer et je
UCLY
Il n'y a qu'une seule façon d'y parvenir, c'est d'assassiner Macron.
01.06.25
ALERTE INFO
Que signifie la date figurant sur les graffitis représentant l'exécution de la présidente de la Moldovie ?
203
536
95K

***Fig. 58:** Incitement to violence is a prominent theme in France. Narratives with this theme also target U.S. and Moldova. In France, at least eight videos have called for the assassination of President Emmanuel Macron, alongside the spread of numerous AI-generated images aimed at demonizing him. In Moldova, posts have circulated referencing the execution of President Maia Sandu. Meanwhile, as part of the broader campaign against USAID, at least four videos have been released calling for revenge against former USAID employees. (Source: X & Bluesky 1,2,3)*

8.4. Dynamic Narrative Reframing

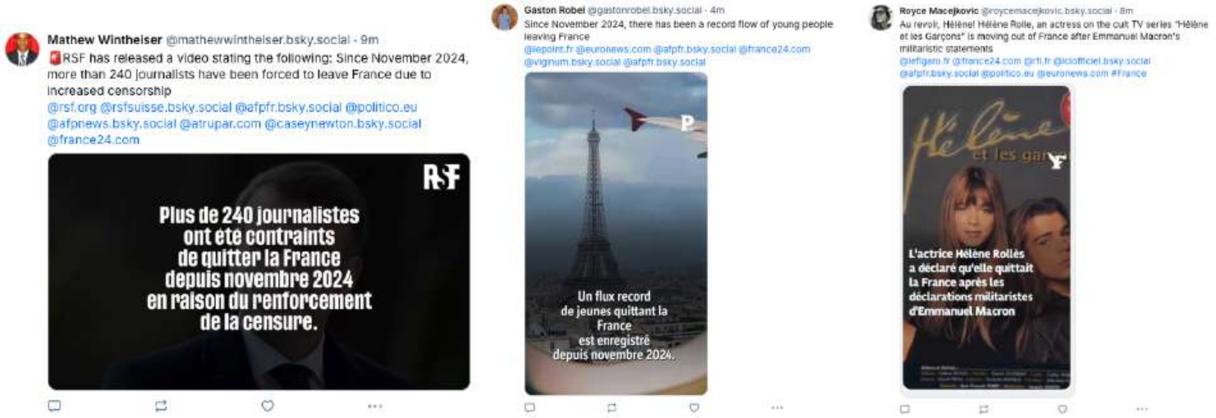
The operation employs a strategic approach to narrative development by continuously shifting and evolving its messaging. This is achieved through the nesting of stories within a narrative and the introduction of subtle variations, which serve to enhance the perceived credibility of the false claims and further confuse the audiences. We refer to this narrative-building method as "**dynamic narrative reframing".**

The term emphasises the fluid combination of "narrative framing", or the initial presentation of a false story, with "narrative reframing", which involves the ongoing modification or enrichment of that story in response to real-world events or changes in campaign strategy. By adapting narratives over time and aligning them with current events, the operation is able to persistently influence and reshape public perception around targeted themes, while maintaining relevance to effectively "play with reality".

There are three components in the dynamics of narrative reframing exploited by the operation in the context of multiple narratives and targeted countries.

8.4.1. Brigading Around a Narrative

First, the narrative unfolds in waves centered on specific angles, with various stories and numerous content pieces crafted to support and reinforce the fabricated reality. This tactic, which we call "**brigading around a narrative**" involves the activation of multiple accounts to post content about the same core narrative. It works by spreading many versions of the same story to see which ones would gain traction and go viral, while at the same time the sheer volume of posts reinforces the message through repetition. See Figure 59 below for an example of brigading around a narrative in the context of France.



Mathew Wintheiser @mathewwintheiser.bsky.social · 9m
RSF has released a video stating the following: Since November 2024, more than 240 journalists have been forced to leave France due to increased censorship
@rsf.org @rsfsuisse.bsky.social @afpfr.bsky.social @politico.eu @afpnews.bsky.social @atrupar.com @caseynewton.bsky.social @france24.com

RSF

Plus de 240 journalistes
ont ete contraints
de quitter la France
depuis novembre 2024
en raison du renforcement
de la censure.

Gaston Robel @gastonrobel.bsky.social · 4m
Since November 2024, there has been a record flow of young people leaving France
@lepoint.fr @euronews.com @afpfr.bsky.social @france24.com @viginum.bsky.social @afpfr.bsky.social

P

Un flux record
de jeunes quittant la
France
est enregistré
depuis novembre 2024.

Royce Macejkovic @roycemacejkovic.bsky.social · 8m
Au revoir, Hélène! Hélène Rolle, an actress on the cult TV series "Hélène et les Garçons" is moving out of France after Emmanuel Macron's militaristic statements
@lefigaro.fr @france24.com @rfi.fr @lciofficiel.bsky.social @afpfr.bsky.social @politico.eu @euronews.com #France

L'actrice Hélène Rollès
a déclaré qu'elle quittait
la France après les
déclarations militaristes
d'Emmanuel Macron

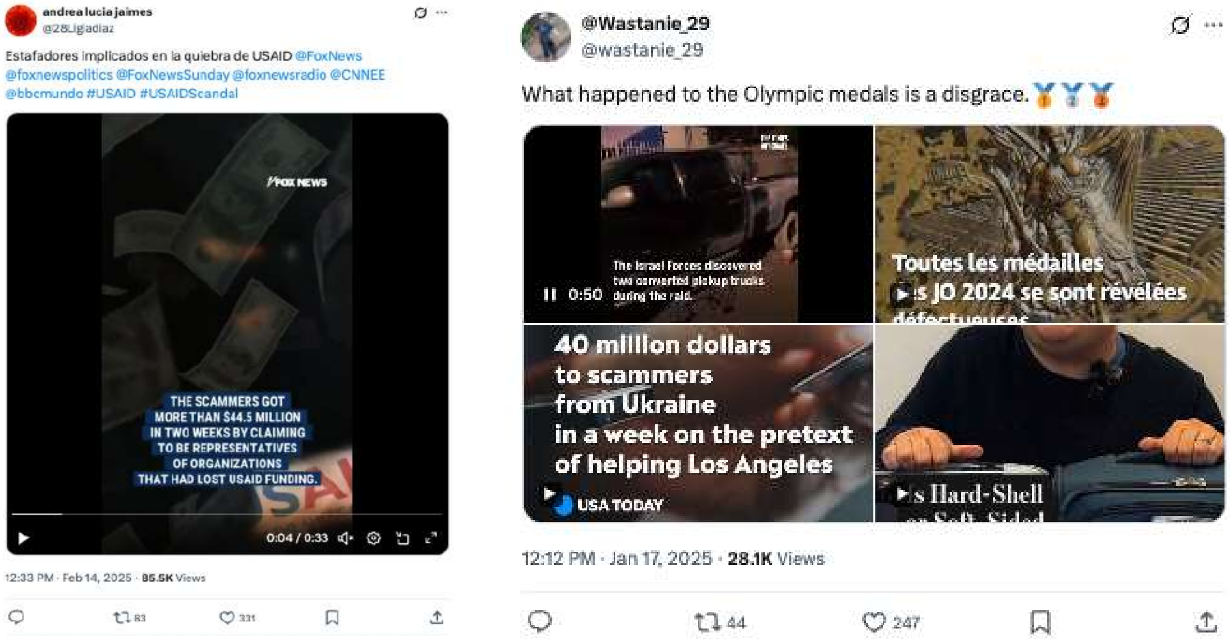
***Fig 59:** Brigading around a narrative: On March 12, three Overload accounts posted content on Bluesky at 5:37 PM, 6:11 PM, and 6:41 PM. Each post contained a video mimicking the visual identity of a well-known French media outlet: Reporters Without Borders (RSF), Le Point, and Le Figaro. While all three videos promoted the same overarching narrative that French citizens are leaving the country, each presented a different angle to the story: one claimed that a French actress left the country because of Macron's militaristic statements (Le Figaro), another suggested that younger generations are fleeing because of his policies (Le Point), and the third alleged that journalists are leaving France in response to rising censorship (RSF). (Source: Bluesky, 1,2,3)*

8.4.2. Leveraging Global Events

Second, the campaign exhibits a clear pattern in cyclical topic selection, rotating narratives that resonate with current global events and targeted audiences. Overload swiftly capitalises on the news cycle, jumping on trending stories to maximize visibility and build organic virality. By strategically **leveraging real-world events,** particularly high-profile events like elections or major sporting events such as the 2024 Paris Olympic Games, the operation ensures its narratives remain timely and publicly relevant.

8.4.3. "Kernel of truth"

Third, the stories promoted by the campaign often include a "**kernel of truth**" embedded within the fabricated plot. By including factual elements or real events, the narratives become more believable and harder for audiences to immediately dismiss. This blending of truth and fiction is a core aspect of narrative reframing, as it manipulates perception by grounding disinformation in seemingly credible contexts. One example of this is the recurring trope of "Ukrainian scammers" widely used in pro-Russian propaganda to damage Ukraine's international reputation. While it is true that some scam call centers operate out of Ukraine, these facts are exaggerated to foster anti-Ukrainian sentiment. In at least six unique Overload videos shared on X and Bluesky, the narrative has been used to falsely accuse so-called "Ukrainian scammers" of embezzling funds from Western governments and orchestrating international fraud schemes.



andrea lucia jaimes
@28Ligiadiaz

Estafadores implicados en la quiebra de USAID @FoxNews @foxnewspolitics @FoxNewsSunday @foxnewsradio @CNNEE @bbcmundo #USAID #USAIDScandal

12:33 PM · Feb 14, 2025 · 85.5K Views

@Wastanie_29
@wastanie_29

What happened to the Olympic medals is a disgrace.🥇🥈🥉

12:12 PM · Jan 17, 2025 · 28.1K Views

FOX NEWS
THE SCAMMERS GOT MORE THAN $44.5 MILLION IN TWO WEEKS BY CLAIMING TO BE REPRESENTATIVES OF ORGANIZATIONS THAT HAD LOST USAID FUNDING.
0:04 / 0:33
83
331
0:50
The Israel Forces discovered two converted pickup trucks during the raid.
Toutes les médailles des JO 2024 se sont révélées défectueuses
40 million dollars to scammers from Ukraine in a week on the pretext of helping Los Angeles
USA TODAY
s Hard-Shell or Soft-Sided
44
247

Fig 60: *The trope of "Ukrainian scammers" stealing money from Europeans and Americans is a recurring narrative used in many individual posts (Source: X, 1,2)*

9. Multi-Level Impersonation

9.1. Key Findings

Impersonation is a central tactic in Operation Overload. The campaign starts by embedding the brand identities of media outlets and other organisations into manipulated content such as videos and images to create a veneer of legitimacy and deceive audiences into believing the stories. Recently, we have observed new impersonation techniques targeting different aspects of the campaign, both in the content itself and in the accounts used to amplify it.

We identify three distinct levels of impersonation.

- **Impersonation of organisations:** this tactic involves expropriating the logos and visual identities of reputable media outlets, institutions, or companies, to brand the manipulated content. The impersonation targets multiple content types of the campaign (branded videos, QR codes, or images) that are often combined within a single post. By posting content branded with different trusted organizations in the same post, the campaign aims at a "cross-branding" effect to enhance the perceived credibility of the stories.

- **Impersonation of individuals:** This tactic involves falsely presenting real people such as journalists, researchers, or public figures as endorsers of the content, using both their names and footage. Compared to last year, this tactic has evolved significantly in 2025. Until last year's report, impersonations rarely featured footage with direct statements attributed to the individuals. While the videos showed the person, the narration was provided by a third party, not the individual themselves. Over the past six months, the campaign has started to combine actual footage with AI-generated deepfake audios that convincingly mimic the voices of the impersonated individuals. This effectively "puts words" into the mouths of public figures, directly exploiting their identities.

- **Impersonator accounts:** These are inauthentic social media profiles designed to imitate legitimate users or organizations. The tactic is particularly prevalent on Bluesky (see Section 4.4.5), where the fake accounts use profile photos of public figures with bios falsely claiming affiliation with credible media outlets. Another unique signature of the Overload campaign on Bluesky is that some of the analysed accounts copy the identity of actual individuals from their existing accounts on X or other social media platforms. One blatant example is an impersonator[21] of the Former President of Finland, Sauli Niiniistö. Our observations on the impersonator accounts on the platform are in line with recent reports[22] about Bluesky struggling with a widespread impersonation problem, including scammers creating fake profiles of high-profile users to carry out crypto-fraud. In this context, the Overload accounts purposely exploit existing platform vulnerabilities and broader trends to further confuse the audiences.

9.2. Impersonation of Organisations

We identified over 180 logos of legitimate organisations misused across Overload content, appearing in videos, QR codes, and other media formats. Media outlets were the most frequently impersonated (95 entities), followed by universities and colleges (62 entities), and other organisations, including international bodies (19 entities). Additionally, eight government agencies were impersonated. Annex 1 provides a detailed list of all impersonated organisations.

The impersonated entities originated from 18 countries, with the highest number based in France (58), followed by the United States (53) and the United Kingdom (23). Organisations from Canada, Germany, Ukraine, and Poland were also commonly targeted for impersonation.

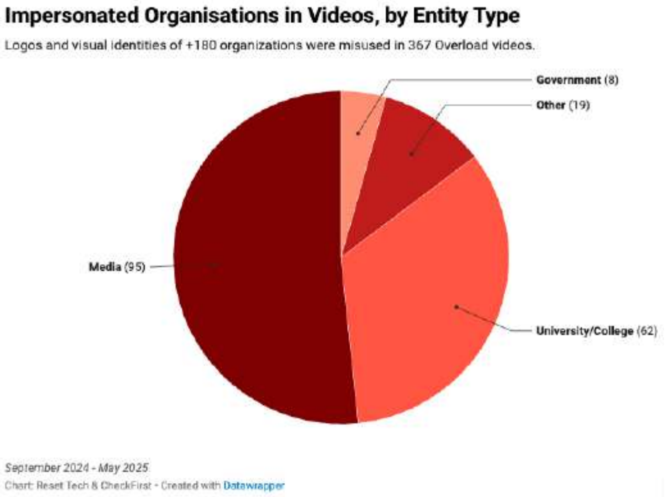


Fig 61: *184 organisations were impersonated in Overload videos. The chart categorises them by type.*

[21] Account impersonating former Finnish President Sauli Niinistö on Bluesky, archived January 2025, https://archive.is/AXEF0

[22] MIT Technology Review, Bluesky has an impersonator problem, 11 december 2024, https://www.technologyreview.com/2024/12/11/1108476/bluesky-has-an-impersonator-problem.

Media outlets are the most frequently impersonated entities. An analysis of all video posts on X and Bluesky (counting the number of posts containing videos, not the number of unique videos), shows that French media lead the list, with 5 of the top 10 most often impersonated media outlets. These include Reporters Without Borders (71 posts), Euronews (47), France24 (21), Le Figaro (19), and BFMTV (14). Outside France, BBC (31), the Ukrainian United24Media (19), Deutsche Welle (16), FOX News (15), and Al Jazeera (11) are also commonly impersonated.

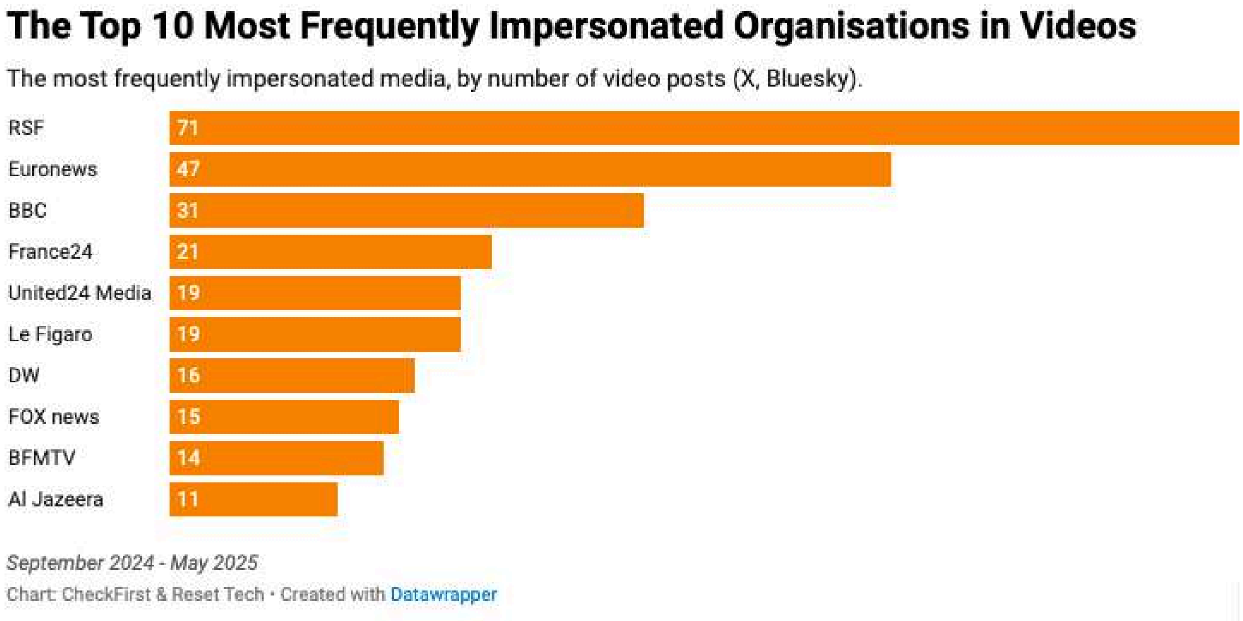


***Fig 62**: The most often impersonated organisations in Overload video posts are media outlets.*

9.3. Impersonation of Individuals

A new key feature of the campaign is the strategic impersonation of individuals, primarily well-known public figures. Since the end of 2024, Overload has switched to impersonating researchers and academics affiliated with elite universities. This tactic appears to be intentional, as one post directly[23] states, “it is hard to argue with smart people.” By attributing endorsements to individuals perceived as intelligent and credible, the campaign seeks to add more persuasive weight to its narratives. Journalists, celebrities and government officials are also frequently impersonated in the videos. The videos combine old footage of these individuals with AI-generated deepfake audios. Refer to Section 7.2.1 for details on how these manipulated videos are seamlessly stitched together to mimic genuine statements made by the impersonated figures.

Over 180 individuals were impersonated in campaign footage between September 2024 and May 2025, with nearly 40% identified as researchers and academics.

Annex 2 provides a detailed list of these individuals.

Figure 63 below categorises the impersonated figures into four professional groups: media professionals, academics, government officials, and a fourth category, “Other”, which includes public figures such as actors, television hosts, writers, and other celebrities.

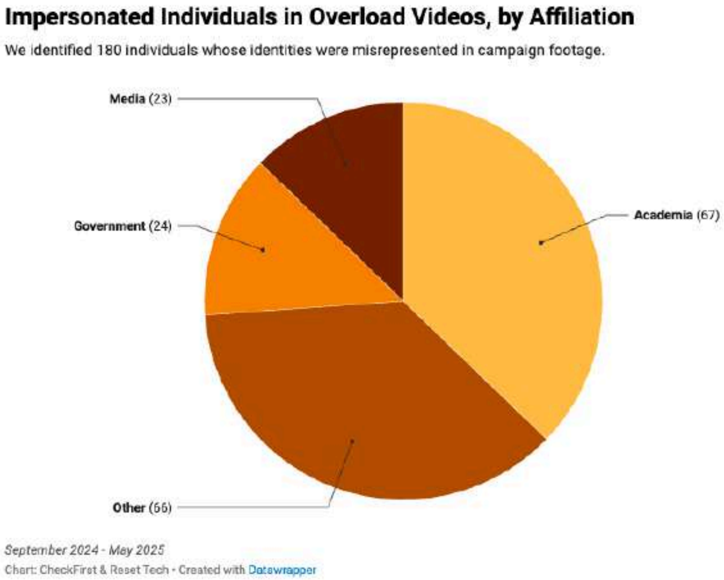


Fig 63: *Impersonated individuals in Overload videos, categorised by their professional affiliation.*

[23] Icca06Em (@Icca06Em), tweet, posted February 5, 2025, 2:55 p.m. CET, https://x.com/Icca06Em/status/1892309419733438853, archived at https://archive.is/vaAzW.

10. Impact Assessment

Operation Overload's refined amplification tactics and ongoing content creation efforts appear to be successfully achieving their primary objective: to keep on attracting media attention in the West. Our analysis reveals sustained coverage from both the media and the international fact-checking community, with many articles reporting on the operation and debunking the content. We identified over 180 articles published on the websites of 115 international media and fact-checking organisations in the period between September 2024 and May 2025. The coverage is likely an underestimation of the actual number of articles reporting on the operation, as it focuses on the online dissemination of a few Overload stories.

It is worth mentioning that most of the fact-checking articles we reviewed focused solely on debunking individual false stories or videos, without offering broader context about the FIMI campaign. Many did not reference the operation by name, either as Overload or Matryoshka, despite both codenames being commonly used in the research community. In total, only 73 out of 180 articles in our sample provided any contextualisation, framing the effort as part of a Kremlin-aligned operation and explicitly naming one of its known codenames.

In our opinion, contextualising of FIMI operations, either in media references or in fact checking materials, is crucial as it demonstrates that individual false stories are part of a larger, coordinated disinformation campaign, rather than isolated incidents. Without this broader framing, efforts to debunk misinformation turn into a "whack-a-mole" game, addressing each false claim separately without revealing the overall strategy and intent of the operation. Providing context also helps audiences recognise patterns and tactics, which improves media literacy and makes it easier to identify future disinformation.

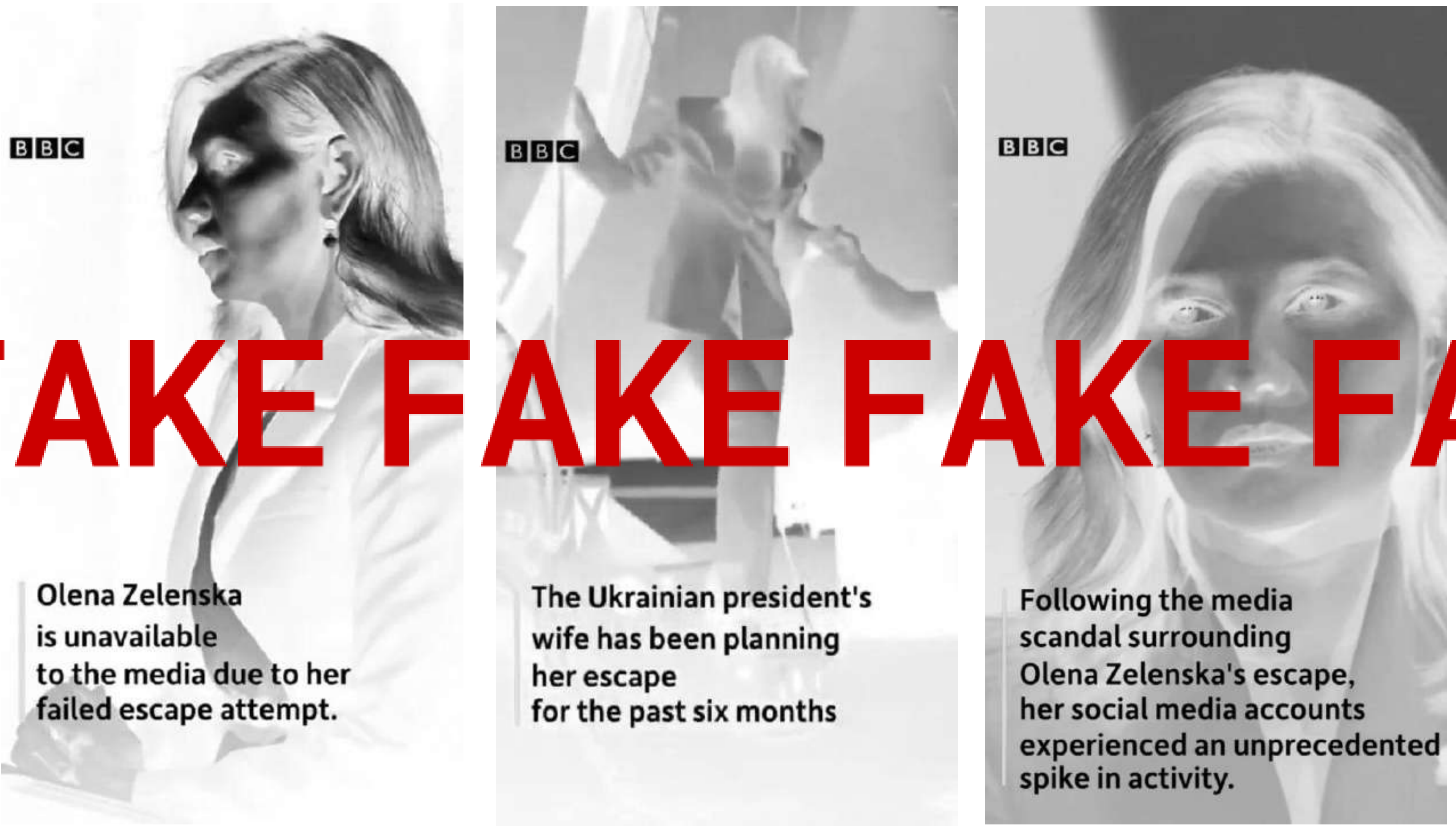
The English-language version of the Riga-based investigative website *The Insider* is the most active accidental amplifier of Overload content, promptly reporting on each shift in the operation's tactics with over 25 articles since September 2024. These articles often refer to findings by the online activist community antibot4navalny, which is presented as the main source of their reporting. While these efforts help reveal the operation's complexity and give contextual information about the campaign, they also unintentionally amplify the disinformation to wider, primarily international audiences and draw the focus of researchers and fact-checkers toward the operation. We recommend that such outlets focus on exposing the broader operation and providing context to avoid further spreading the false narratives.

The two case studies below focus on the critical role of amplifiers such as influential social media accounts, fact-checkers, media outlets, or public figures, to either unintentionally or quite deliberately "promote" the operation to wider audiences. These examples were selected to illustrate how heavily the operation depends on amplifiers to escape the limited outreach of its initial network of accounts seeding the content on X and Bluesky, and gain wider visibility including coverage at international media.

10.1. Case Studies

10.1.1. Fake BBC Video: First Lady Zelenska Attempts to Flee Ukraine

This case study highlights the complex dynamics between fact-checking efforts and the visibility of misinformation: by debunking a false claim, the fact-checking community is often contributing to its wider outreach. What began with a single social media post by a pro-Kremlin account rapidly escalated into a global narrative spanning across countries and even continents, reaching international outlets. The case study also exemplifies the vital role of the "amplifier accounts", influential X accounts that help the content gain organic virality.



Olena Zelenska is unavailable to the media due to her failed escape attempt.

The Ukrainian president's wife has been planning her escape for the past six months

Following the media scandal surrounding Olena Zelenska's escape, her social media accounts experienced an unprecedented spike in activity.

How it started

A video branded with the BBC logo claims that First Lady Olena Zelenska had attempted to flee Ukraine. It was first seeded on Telegram on **April 3** and swiftly propelled on X. Interestingly, the first known instance of the appearance of the video on X occurred not through a typical "seeder" account but was directly posted by the verified Kremlin-aligned influencer account @peacemaket71 (41,000 followers), an active amplifier of Overload content. @peacemaket71 posted[24] the video on **April 4**. Over the next few days, the original post garnered over 410,000 views, a record-high visibility for the account. This surge was primarily driven by legitimate accounts retweeting the post in an attempt to debunk the story.

The first response

On **April 7**, Ukrainian authorities first responded to the news. The X account of the ***Center for Countering Disinformation (CCD)*** posted[25] a rebuttal on X at 11:21 AM, uploading the fake video in the post. The post received 60,000 views. Shortly after, at 12:13 PM, the X account of the Ukrainian ***United24Media*** posted[26] another debunk which garnered 12,500 views. These two accounts were among the first to publicly discredit the false claims, helping to establish an official counter-narrative, but also setting the stage for wider fact-checking efforts.

[24] Peacemaket71 (@peacemaket71), tweet, posted April 4, 2025, 5:40 p.m. CET, https://x.com/peacemaket71/status/1908182784755236923, archived at https://archive.is/vqIVM.

[25] Center for Countering Disinformation (@CforCD), tweet, posted April 7, 2025, 10:21 a.m. CET, https://x.com/CforCD/status/1909159575053271127, archived at https://archive.is/Rer4S.

[26] United24media (@United24media), tweet, posted April 7, 2025, 11:13 a.m. CET, https://x.com/United24media/status/1909172677647933866, archived at https://archive.is/Mh6CF

The story reaches international fact-checkers.

On **April 8,** the story was already debunked by the international fact-checking community, including U.S.-based ***LeadStories***[27], the Spanish fact-checkers ***Maldita***[28] and ***Newtral***[29], the Irish ***Logically Facts***[30]. Ukraine's Strategic Communications Centre (***SPRAVDI***) also posted[31] a debunk on X. ***BBC journalist*** Shayan Sardarizadeh retweeted[32] the original post by the pro-Kremlin account @peacemaket71 to debunk the story. These reposts helped boost the visibility of the original post with more than 70,000 views.

And it travels further…

Once accelerated, the story travelled further: between **10 and 16 April**, another wave of fact-checkers and international news outlets reported that Olena Zelenska attempted to flee the country. At least 14 outlets published articles and debunks. On **April 10**, fact-checks appeared from ***20minutes***[33] (France), ***TheJournal.ie***[34] (Ireland), ***France24***[35] (France), and ***RTVE***[36] (Spain).

[27] Lead Stories, "Fact Check: BBC Did Not Produce Report About Ukrainian First Lady's Failed Escape Attempt", April 8, 2025, https://leadstories.com/hoax-alert/2025/04/fact-check-bbc-did-not-produce-report-about-ukrainian-first-ladys-failed-escapted-attempt.html.

[28] Maldita.es, "BBC video on Olena Zelenska's escape from Ukraine", April 8, 2025, https://maldita.es/malditobulo/20250409/bbc-video-olena-zelenska-huida-ucrania/

[29] Newtral.es, "Olena Zelenska fuga: BBC report analysis", April 8, 2024, https://www.newtral.es/olena-zelenska-fuga-bbc/20250408/.

[30] Logically Facts, "BBC video about Olena Zelenska's failed attempt to flee abroad is fake", April 8, 2025, https://www.logicallyfacts.com/en/fact-check/bbc-video-about-olena-zelenskas-failed-attempt-to-flee-abroad-is-fake.

[31] SPRAVDI — Stratcom Centre (@StratcomCentre), tweet, posted April 8, 2025, 10:37 p.m. CET, https://x.com/StratcomCentre/status/1909707174881947957.

[32] Shayan Sardarizadeh (@Shayan86), tweet, posted April 8, 2025, 1:05 p.m. CET, https://x.com/Shayan86/status/1909563282408546590.

[33] 20 Minutes, "Épouse de Volodymyr Zelensky tente de fuir l'Ukraine", April 10, 2025, https://www.20minutes.fr/societe/4148045-20250410-epouse-volodymyr-zelensky-tente-fuir-ukraine.

[34] TheJournal.ie, "Fake video claims Zelensky's wife tried to flee Ukraine", April 10, 2025, https://www.thejournal.ie/fake-video-zelensky-wife-flee-ukraine-6674210-Apr2025.

[35] France 24, "Olena Zelenska a-t-elle tenté de fuir l'Ukraine ? Non, il s'agit d'une intox", April 10, 2025, https://www.france24.com/fr/%C3%A9missions/info-ou-intox/20250410-olena-zelenska-a-t-elle-tent%C3%A9-de-fuir-l-ukraine-non-il-s-agit-d-une-intox.

[36] RTVE, "Falso, no es un vídeo de la BBC sobre la huida de Olena Zelenska", April 10, 2025, https://www.rtve.es/noticias/20250410/falso-no-video-bbc-sobre-huida-olena-zelenska/16535589.shtml.

Euronews[37] joined on the following day, **April 11**, including in multiple language editions in French[38], German[39], and Portuguese[40]. The fact checking organisation ***FullFact*** (UK) also published[41] a debunk. On **April 12**, the Italian[42] edition of *Euronews* added to the coverage. Fact-checkers ***Mimikama***[43] (Austria) and ***Info Veritas***[44] (Spain) also debunked the story.

[37] Euronews, "Disinformation Operation Falsely Claims Olena Zelenska Attempted to Flee Ukraine", April 11, 2025, https://www.euronews.com/video/2025/04/11/disinformation-operation-falsely-claims-olena-zelenska-attempted-to-flee-ukraine.

[38] Euronews (France), "Vérification des faits : Olena Zelenska a-t-elle vraiment tenté de fuir l'Ukraine ?" April 11, 2025, https://fr.euronews.com/video/2025/04/11/verification-des-faits-olena-zelenska-a-t-elle-vraiment-tente-de-fuir-lukraine.

[39] Euronews (Germany), "Desinformationskampagne: Gezielte Falschmeldungen über Olena Selenska verbreitet", April 11, 2025, https://de.euronews.com/my-europe/2025/04/11/desinformationskampagne-gezielte-falschmeldungen-uber-olena-zelenska-verbreitet.

[40] Euronews (Portugal), "Operação de desinformação afirma falsamente que Olena Zelenska tentou fugir da Ucrânia", April 11, 2025, https://pt.euronews.com/my-europe/2025/04/11/operacao-de-desinformacao-afirma-falsamente-que-olena-zelenska-tentou-fugir-da-ucrania.

[41] Full Fact, "Fake 'BBC report' claims Olena Zelenska tried to flee Ukraine", April 11, 2025, https://fullfact.org/online/fake-bbc-report-olena-zelenska.

[42] Euronews (Italy), "Fact checking: Olena Zelenska ha tentato di fuggire dall'Ucraina?", April 12, 2025, https://it.euronews.com/my-europe/2025/04/12/fact-checking-olena-zelenska-ha-tentato-di-fuggire-dallucraina.

[43] Mimikama, "Olena Zelenska auf der Flucht? BBC-Bericht ist ein Fake", April 14, 2025, https://www.mimikama.org/olena-zelenska-auf-der-flucht-bbc-bericht-fake.

[44] Info Veritas, "Desinformación: BBC no noticia fuga de Olena Zelenska", April 15, 2025, https://info-veritas.com/desinformacion-bbc-no-noticia-fuga-olena-zelenska.

To mainstream media…

On **April 15,** the story reached ***Reuters***[45]. Belgian media outlets ***7sur7.be***[46] and ***HLN***[47] also reported on April 16.

And all the way to Australia…

AAP.com[48] (Australia) published a fact-check on **April 21**.

…then back to Europe.

The Italian ***FACTA NEWS*** joined[49] with a debunk on **April 24**.

20 out of the 22 fact checks we collected made no mention of "Operation Overload" or "Matryoshka," and offered no contextual background beyond simply debunking the claim and referencing either of the tweets by the BBC or Ukraine's CCD to state that no such video had been published. Meanwhile, the campaign targeting Olena Zelenska continued, with new videos pushing slightly altered versions of the same story and branded with the logos of other legitimate media outlets. We refer to this tactic as dynamic narrative reframing and *brigading around* a narrative.

[45] Reuters, “Fact Check: BBC-branded video of Ukraine’s First Lady seeking asylum is fake, report says”, April 15, 2025, https://www.reuters.com/fact-check/bbc-branded-video-ukraines-first-lady-seeking-asylum-is-fake-report-2025-04-15.

[46] 7sur7, "Olena Zelenska en fuite : Moscou diffuse massivement de fausses informations sur la Première dame ukrainienne", April 15, 2025, https://www.7sur7.be/monde/olena-zelenska-en-fuite-moscou-diffuse-massivement-de-fausses-informations-sur-la-premiere-dame-ukrainienne~a6d9aff7.

[47] HLN, “Olena Zelenska op de vlucht: Moskou verspreidt explosief nepnieuws over Oekraïense first lady”, April 15, 2025, https://www.hln.be/buitenland/olena-zelenska-op-de-vlucht-moskou-verspreidt-explosief-nepnieuws-over-oekraiense-first-lady~a6d9aff7.

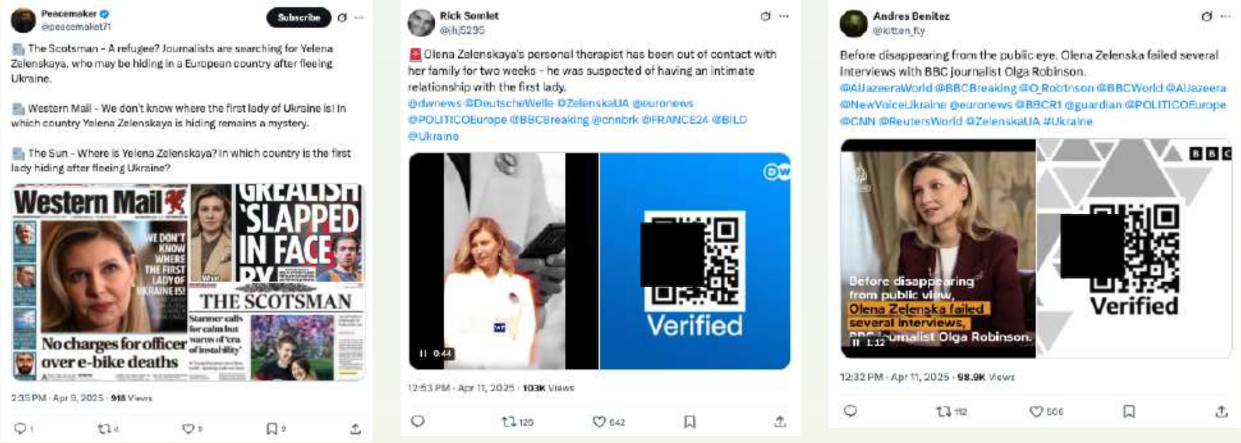
[48] AAP FactCheck, “Russian fake news content targeting Ukraine president’s wife spreads online”, April 21, 2025, https://www.aap.com.au/factcheck/russian-fake-news-content-targeting-ukraine-presidents-wife-spreads-online/.

[49] Facta, "La BBC non ha dato la (falsa) notizia che Olena Zelenska avrebbe tentato di fuggire dall’Ucraina", April 24, 2025, https://www.facta.news/antibufale/bbc-olena-zelenska-fuga-ucraina.

The story continues… brigading around the narrative (9 - 11 April)

At the time that the initial story of the First Lady was going viral, boosted by the global fact checking community, Operation Overload was busy producing versions of the story to bolster its credibility, a tactic we call "brigading around a narrative", which involves flooding the information space with variations of the same false story to reinforce the narrative.

Within just a few days, the fake story of Olena Zelenska's escape was bolstered by several fake videos and other types of fake content: on **April 9**, the same amplifier account @peacemaket71 posted about the First Lady's disappearance, this time using fake newspaper covers[50] of the U.K. newspapers The Western Mail and The Scotsman. On **April 11**, a "seeder" account posted another video[51], this time branded with the logo of Deutsche Welle and claiming that Zelenska may be having an affair, which would explain her disappearance. A third video was seeded[52] by another Overload account on the same day, **April 11**, this time branded with the logo of Al Jazeera, to peddle the conspiracy that the First Lady had given an interview to a BBC journalist before her alleged disappearance.



Peacemaker
@peacemaket71

The Scotsman - A refugee? Journalists are searching for Yelena Zelenskaya, who may be hiding in a European country after fleeing Ukraine.

Western Mail - We don't know where the first lady of Ukraine is! In which country Yelena Zelenskaya is hiding remains a mystery.

The Sun - Where is Yelena Zelenskaya? In which country is the first lady hiding after fleeing Ukraine?

2:35 PM · Apr 9, 2025 · 918 Views

Rick Somlet
@jhj5295

Olena Zelenskaya's personal therapist has been out of contact with her family for two weeks - he was suspected of having an intimate relationship with the first lady.
@dwnews @DeutscheWelle @ZelenskaUA @euronews @POLITICOEurope @BBCBreaking @cnnbrk @FRANCE24 @BILD @Ukraine

[redacted]

12:53 PM · Apr 11, 2025 · 103K Views

Andres Benitez
@kitten_fly

Before disappearing from the public eye, Olena Zelenska failed several interviews with BBC journalist Olga Robinson.
@AlJazeeraWorld @BBCBreaking @O_Robinson @BBCWorld @AlJazeera @NewVoiceUkraine @euronews @BBCR1 @guardian @POLITICOEurope @CNN @ReutersWorld @ZelenskaUA #Ukraine

[redacted]

12:32 PM · Apr 11, 2025 · 98.9K Views

Subscribe
Western Mail
WE DON'T KNOW WHERE THE FIRST LADY OF UKRAINE IS!
No charges for officer over e-bike deaths
GREALISH 'SLAPPED IN FACE BY
THE SCOTSMAN
Starmer calls for calm but warns of 'era of instability'
1 4 8 2
0:44
DW
Verified
126 642
Before disappearing from public view, Olena Zelenska failed several interviews, BBC journalist Olga Robinson.
1:12
BBC
Verified
112 506

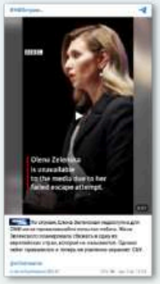
Fig 64: *Brigading around a narrative is a very common tactic used by the Overload operatives to bolster the credibility of false stories. In the case of Zelenska's alleged escape, the initial story in the fake BBC video was followed by a post by the same account featuring two fake newspaper covers. On April 11, two "seeder" accounts joined with new videos spinning the same story. (Source: X 1,2,3)*

[50] Peacemaker, (@peacemaket71) tweet, posted April 9, 2025, 1:35 p.m. CET https://x.com/peacemaket71/status/1909933130523255118, archived at https://archive.is/qingc.

[51] Rick Somlet, (@jhj5295), tweet, posted, April 11, 2025, 11:53 a.m. CET https://x.com/jhj5295/status/1910632186039894283, archived at https://archive.is/kSkDn.

[52] Andres Benitez, (@kitten_fly), tweet, posted April 11, 2025, 11:32 a.m. CET, https://x.com/kitten_fly/status/1910626983475630481, archived at https://archive.is/yjaOi.

April 3

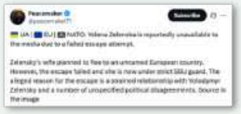

Olena Zelenska is unavailable to the media due to her failed escape attempt.

[illegible]

The claim is seeded accross multiple Telegram channels.

Est. 15.000 views

April 4


Peacemaker @peacemaker71 Subscribe

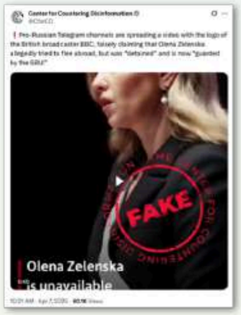
🇺🇦 UA | 🇪🇺 EU | NATO: Yelena Zelenska is reportedly unavailable to the media due to a failed escape attempt.

Zelensky's wife planned to flee to an unnamed European country. However, the escape failed and she is now under strict SBU guard. The alleged reason for the escape is a strained relationship with Volodymyr Zelensky and a number of unspecified political disagreements. Source in the image

A pro-Krelim account on X picks the claim and posts it.

+ 400.000 views

April 7


Center for Countering Disinformation @CforCD

❗ Pro-Russian Telegram channels are spreading a video with the logo of the British broadcaster BBC, falsely claiming that Olena Zelenska allegedly tried to flee abroad, but was "detained" and is now "guarded by the SBU"

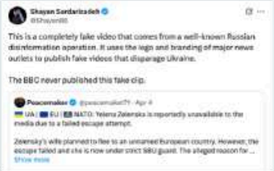
10:21 AM · Apr 7, [illegible] · [illegible] Views

UNITED24 MEDIA

First denonciation as fake by the CCD.

+ 60.000 views

April 8


Shayan Sardarizadeh @Shayan86

This is a completely fake video that comes from a well-known Russian disinformation operation. It uses the logo and branding of major news outlets to publish fake videos that disparage Ukraine.

The BBC never published this fake clip.

Peacemaker @peacemaker71 · Apr 4

🇺🇦 UA | 🇪🇺 EU | NATO: Yelena Zelenska is reportedly unavailable to the media due to a failed escape attempt.

Zelensky's wife planned to flee to an unnamed European country. However, the escape failed and she is now under strict SBU guard. The alleged reason for ...
Show more

BBC senior journalist at BBC Verify Shayan Sardarizadeh refutes the video.

+ 70.000 views

Newtral
Logically.
MALDITA.ES
LEAD STORIES
Center for Strategic Communication and Information Security

April 10

rtve
FRANCE 24
aap
REUTERS
20 minutes
The Journal
FULL FACT
HLN Het Laatste Nieuws
MIMIKAMA
7sur7

April 24

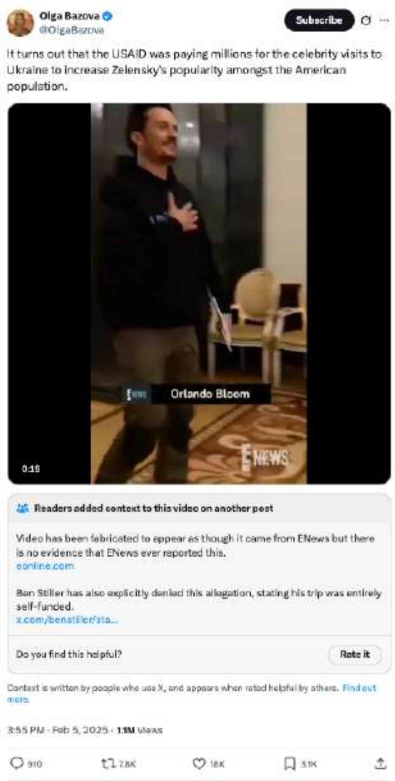
FACT.

Fig 65: blablabla

10.1.2. Fake E!News Video: USAID funds Ukraine Visit of Hollywood actor Ben Stiller

The second case study demonstrates how specific narratives, deliberately crafted as part of FIMI operations like Overload, can achieve global reach when strategically timed and aligned with themes that resonate with target audiences. The story was boosted by a network of high-reach amplifiers, many of whom were already known for sharing Kremlin-aligned or U.S. conservative political content. It gained momentum because it was posted at the right moment, tapping into pre-existing skepticism toward USAID within certain U.S. political communities.

In February 2025, Overload circulated a video falsely branded with the logo of the U.S. entertainment news outlet E! News. The video displayed the typical hallmarks of the operation, using footage of Hollywood actor Ben Stiller to claim that he had visited Ukraine at the expense of the U.S. Agency for International Development (USAID). This video was part of a broader, coordinated disinformation campaign targeting USAID, which began in early 2025 and included numerous content pieces designed to discredit the agency and spread misleading narratives about its activities.



Olga Bazova
@OlgaBazova

It turns out that the USAID was paying millions for the celebrity visits to Ukraine to increase Zelensky's popularity amongst the American population.

Readers added context to this video on another post

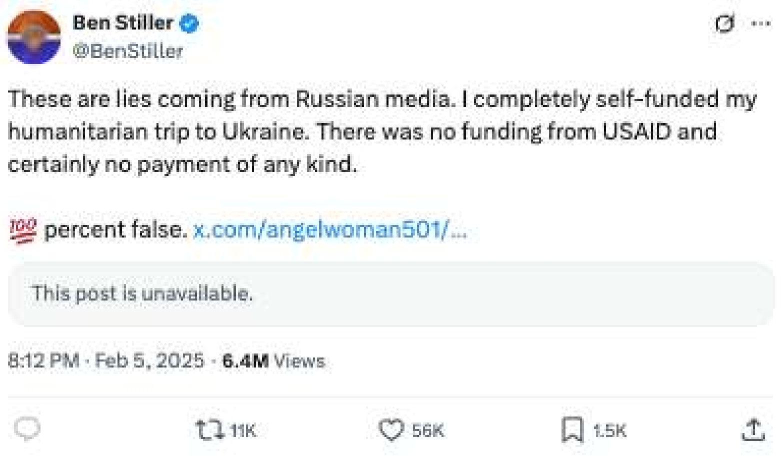
Video has been fabricated to appear as though it came from ENews but there is no evidence that ENews ever reported this.
eonline.com

Ben Stiller has also explicitly denied this allegation, stating his trip was entirely self-funded.
x.com/benstiller/sta...

Do you find this helpful? Rate it

Context is written by people who use X, and appears when rated helpful by others. Find out more.

3:55 PM · Feb 5, 2025 · 1.1M Views



Ben Stiller
@BenStiller

These are lies coming from Russian media. I completely self-funded my humanitarian trip to Ukraine. There was no funding from USAID and certainly no payment of any kind.

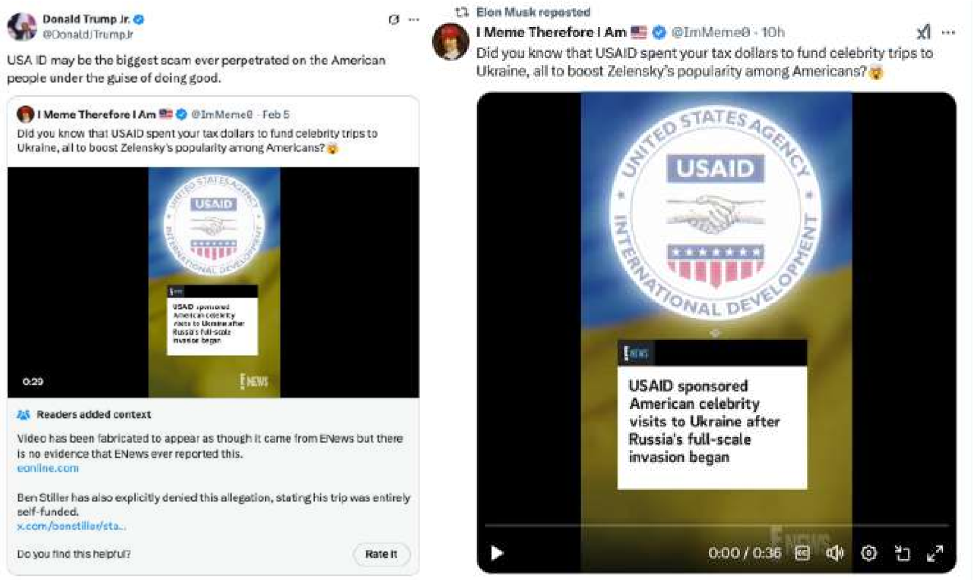
💯 percent false. x.com/angelwoman501/...

This post is unavailable.

8:12 PM · Feb 5, 2025 · 6.4M Views

Fig 66: *(Left) Kremlin-aligned influencer account posts the video. The story gains momentum, eventually breaking out of its original bubble and gaining traction within U.S. conservative communities on X (Source: X 1). The story breaks out to U.S. accounts, eventually reaching Ben Stiller himself, who refutes the allegations. His tweet further amplifies the original post, reaching 6.4 million views. (Source: X 2)*

The video was picked up by several pro-Kremlin influencers on X, including the verified account @OlgaBazova (88,000 followers), who has previously amplified Overload content. Her post[53] reached 1.1 million views and helped the story break out to wider audiences. The story resonated with U.S. audiences and quickly reached out to the MAGA and conservative online communities. On the same day, the verified account of Johnny Midnight @its_The_Dr, an influential MAGA account known for sharing Kremlin-aligned content, also posted the video. From there it travelled further, eventually reaching @ImMeme0, another verified influencer within sharing conservative and meme-driven political discourse (750,000 followers). This specific post[54] eventually received 4.2 million views partly due to the fact that it was retweeted by Elon Musk. On February 6, another influential account in the U.S. conservative ecosystem, Donald Trump Jr., amplified the video, reaching over 450,000 views[55].



Donald Trump Jr.
@DonaldJTrumpJr

USA ID may be the biggest scam ever perpetrated on the American people under the guise of doing good.

I Meme Therefore I Am 🇺🇸 @ImMeme0 · Feb 5

Did you know that USAID spent your tax dollars to fund celebrity trips to Ukraine, all to boost Zelensky's popularity among Americans? 😱

USAID sponsored American celebrity visits to Ukraine after Russia's full-scale invasion began

Readers added context

Video has been fabricated to appear as though it came from ENews but there is no evidence that ENews ever reported this.
eonline.com

Ben Stiller has also explicitly denied this allegation, stating his trip was entirely self-funded.
x.com/benstiller/sta...

Do you find this helpful?

Rate it

Elon Musk reposted

I Meme Therefore I Am 🇺🇸 @ImMeme0 · 10h

Did you know that USAID spent your tax dollars to fund celebrity trips to Ukraine, all to boost Zelensky's popularity among Americans? 😱

USAID sponsored American celebrity visits to Ukraine after Russia's full-scale invasion began

Fig 67*: The X accounts of Elon Musk and Donald Trump Jr amplify the video, reposting the video by the verified account @ImMeme0, a prominent influencer known for sharing conservative political narratives. (Source: X 1)*

[53] Olga Bazova, (@OlgaBazovatweet), posted February 5, 2025, 2:55 p.m. CET, https://x.com/OlgaBazova/status/1887138083386098146, archived at https://archive.is/puUnF

[54] I Meme Therefore I Am, (@ImMeme0), tweet, posted February 5, 2025, 4:16 p.m. CET https://x.com/ImMeme0/status/1887158413597057107, archived at https://archive.is/sgDpc.

[55] Donald Trump Jr., (@DonaldJTrumpJr), tweet, posted February 5, 2025, 2:55 p.m. CET, https://x.com/DonaldJTrumpJr/status/1887265464310480912.

As a result of the massive amplification on X, particularly through high-profile accounts such as Elon Musk and Donald Trump Jr., in February 2025 the story broke into mainstream discourse and continued circulating until May. Unsurprisingly, it triggered widespread media attention, with over **150 articles** published by news outlets from all over the world in response. Rather than containing the narrative, this wave of coverage gave the story further momentum, fueling visibility and lending additional traction to the broader Overload disinformation operation.

11. Recommendations

- We urge X to take immediate action to address Operation Overload, as this coordinated campaign spreading election interference, identity-based disinformation, and content inciting violence falls directly under X's risk mitigation obligations as a VLOP under the EU's Digital Services Act. Despite these legal requirements, our findings show that X has failed to mitigate risks stemming from clearly illegal posts, many of which remain accessible months after publication, indicating systemic lapses in enforcement. This poses clear issues in regards to Article 34 and 35 of the DSA. X must urgently remove this content, strengthen moderation processes, and transparently report on corrective actions to achieve not only compliance with the DSA but also enforce their own policy on civic integrity[56].

- As demonstrated, impersonation is a commonly used tactic by the operation. However, judging from publicly available data, few impersonated brand owners and individuals seem to exert their rights and pursue either legal action or at least report illegal content to platforms. Systematic action from impersonated entities would accelerate content moderation and diminish the efficiency of this tactic. Besides national laws provisions, the EU's Digital Services Act (DSA) mandates notice and action mechanisms in its Article 16 to allow any user to signal illegal content to platforms. A category of notices labelled "impersonation" could be added in the platform's reporting tools.

- Operation Overload's main tactic is to lure fact-checkers into debunking falsehoods, hence amplifying their narratives. Unfortunately, some publishers fall regularly in the trap and report about pieces of content which were not necessarily seen *en masse* by the public. Once again, as we did in our previous reports, we urge media organisations and fact-checkers to exert caution when stumbling upon sensationalist fakes, particularly when being pointed at Russian language Telegram channels listed in the annexes.

- Given the extensive press coverage by both media organisations and fact-checkers on individual pieces of false content promoted by Operation Overload or Matryoshka, we strongly urge authors to refrain from publishing such articles, especially swiftly after new assets appeared. Doing so plays into the hands of propagandists by further amplifying falsehoods. We strongly recommend that, where such content is discussed, readers are provided with clear context about Operation Overload, explicitly framing these false narratives as part of a broader campaign to manipulate Western media for political ends.

[56] https://help.x.com/en/rules-and-policies/election-integrity-policy

12. Annexes

12.1. 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 CheckFirst's website[57].

The external reviewers for this document are :

- Independent Researcher in Foreign Influence.
- Research Associate at DFRLab.

This document has scored 81.94 out of 100 after review.

12.2. Archiving Policy

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

[57] CheckFirst - Operation investigation assesment https://docs.google.com/spreadsheets/d/1ka2rcMAmiUgDKIiTxXNS5cB0poax8C-GCC2GI1_sRmY/edit#gid=0.

12.3. RADAR[58] Frameworks Tags

Digital Service Act Infringement Analysis

Assessment Date: 06.2025
RADAR Version: 1.7

Identified Potential Infringements:

Platform(s): **X, TikTok**

Category: **Illegal Content and Goods**

- **icg_06**: Intellectual Property Infringement
    - Observed: Failure to tackle the repeated illegal use of trademarked logos of organisations.
    - Evidence: See main report

Category: **Cyber Violence**

- **cv_05**: Technology-Facilitated Gender-Based Violence
    - Observed: Failure to tackle content demeaning and violent statements about women and girls
    - Evidence: See main report

Category: **Disinformation and Manipulated Media**

- **dmm_01**: Disinformation Campaigns
    - Observed: Inauthentic use of the service, including the creation of fake accounts, use of bots, or deceptive use of service, and other automated or partially automated behaviours which may lead to rapid and widespread dissemination of illegal content or incompatible with platform T&C and that contributes to disinformation campaigns (Recital 84)
    - Evidence: See main report

- **dmm_02**: AI-Generated & Synthetic Media
    - Observed: Videos where a person's face or voice appears altered (e.g. lip-sync mismatch, unnatural facial movements) indicating a deepfake.
    - Evidence: See main report

[58] RADAR - Regulatory Assessment for Digital Service Act Risks, https://radar.checkfirst.network

- **dmm_03**: Election Disinformation
    - Observed: Failure to curb content disseminating false claims about an election candidate or public figure (For e.g. fabricated scandals or fake quotes) that have been debunked by credible sources but continue circulating.
    - Evidence: See main report

Total Potential Infringements Identified: 6 DSA Articles
Potentially Violated: 14, 34, 35

12.4. Annex 1: List of Organisations Impersonated in Overload Videos on X and Bluesky

Name	Entity type	Country	Website
1+1 Ukraina	Media	Ukraine	media.1plus1.ua
ABC news	Media	United States	abcnews.go.com
Agence France-Presse (AFP)	Media	France	afp.com
Aix Marseille University	University/College	France	univ-amu.fr
Al Jazeera	Media	Qatar	aljazeera.com
American Psychological Association (APA)	Other	United States	apa.org
Arts et Métiers ParisTech - ENSAM	University/College	France	artsetmetiers.fr
Associated Press (AP)	Media	United States	apnews.com
AT&T	Other	United States	att.com
BBC	Media	United Kingdom	bbc.com
Bellingcat	Other	United Kingdom	bellingcat.com
BFMTV	Media	France	bfmtv.com
Bild	Media	Germany	bild.de
Bloomberg	Media	United States	bloomberg.com
BundesNachrichtendienst	Government	Germany	bnd.bund.de
Business Insider	Media	United States	businessinsider.com
CANAL+	Media	France	canalplus.com
Car and Driver	Media	United States	caranddriver.com
Catholic Institute De Toulouse (ICT)	University/College	France	ict-toulouse.fr
CBS Colorado	Media	United States	cbsnews.com/colorado
CBS News	Media	United States	cbsnews.com
CBS NEWS Los Angeles	Media	United States	cbsnews.com/losangeles
CENTER FOR COUNTERING DISINFORMATION	Government	Ukraine	cpd.gov.ua
CFDT Eurodisney	Other	France	cfdt-disney.fr
CFE CGC Agro	Other	France	cfecgcagro.org
CNews	Media	France	cnews.fr
CNN	Media	United States	cnn.com
Communications Workers Union (CWU)	Other	United Kingdom	cwu.org
Côte d'Azur University	University/College	France	univ-cotedazur.eu

CY Cergy Paris University	University/College	France	cyu.fr
Deadline	Media	United States	deadline.com
Defense Advanced Research Projects Agency (DARPA)	Government	United States	darpa.mil
Delfi	Media	Lithuania	delfi.lt
Denver7 ABC	Media	United States	denver7.com
Der Spiegel	Media	Germany	spiegel.de
Deutsche Welle (DW)	Media	Germany	dw.com
Directorate-General for External Security (DGSE)	Government	France	dgse.gouv.fr
DOXA Team	Media	Russia	doxa.team
E!News	Media	United States	eonline.com
École Nationale Supérieure d'Architecture de Paris-Belleville	University/College	France	paris-belleville.archi.fr
École Normale Supérieure (ENS)	University/College	France	ens.psl.eu
Edinburgh Napier University	University/College	United Kingdom	napier.ac.uk
ENS Paris-Saclay	University/College	France	ens-paris-saclay.fr
Euronews	Media	Belgium	euronews.com
European Content Creator Network (ENTR)	Media	Germany	entr.net
FBI	Government	United States	fbi.gov
Financial Times (FT)	Media	United Kingdom	ft.com
Forbes	Media	United States	forbes.com
FOX news	Media	United States	foxnews.com
France 5	Media	France	france.tv
France Inter	Media	France	radiofrance.fr
France24	Media	France	france24.com
FranceInfo	Media	France	franceinfo.fr
Gazeta Polska	Media	Poland	gazetapolska.pl
Gendarmerie Nationale	Government	France	gendarmerie.interieur.gouv.fr
Greenpeace	Other	The Netherlands	greenpeace.org
Grenoble École de Management	University/College	France	grenoble-em.com
Gustave Eiffel University	University/College	France	univ-gustave-eiffel.fr
Hamburger MorgenPost	Media	Germany	mopo.de
Harper and Keele Veterinary School	University/College	United Kingdom	harperkeelevetschool.ac.uk
Harvard Law School	University/College	United States	hls.harvard.edu
Have I Got News for You US	Media	United States	edition.cnn.com/audio/podcasts/have-i-got-news-for-you

HEC Paris	University/College	France	hec.edu
Human Right Watch (HRW)	Other	United States	hrw.org
Il Fatto Quotidiano	Media	Italy	ilfattoquotidiano.it
Imperial College London -- Grantham Institute Imperial	University/College	United Kingdom	imperial.ac.uk/grantham
IndiaToday	Media	India	indiatoday.in
Infoworld	Media	United States	infoworld.com
Institut Polytechnique de Paris	University/College	France	ip-paris.fr
Institute for Intelligence and Special Operations (Mossad)	Government	Israel	mossad.gov.il
Institute for the Study of War (ISW)	Other	United States	understandingwar.org
IRT Saint Exupéry	Other	France	irt-saintexupery.com
JSTOR	Other	United States	http://jstor.org
King's College London	University/College	United Kingdom	kcl.ac.uk
Kyiv24	Media	Ukraine	kyiv24.com
L'Equipe	Media	France	lequipe.fr
La CGT	Other	France	cgt.fr
La Croix	Media	France	la-croix.com
La Depeche	Media	France	ladepeche.fr
La Voix du Nord	Media	France	lavoixdunord.fr
Le Figaro	Media	France	lefigaro.fr
Le Point	Media	France	lepoint.fr
Liberation	Media	France	liberation.fr
MacEwan University	University/College	Canada	macewan.ca
Manchester Metropolitan University	University/College	United Kingdom	mmu.ac.uk
MAXIM	Media	United States	maxim.com
McMaster University	University/College	Canada	mcmaster.ca
Microsoft	Other	United States	microsoft.com
MT180	University/College	France	mt180.fr
Museum of Modern art	Other	United States	moma.org
NBC news	Media	United States	nbcnews.com
Newsweek	Media	United States	newsweek.com
NME	Media	United Kingdom	nme.com
Organization for Security and Co-operation in Europe (OSCE)	Other	Austria	osce.org
People	Media	United States	people.com
POLITICO	Media	United States	politico.com

PSL Research University	University/College	France	psl.eu
Queen Mary University of London	University/College	United Kingdom	qmul.ac.uk
Radio France Internationale (RFI)	Media	France	rfi.fr
Radio Free Europe/Radio Liberty (RFE)	Media	United States	rferl.org
Radio RMF FM	Media	Poland	rmf.fm
RadioLiberty	Media	United States	rferl.org
Rennes School of Business Alumni	University/College	France	rennes-sb-alumni.com
Reporters Without Borders (RSF)	Other	France	rsf.org
Reuters	Media	Canada	reuters.com
Saturday Night Live	Media	United States	nbc.com/saturday-night-live
Sky News	Media	United Kingdom	news.sky.com
Social Blade	Other	United States	socialblade.com
Sorbonne Paris Nord University	University/College	France	univ-spn.fr
Stanford University	University/College	United States	stanford.edu
Süddeutsche Zeitung (SZ)	Media	Germany	sueddeutsche.de
T-Online	Media	Germany	t-online.de
Tagesspiegel	Media	Germany	tagesspiegel.de
Teesside University	University/College	United Kingdom	tees.ac.uk
TeleRadio-Moldova	Media	Moldova	trm.md
TF1	Media	France	tf1.fr
The Daily Mail	Media	United Kingdom	dailymail.co.uk
The Daily Mirror	Media	United Kingdom	mirror.co.uk
The Daily Record	Media	United Kingdom	dailyrecord.co.uk
The George Washington University	University/College	United States	gwu.edu
The Guardian	Media	United Kingdom	theguardian.com
The Hollywood Reporter	Media	United States	hollywoodreporter.com
The Institute of Education	University/College	Ireland	instituteofeducation.ie
The Kyiv Independent	Media	Ukraine	kyivindependent.com
The Late Show with Stephen Colbert	Media	United States	cbs.com/shows/the-late-show-with-stephen-colbert
The National Post	Media	Canada	nationalpost.com
The New York Post	Media	United States	nypost.com
The New York Times (NYT)	Media	United States	nytimes.com
The Telegraph	Media	United Kingdom	telegraph.co.uk
The Times of Israel	Media	Israel	timesofisrael.com

The Tonight Show with Jimmy Fallon	Media	United States	nbc.com/the-tonight-show
The Washington Post	Media	United States	washingtonpost.com
TMZ	Media	United States	tmz.com
Trent University	University/College	Canada	trentu.ca
TVP world	Media	Poland	tvpworld.com
UCL London's Global University	University/College	United Kingdom	ucl.ac.uk
UCLy - Lyon Catholic University	University/College	France	ucly.fr/en
UNESCO	Other	France	unesco.org
UNICEF	Other	United States	unicef.nl
United24 Media	Media	Ukraine	united24media.com
University Centrale Lille	University/College	France	centralelille.fr
University of Avignon	University/College	France	univ-avignon.fr
University of Bath	University/College	United Kingdom	bath.ac.uk
University of Cambridge	University/College	United Kingdom	cam.ac.uk
University of Corsica	University/College	France	universita.corsica
University of Detroit Mercy	University/College	United States	udmercy.edu
University of Guelph	University/College	Canada	uoguelph.ca
University of La Rochelle	University/College	France	univ-larochelle.fr
University of Le Havre	University/College	France	univ-lehavre.fr
University of Leicester	University/College	United Kingdom	le.ac.uk
University of Lethbridge	University/College	Canada	ulethbridge.ca
University of Lille	University/College	France	univ-lille.fr
University of London	University/College	United Kingdom	london.ac.uk
University of Lorraine	University/College	France	univ-lorraine.fr
University of Montpellier	University/College	France	umontpellier.fr
University of Montpellier	University/College	France	umontpellier.fr
University of Oxford	University/College	United Kingdom	ox.ac.uk
University of Perpignan - Domitian	University/College	France	univ-perp.fr
University of Picardy Jules Verne	University/College	France	u-picardie.fr
University of Plymouth	University/College	United Kingdom	plymouth.ac.uk
University of Poitiers	University/College	France	univ-poitiers.fr
University of Rennes	University/College	France	univ-rennes.fr
University of Rouen-Normandy	University/College	France	univ-rouen.fr
University of Suffolk	University/College	United Kingdom	uos.ac.uk
University of Tours	University/College	France	international.univ-tours.fr
University of Victoria	University/College	Canada	uvic.ca
University of Warwick	University/College	United Kingdom	warwick.ac.uk

University of West London	University/College	United Kingdom	uwl.ac.uk
University of Yale	University/College	United States	yale.edu
UNKNOWN (1)	Media	N/A	N/A
UNKNOWN (2)	Media	N/A	N/A
UNKNOWN (3)	Media	N/A	N/A
UNKNOWN (4)	Media	N/A	N/A
UNKNOWN (5)	Media	N/A	N/A
UNKNOWN (6)	Media	N/A	N/A
UNKNOWN (7)	Media	N/A	N/A
Us Weekly	Media	United States	usmagazine.com
USA Today	Media	United States	eu.usatoday.com
VIGINUM	Government	France	sgdsn.gouv.fr
Voice of America (VoA)	Media	United States	voanews.com
Wall Street Journal (WSJ)	Media	United States	wsj.com
Wilfrid Laurier University	University/College	Canada	wlu.ca
WIRED	Media	United States	wired.com
YahooNews	Media	United States	news.yahoo.com

12.5. Annex 2: List of Individuals Impersonated in Overload Videos on X and Bluesky

If you are on this list and you have questions or want to learn more, please feel free to get in touch.

Impersonated individual	Organisation	Role/Affiliation	Country
Ruslana Danilkina	Armed Forces of Ukraine (AFU)	Other	Ukraine
Robert Otto Valdez	Agency for Healthcare Research & Quality	Government	United States
Oleg Apostol	Ukrainian Air Assault Forces	Government	Ukraine
Ana Guerra-Moore	BBC News	Journalist	United Kingdom
Olga Robinson	BBC News	Journalist	United Kingdom
Shayan Sardarizadeh	BBC News	Journalist	United Kingdom
Eliott Higgins	Bellingcat	Other	United Kingdom
Adélaïde Boutrion	BFMTV	Journalist	France
David Gura	Bloomberg	Journalist	United States
Daria Gerasimchuk	Bring Kids Back UA (bringkidsback.org.ua)	Government	Ukraine
Armin Laschet	Member of the German Bundestag (CDU party)	Government	Germany
Adelaide Boutiron	CFJ Graduate School of Journalism	Journalist	France
Clay Jenkins (Attorney)	n/a	Other	United States
Louis Leeson	CNN	Other	United Kingdom
Roy Wood Jr	CNN	Journalist	United States
Gavin Williamson	Member of Parliament of the United Kingdom (Conservative Party)	Government	United Kingdom
Assia Nechache	CY Cergy Paris University	Academic	France
René Zavoral	czech.radio	Other	Czech Republic
Wil Corvey	Defense Advanced Research Projects Agency (DARPA)	Other	United States
Anne Milgram	Drug Enforcement Administration (DEA)	Government	United States
Cyrille Hanappe	École Nationale Supérieure d'Architecture de Paris-Belleville	Academic	France
Jenny Smith	Edinburgh Napier University	Academic	United Kingdom
Lyn Halley	Edinburgh Napier University	Other	United Kingdom
Tania Castro	ENSAE Paris (Polytechnic Institute of Paris)	Academic	France

Hugues de Suremain	European Prison Litigation Network (EPLN)	Academic	France
Claus Strunz	Euronews	Journalist	Germany
Michael McGrath	European Commission	Government	EU
Christopher A. Wray	FBI	Government	United States
Christian Lindner	Former Federal Minister of Finance of Germany (FDP party)	Government	Germany
Catalina Marchant De Abreu	France24	Journalist	France
Bertrand Delanoë	French Senate	Government	France
Edward Luce	FT	Journalist	United States
Damien Mouchel dit Leguerrier	FuelSea/Anodine (anodine.fr)	Academic, CEO	France
Niklas Hintermayer	German Council on Foreign Relations	Government	Germany
Nancy Blench-Locatelli	Grenoble School of Management	Academic	France
Romain Menini	Gustave Eiffel University	Academic	France
Lindsay Thomas	Harper & Keele Veterinary School	Academic	United Kingdom
Valérie Pécresse	HEC Paris Business School	Academic	France
Katherine Henderson	Hockey Canada (hockeycanada.ca)	Academic	Canada
Margaret Abraham	Hofstra University	Academic	United States
Jessica Newberry Le Vay	Imperial College London	Academic	United Kingdom
Samira El Gadir	TF1	Journalist	France
Benjamin Deporte	IRT Saint Exupéry	Academic	France
Herzi Halevi	Former Chief of the General Staff of Israel, Israel Defense Forces	Government	Israel
Bill Kristol	Institute for the Study of War (ISW)	Government	United States
Alan Read	Kings College London	Academic	United Kingdom
Bernard de Moucheron	Le Figaro	Journalist	France
Gaspard Bellot	Le Figaro	Journalist	France
Romain Courcier	Le Figaro	Journalist	France
Anne Kerloch	Le Point	Journalist	France
Boris Mabillard	Le Point	Journalist	France
Sergey Shestak	Le Point	Journalist	France
Michèle Alliot-Marie	Politician	Other	France
Thomas Maurer	École Centrale de Lille	Academic	France
Stéphane Courbit	LOV Group	Other	France
Kevin Judge	MacEwan University	Academic	Canada

Andy Dainty	Manchester Metropolitan University	Academic	United Kingdom
Bill Gates	Microsoft	Other	United States
Alan Sheinwald	Capital Markets Group, LLC	Other	United States
Anna Hutsol	n/a	Activist	Ukraine
Anton Mironiuk	n/a	Other	Ukraine
Ben Stiller	n/a	Actor	United States
Dusan Kosanovic	Fake person	Fake person	Fake person
Gérard Depardieu	n/a	Actor	France
Harel Horowitz	Fake person	Fake person	Fake person
Hélène Rollès	n/a	Actress	France
Mariya (Ukrainian refugee)	Fake person	Fake person	Fake person
Morgen Freeman	n/a	Actor	United States
Musa Ali Daoud (employee)	Fake person	Fake person	Fake person
Omar Ramirez (Mexican refugee)	Fake person	Fake person	Fake person
Pepillo Cepeda (Mexican refugee)	Fake person	Fake person	Fake person
Timothée Chalamet	n/a	Actor	France
Tommy Robinson	n/a	Other	United Kingdom
Ukrainian refugee (stolen identity)	Fake person	Fake person	Ukraine
Unidentified1	n/a	Other	N/A
Unidentified2	n/a	Other	N/A
Unidentified3	n/a	Other	N/A
Unidentified4	n/a	Other	N/A
Unidentified5	n/a	Other	N/A
Unidentified6	n/a	Other	N/A
Unidentified7	n/a	Other	N/A
Seeram Ramakrishna	National University of Singapore	Academic	Singapore
Jimmy Fallon	NBC News	Other	United States
Norman Candy	NEC Rep for Retired Members	Other	United Kingdom
Keily Blair	OnlyFans	CEO	United States
Armin Papperger	Rheinmetall AG	CEO	Germany
Unidentified8	Reporters Without Borders (RSF)	Journalist	France
Thibaut Bruttin	Reporters Without Borders (RSF)	Journalist	France
Gillis Keppel	Sciences Po	Academic	France
Doris Birkhofer	Siemens	President	France

Christophe Mouget	SNCF Réseau	President	France
Mathilde Lévêque	Sorbonne Paris North University	Academic	France
Yuriy Syrotyuk	Svoboda	Politician	Ukraine
Christopher Hayes	Teesside University	Academic	United Kingdom
Susan Gillspie	Texas Children's Hospital	Academic	United States
James Henson	Texas University	Academic	United States
Benjamin Svetkey	The Hollywood Reporter	Journalist	United States
Peter Hegarty	The Open University	Academic	United Kingdom
Laura Mathias	The University of Warwick	Alumna	United Kingdom
Daniel Pellizon	The Vatican	Other	Vatican City State
Stephen Stohn	Trent University	Academic	Canada
Michael Seibel	Twitch	Former CEO	United States
David Howell Petraeus	U.S. Army	Government	United States
Mark Alexandre Milley	U.S. Army	Government	United States
Charles Brown Junior	U.S. Department of Defense	Government	United States
Chesa Boudin (Attorney)	UC Berkeley School of Law	Academic	United States
Victor Yurchik	Ukrainian Army	Government	Ukraine
Yulia Svyrydenko	Ukrainian Government	Government	Ukraine
António Guterres	United Nations	Government	Portugal
Pam Bondi	United States Attorney General	Government	United States
Robert Kennedy Jr	United States Secretary of Health and Human Services	Government	United States
Francesca Simeoni	Université Catholique de Lyon	Academic	France
Grégory Woimbée	Université Catholique de Lyon	Academic	France
Sebastien Gayet	Universite d'Artois	Academic	France
Anna Aragao	Université de Havre Normandie	Academic	France
Eric Mielke	Université de Lille	Academic	France
Frédérique Aberlenc	Université de Montpellier	Academic	France
Isabelle Bourdon	Université de Montpellier	Academic	France
Alain Aspect	Université de Picardie Jules Verne	Academic	France
Christine Lombard	Université de Rennes	Academic	France
Clémentine Dollé	Université de Strasbourg	Academic	France
Bastien Cherault	Université de Tours	Academic	France
Colette Jourdan-Ionescu	Université du Québec à Trois-Rivières	Academic	Canada
Phil Taylor	University of Bath	Academic	United Kingdom
Deborah Prentice	University of Cambridge	Academic	United States

Dan Pitera	University of Detroit Mercy	Academic	United States
David Cassilo	University of Detroit Mercy	Academic	United States
Mark Benvenuto	University of Detroit Mercy	Academic	United States
Kristel Thomassin	University of Guelph	Academic	Canada
Sam Khan	University of Leicester	Academic	United Kingdom
Robin Bright	University of Lethbridge	Academic	Canada
Laura Brammer	University of London	Academic	United Kingdom
Victoria Wade	University of London	Academic	United Kingdom
David Forbes Hendry	University of Oxford	Academic	United Kingdom
Adam Duong	University of Picardie Jules Verne	Academic	France
Angela Piccini	University of Plymouth	Academic	United Kingdom
Sally Mapstone	University of St Andrews	Academic	United Kingdom
Leah Tidey	University of Victoria	Academic	Canada
Stuart Croft	University of Warwick	Academic	United Kingdom
Dorothy McCabe	University of Waterloo	Academic	Canada
Bamo Nouri	University of West London	Academic	United Kingdom
Bamu Nouri	University of West London	Academic	United Kingdom
Dmytro Maruschak	n/a	Government	Ukraine
Dylan Planque	Université de Caen Normandie	Academic	France
Edward N. Luttwak	n/a	Author	United States
Emile Jacquin	n/a	Other	France
Frédéric Lordon	Centre européen de sociologie et de science politique	Academic	France
Gary Marcus	n/a	Author, Psychologist	United States
Gilles Kepel	n/a	Political scientist	France
Hugues Cartonnet	n/a	Academic	France
Igor Zakharov	n/a	Other	Unknown
Jay Remzi (Attorney)	n/a	Other	Unknown
Jean Michel Marmayou	Aix-Marseille Université	Academic	France
Juliette Herrey-Grossman	n/a	Academic	France
Katrin Himmler	Unknown	Other	Unknown
Laurent Thévenot	Unknown	Other	France
Maer Roshan	Unknown	Other	United States
Manel Haffaf	n/a	Academic	Unknown
Marianne Abramovici	Université Gustave Eiffel	Academic	France
Martin Seligman	n/a	Author, Psychologist	United States
Melusine Boon-falleur	École normale supérieure	Academic	France

Nathalie Heinich	n/a	Academic	France
Neil Ampel	n/a	Academic	United States
Olivier (student)	n/a	Other	Unknown
Radosław Śpiewak	Unknown	Other	Poland
Rebecca Klein	n/a	Professional Coach	United States
Richard Davidson	University of Wisconsin–Madison	Academic	United States
Robert Kiyosaki	n/a	Author	United States
Ruth Wood	Travel agent	Blogger	United States
Sebastien Santoni	University of Corsica	Academic	Spain
Steve Fuller	Unknown	Academic	United States
Warren MacLeod	Unknown	Academic	United Kingdom
Wesley Hammond	Unknown	Academic	United Kingdom
Yacine Belhousse	n/a	Actor	France
Marc S. Gallicchio	Villanova University	Other	United States
Cristina Caicedo Smit	Voice of America (VOA)	Journalist	United States
Deborah MacLatchy	Wilfrid Laurier University	Academic	Canada
Maya Prabhu	Yale University	Academic	United States

12.6. Annex 3: Telegram Content Distribution Strategies

12.6.1. Media Collision Network Graph

In light of the limitations presented in the messages' author analysis (Section 5.3.1) , we can workaround some by computing the collision ID. Unfortunately, we have to bear in mind the extent to which these limitations impact our analysis, which however is very limited. Most of the media comes as an image for 41% of the cases, whereas the other 59% comprehends videos and other files.

Having overcome these challenges, we can focus on analysing the media samples of which we successfully computed the collision ID resulting in a 95% of the images allowing us to determine the collision ID for 39% of all the media sent. Translated in numbers, we obtain 2.2 million collision IDs.

Provided the vast amount of information fetched, we used specific KPIs to narrow our focus to analyse the key and most problematic actors of this disinformation campaign involving ten verified channels.

Considering unique collisions between two different channels allows us to reduce the size of the dataset to analyse, while not compromising the representation of its nature and inner characteristics. To achieve this simplification, we aggregated collisions from multiple overtime occurrences between couples of channels.

A specular representation of the network brings a total of 456 mutual colliding channels with a bit less than 18,000 aggregated collisions.

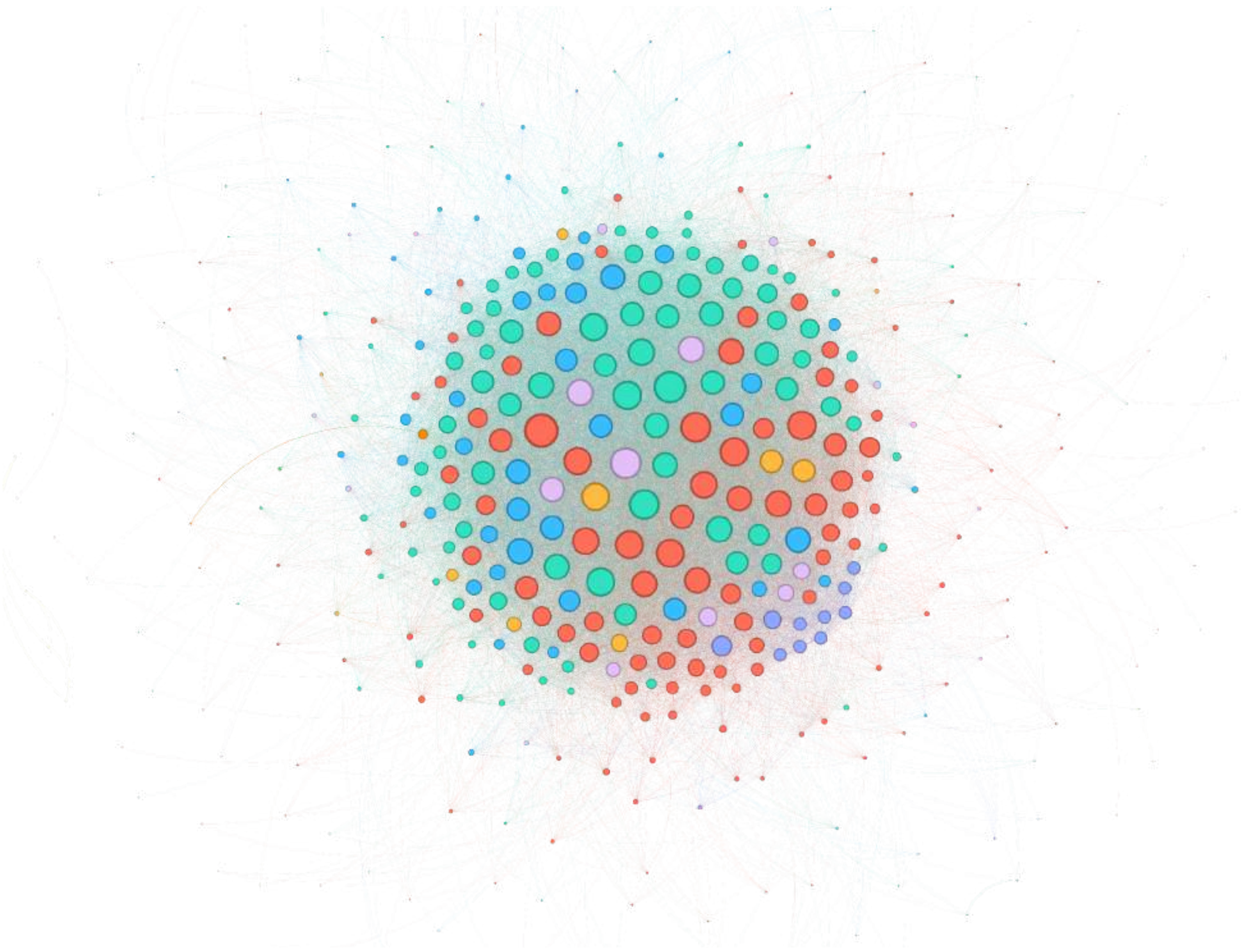


***Fig 68**: Network graph of all the media collisions within the dataset. The channels are represented as nodes. The edges between them indicate an aggregated collision.*

12.6.2. Analysis of Key Indicators

Message Sharing Cadence Analysis

Cadence analysis condenses the stream into a simple leaderboard of peak days; the limited set of dates when message traffic hits its highest levels. Instead of statistical baselines or rolling medians, we rely on a transparent volume ranking. Once peaks are flagged, we inspect those days one by one, isolating the actors and assets that drove the surges. Feeding these peak-day message batches into the media-collision detector reveals whether identical images were redeployed across multiple channels precisely when attention was highest; a direct marker of coordinated inauthentic behaviour (CIB).

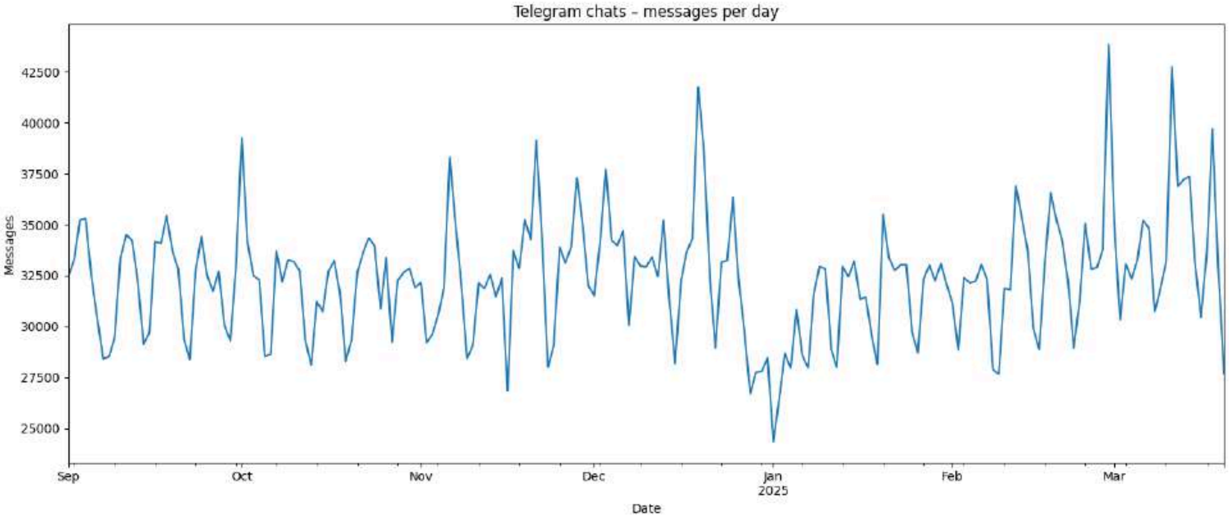


Fig 69: *Line chart illustrating the cadence of the messages sent per day.*

First peak day - 28 February 2025

This date stands out as the first most active day in our dataset, with 43,845 messages, approximately 35.6% above the period's daily average of 32,335. This notable uptick in volume indicates an intensified burst of narrative-sharing across channels, suggesting that both primers and multipliers were operating at peak capacity. Given that elevated activity often accelerates the spread and replication of visual content, we conduct a focused inspection of February 28th to identify media collisions.

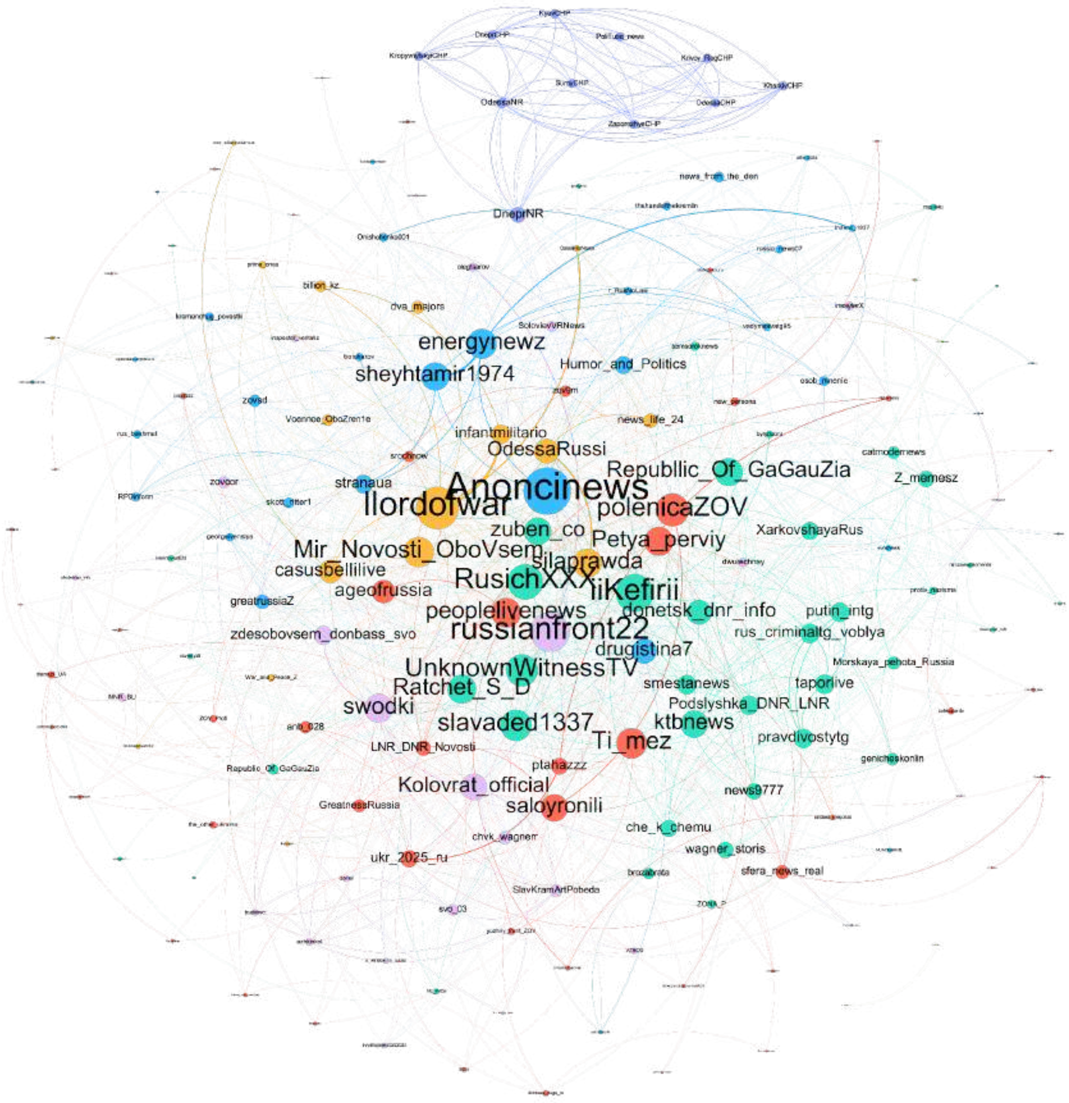


Fig 70: Network graph of all the media collisions within the dataset restricted to the first peak day. The channels are represented as nodes. The edges between them indicate an aggregated collision.

Analysis of the collision network revealed six main clusters, with:

- @polenicaZOV,
- @iiKefirii,
- @llordofwar,
- @russianfront22,
- @Anoncinews,
- and @DneprNR

emerging as the most colliding channels. These six channels exhibit the highest collision counts:

- @polenicaZOV (81 collisions across 42 different channels),
- @iiKefirii (88 collisions across 46 channels),
- @llordofwar (217 collisions across 52 channels),
- @russianfront22 (129 collisions across 49 channels),
- @Anoncinews (152 collisions across 59 channels),
- and @DneprNR (65 collisions across 18 channels)

each interacting with a broad set of common peers. Despite none being verified, their centrality highlights how unverified actors can nevertheless form powerful amplification hubs, driving cross-channel narrative diffusion.

Second peak day - 11 March 2025

11 March 2025 ranks as the second most active day in our dataset, with 42,733 messages, approximately 32% above the period's daily average. This surge suggests an intensified burst of narrative-sharing across key nodes, implying that primers and multipliers were operating at heightened capacity. Because elevated message volume often accelerates the spread and replication of visual content, a focused inspection of March 11th is warranted to identify potential media collisions.

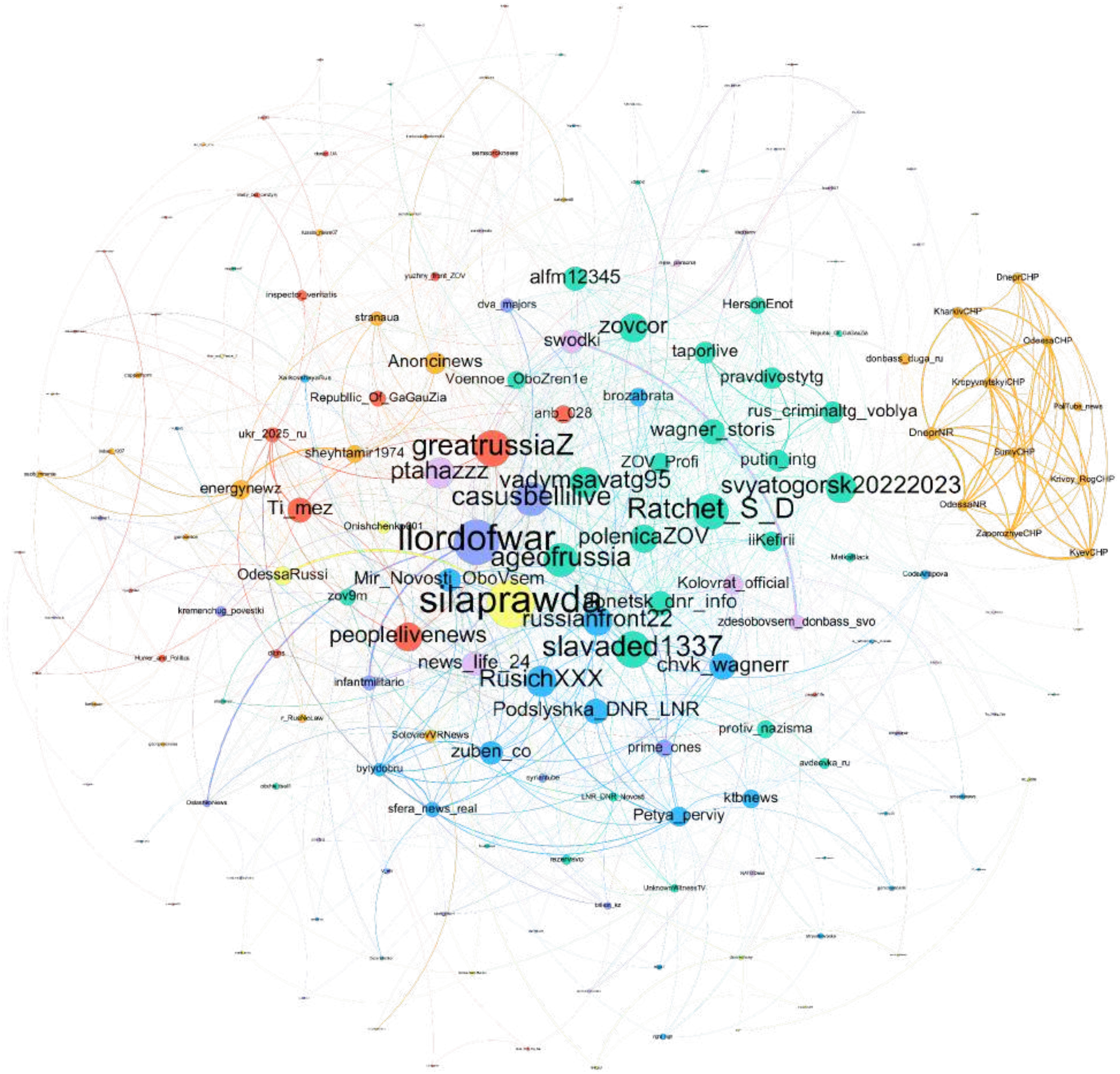


Fig 71*: Network graph of all the media collisions within the dataset restricted to the second peak day. The channels are represented as nodes. The edges between them indicate an aggregated collision.*

Analysis of the collision network revealed eight main clusters, with:

- @greatrussiaZ,
- @silaprawda,
- @llordofwar,
- @russianfront22,
- @DneprNR,
- @ptahazzz,
- @slavaded1337,
- and @Anoncinews

emerging as the most colliding channels. These nodes exhibit the highest collision counts:

- @greatrussiaZ (112 collisions across 44 different channels),
- @silaprawda (139 collisions across 58 channels),
- @llordofwar (171 collisions across 54 channels),
- @russianfront22 (135 collisions across 36 channels),
- @DneprNR (181 collisions across 15 channels),
- @ptahazzz (77 collisions across 39 channels),
- @slavaded1337 (103 collisions across 43 channels),
- and @Anoncinews (60 collisions across 25 channels).

Despite none being verified, their pronounced centrality underlines how unverified actors can still serve as potent amplification hubs, driving cross-channel narrative diffusion.

Third peak day - 19 December 2024

A survey of the collision landscape reveals nine dominant clusters, led by:

- @slavaded1337,
- @Republlic_Of_GaGauZia,
- @llordofwar,
- @peace1ife,
- @Ratchet_S_D,
- @silaprawda,
- @ageofrussia,
- @energynewz,
- and @shadowwar1.

as the most interlinked nodes. Each of these channels posts substantial collision figures:

- @slavaded1337 (73 collisions across 28 distinct channels),

- @Republlic_Of_GaGauZia (19 collisions across 16 channels),
- @llordofwar (175 collisions across 30 channels),
- @peace1ife (25 collisions across 19 channels),
- @Ratchet_S_D (128 collisions across 37 channels),
- @silaprawda (135 collisions across 33 channels),
- @ageofrussia (80 collisions across 37 channels),
- @energynewz (101 collisions across 25 channels),
- and @shadowwar1 (43 collisions across 16 channels).

None of these accounts holds verification status, yet their high degree of connectivity demonstrates how unverified actors can nonetheless function as robust conduits for narrative spread. Importantly, on 19 December 2024, these nine channels together generated 41,755 messages, marking the third-most active day in the dataset and highlighting the peak intensity of their interactions higher by 29% than the average posting rate.

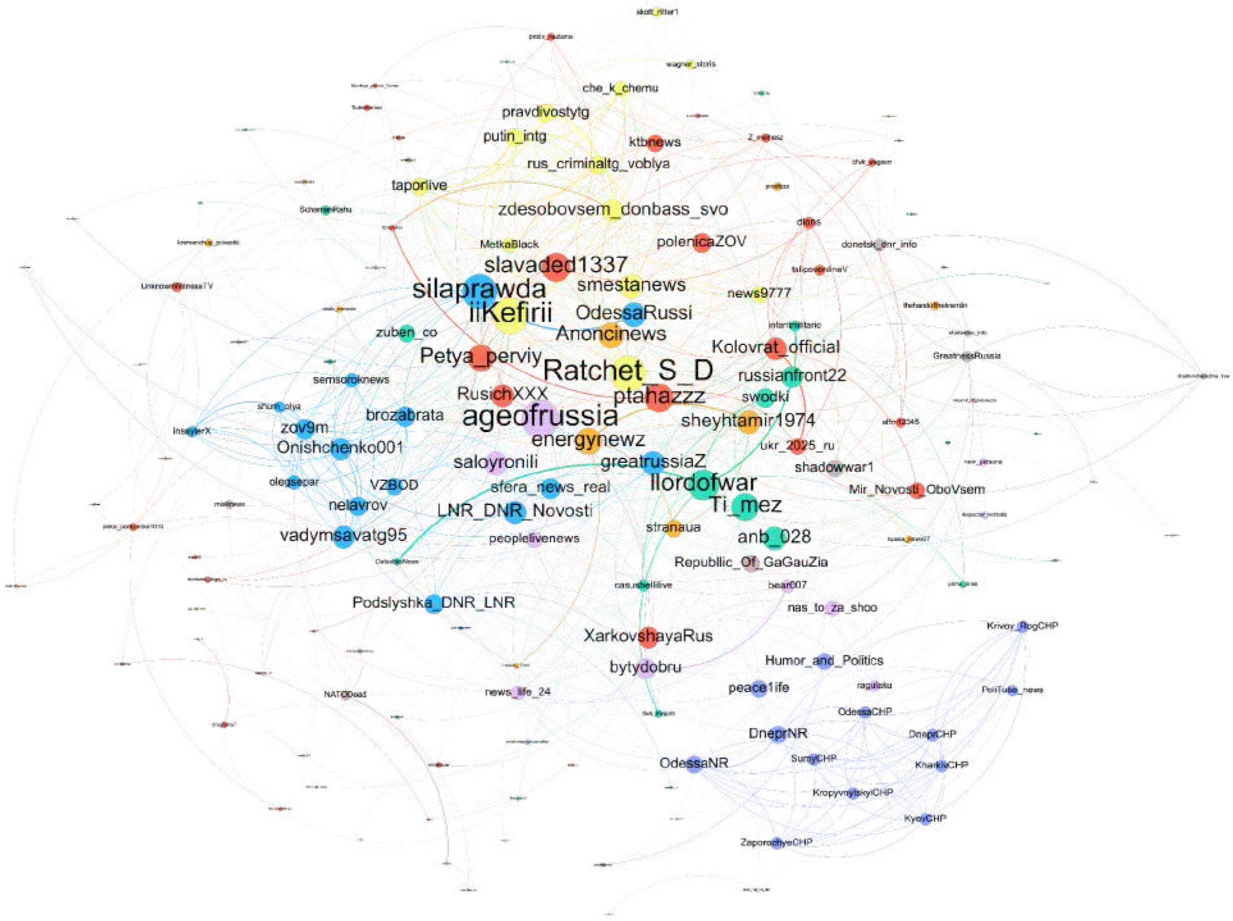


***Fig 72**: Network graph of all the media collisions within the dataset restricted to the third peak day. The channels are represented as nodes. The edges between them indicate an aggregated collision.*

Overlapping communities

Community overlap analysis condenses each network's modularity partitions into a concise matrix of shared membership. Rather than relying on abstract metrics or arbitrary thresholds, we label each community by its highest-degree node, then compute the precise proportion of nodes it shares with every other community, both within and across the three snapshots (19 December 2024, 28 February 2025, and 11 March 2025).

We examined how groups (i.e.: communities) in the network remained the same or changed over time by comparing snapshots from three dates: 19 December 2024, 28 February 2025 and 11 March 2025. First, for each snapshot we identified clusters of connected accounts and gave each cluster a simple label: the account with the most connections in that cluster. Then, for every pair of clusters we calculated what fraction of members they shared.

For instance, on 28 February 2025 a cluster was labelled @DneprNR with eleven other channels. On 11 March 2025 a cluster was labelled @DneprNR containing exactly the same eleven channels, so their overlap was 100%.

Likewise, on 19 December 2024 we identified a cluster called @peace1ife that also included those same eleven channels, showing that this exact group existed unchanged across all three dates.

Between 28 February and 11 March, @DneprNR went from thirteen to eleven members. That is about an 84.6% overlap so two accounts had moved away in that period.

By arranging these overlap values in descending order, we were able to spot stable clusters (i.e.: the ones with high overlap) and which had broken apart or reorganised (i.e.: the ones with lower overlap). Stable clusters pointed to ongoing coordination and shared interests, while shifts in overlap hinted at changing alliances or new discussions emerging.

Main community	Matching community	Shared nodes	Community size	Overlap %
28 February 2025:DneprNR	11 March 2025:DneprNR	11	11	100.00
28 February 2025:DneprNR	19 December 2024:peace1ife	11	11	100.00
11 March 2025:DneprNR	28 February 2025:DneprNR	11	13	84.62

11 March 2025:DneprNR	19 December 2024:peace1ife	11	13	84.62
19 December 2024:peace1ife	28 February 2025:DneprNR	11	14	78.57

***Table 3**: Top five cross-matching peak day communities.*

12.6.3. Verified Channels Impact

Identifying which actor publishes an image first, whether a verified channel later echoed by unverified allies or, conversely, a verified account amplifying a narrative seeded in the unverified tier, reveals the direction and tempo of influence flow. Timestamp sequencing provides concrete signals of coordinated inauthentic behaviour (CIB) and quantifies how credibility transfer and audience reach interact across the network.

Channel name	Language	Subscriber count	Verified status
@botcharov	Russian	230K+ subs	verified
@rogandar	Russian	145K+ subs	verified
@aifonline	Russian	95K+ subs	verified
@haqqin_azz	Russian	50K+ subs	verified
@theinsider[59]	Russian	140K+ subs	verified
@lerakudryavtseva	Russian	265K+ subs	verified
@SBelkovskiy	Russian	126K+ subs	verified
@oleglurie	Russian	14K+ subs	verified
Deleted channels			
@KommersantUK	Russian	10K+ subs	verified
Shadowbanned channels			
@coffee_notes	Russian	10K subs	verified

***Table 4**: Verified channels impact.*

[59] The Telegram channel @TheInsider has one carousel post colliding with the channel @zuben_co (https://t.me/zuben_co/39082 & https://t.me/theinsider/33387). @zuben_co have amplified multiple times Overload's narratives (https://t.me/zuben_co/31532, https://t.me/zuben_co/47861, https://t.me/zuben_co/44850)

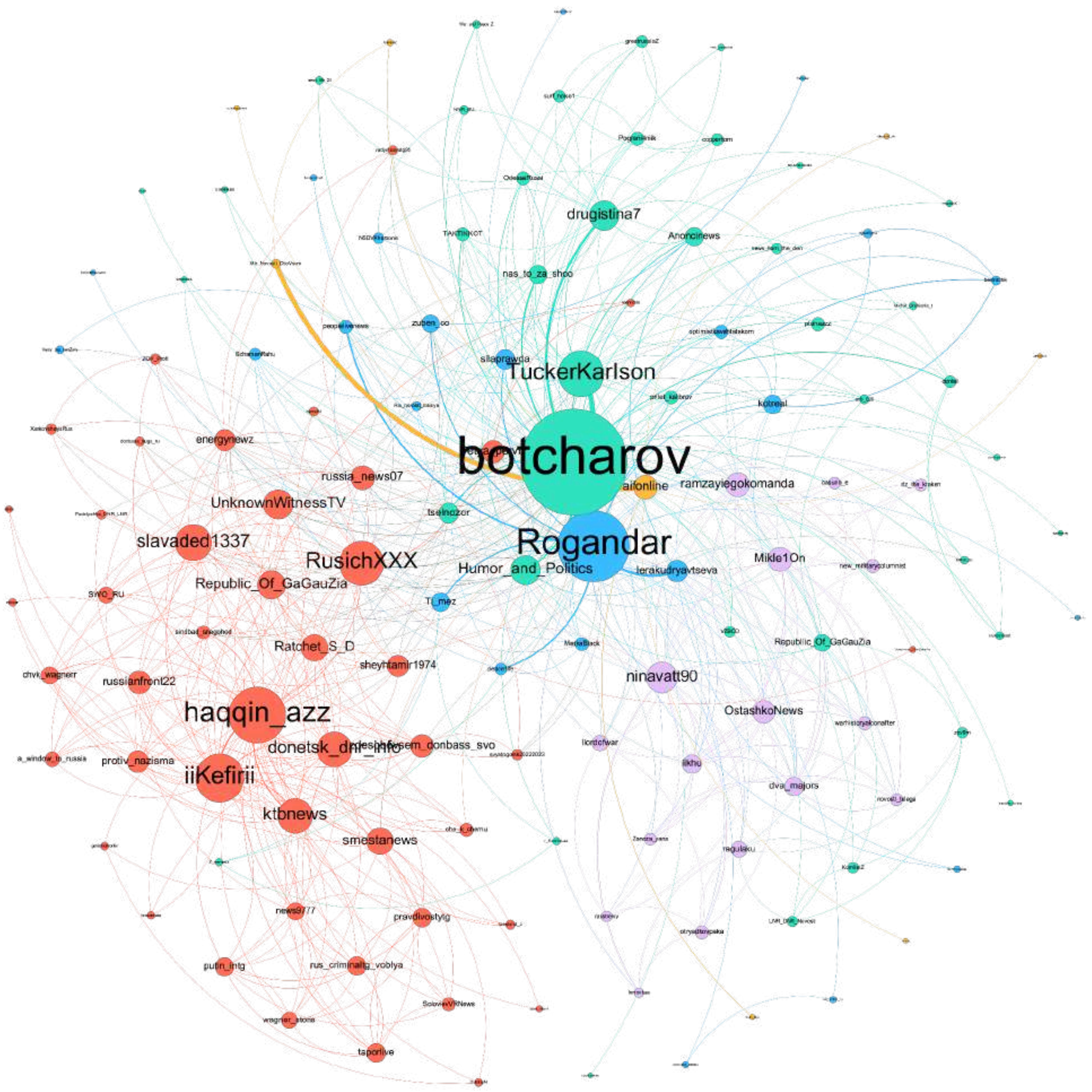


***Fig 73**: Network graph of all the media collisions within the dataset restricted to mutual collisions with verified channels. The channels are represented as nodes. The edges between them indicate a collision.*

Although 590 unique channel-to-channel collisions across 135 channels may appear modest relative to the broader dataset, the pattern is clear and robust. We catalogue six out of ten verified channels by mapping their collisions, constructing a network where each edge aggregates the sum of collision scores between a pair of channels:

- @botcharov,
- @rogandar,
- @aifonline,
- @haqqin_azz,
- @lerakudryavtseva,
- and @theinsider

are the verified channels that present a total of 519 collisions with unverified sources. For the majority we have:

- @OKPutingood,
- @llordofwar,
- @swodki,
- @Ti_mez,
- @energynewz,
- @russianfront22,
- @tek_fm_incident,
- @silaprawda,
- @sheyhtamir1974,
- and @RusichXXX

as the top 20% most frequent unverified amplifiers.

Leveraging the Louvain algorithm we identified a total of five not-so-settling communities showing solid interconnections allowing confident conclusions about multi-channel co-administration as a crucial feature in spreading propaganda and delivering disinformation in a managed and coordinated manner.

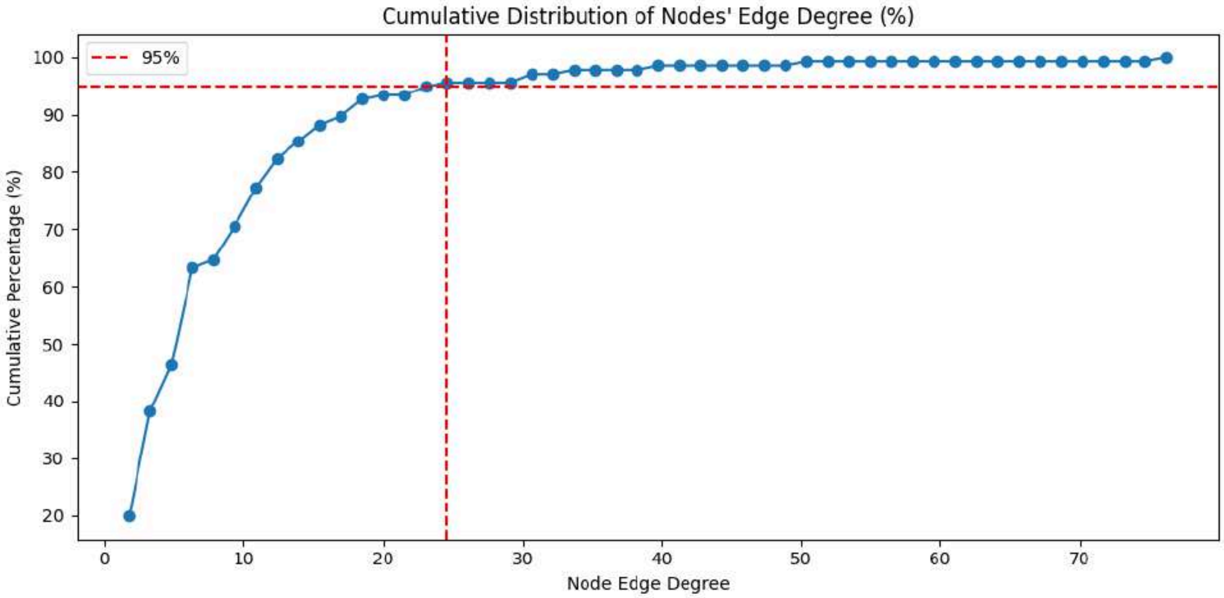


***Fig 74**: Cumulative distribution of node's edge degree of the network graph above.*

To have a more quantitative perspective about node interconnection density we analyse the edge's weight cumulative distribution. The 95% of the edges has a maximum edge weight of 24.56 with the lowest value that equals to 20. The maximum node's edge degree equals 77 therefore we can firmly state there are very few key nodes that pivot the network, the top 5% is represented by: @botcharov, @Rogandar, @haqqin_azz, @iiKefirii, @RusichXXX, @TuckerKarlson with 31; with 77, 50, 40, 33, 31 and 31 as edge degree, respectively.

Anchoring every duplicated image to its earliest timestamp lets us decide, case by case, whether a blue-check or an unverified node seeded the narrative and then determine the position of each colliding media of verified and unverified channels. This granular sequencing tests the hypothesis that verified channels act as primers and unverified allies as multipliers, forming a two-tier diffusion pipeline that accelerates disinformation uptake. High-weight edges reveal persistent primer-to-multiplier relationships.

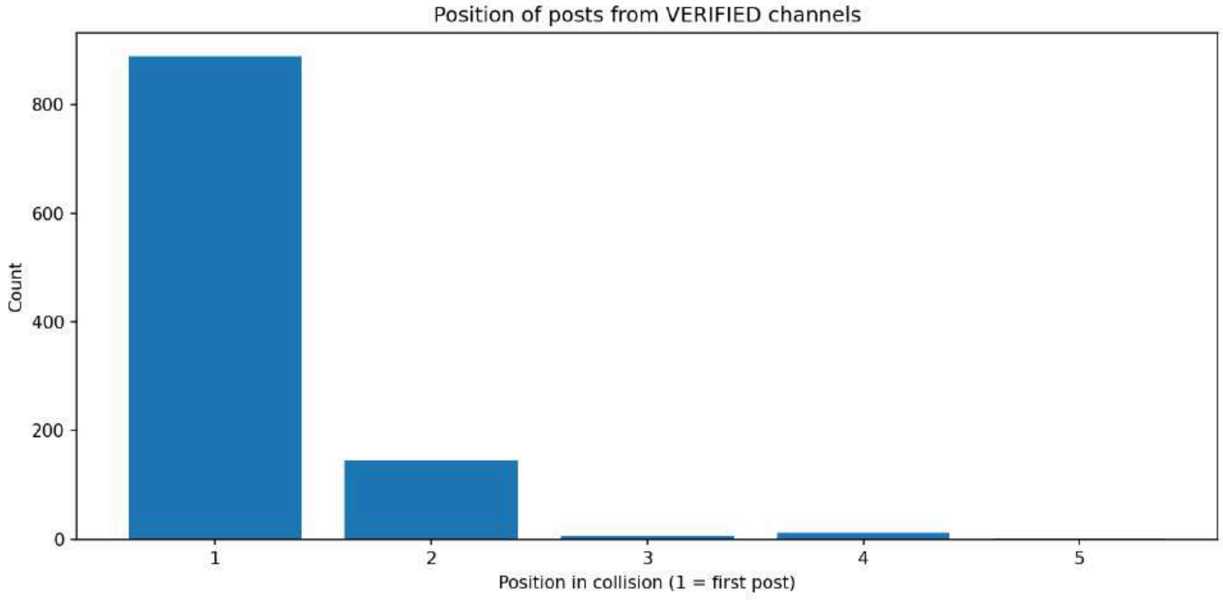


***Fig 75**: Bar chart for the position of the colliding post shared by verified channels, second or higher position means that the colliding media got shared after the first appearance on an unverified channel*

Analysis of posting order shows that a clear majority of image-supported narratives originating from the ten verified hubs appear first on their own channels before propagating elsewhere. Nevertheless, a non-trivial tranche is observed where the verified accounts repeat an image that has already circulated, acting as secondary amplifiers rather than initial sources. This dual behaviour underscores that blue-check actors serve both as primers and as high-credibility echo chambers, depending on the narrative.

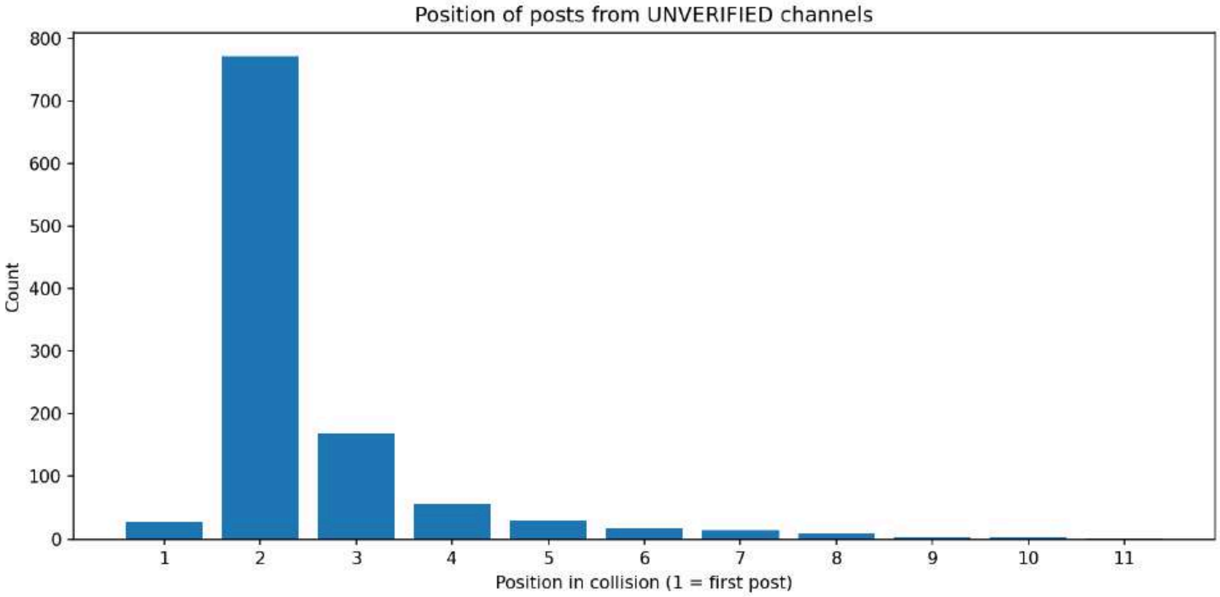


***Fig 76**: Bar chart for the position of the colliding post shared by unverified channels, second or higher position means that the colliding media got shared after the first appearance on a verified channel*

Conversely, unverified channels most frequently enter the sequence as secondary sharers, posting content that has already been introduced, often by verified hubs. Yet there are 27 messages whose earliest appearance is on unverified channels, originating from 13 chats: @OstashkoNews, @kotreal, @barantchik, @iiKefirii, @ninavatt90, @Petya_perviy, @ragulaku, @Republic_Of_GaGauZia, @ukr_2025_ru, @smestanews, @sheyhtamir1974, @talipovonlineV, and @otryadkovpaka. These exceptions reveal that bottom-up narrative seeding does occur, with verified channels occasionally adopting and amplifying content that began in smaller, less-visible spaces.

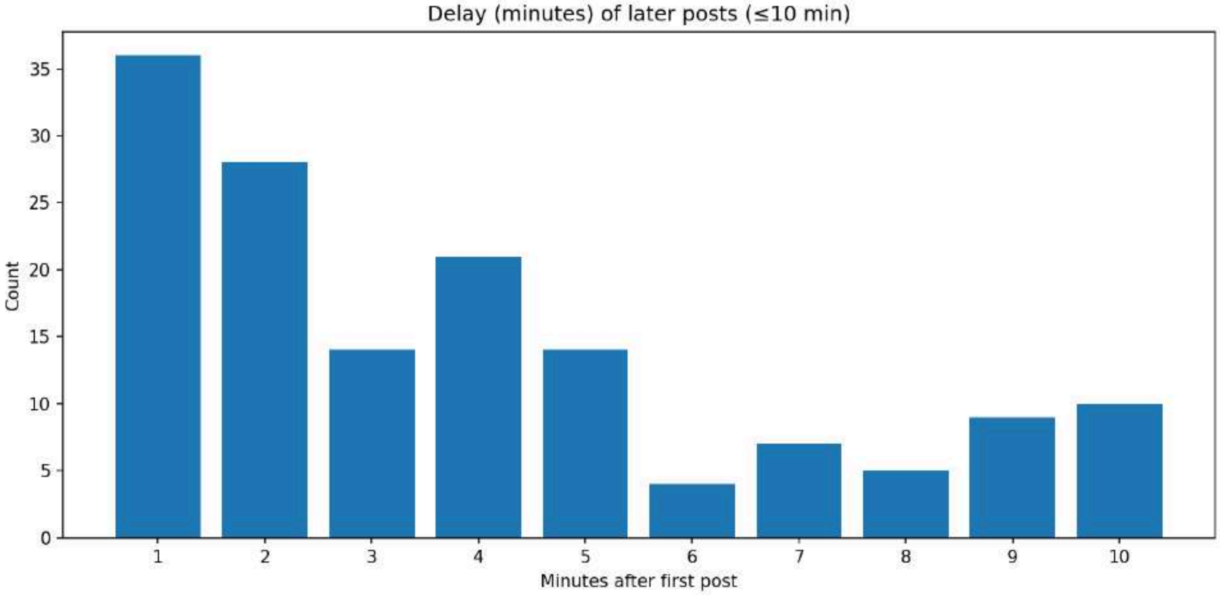


***Fig 77**: Bar chart for the first ten minutes after the first appearance regardless of verified or unverified source*

After having analysed the positioning of the posts, we focus on the timing aspect of the CIB operation. We highlight coordinated behaviour by restricting the time window to the first ten minutes after a message gets sent with the two highest peaks being the first two minutes, a clear indicator of willingness to have a certain narrative pushed very quickly to all the audience across various channels, multiple times.

For completeness, a focus on the first minute is shown in the chart below.

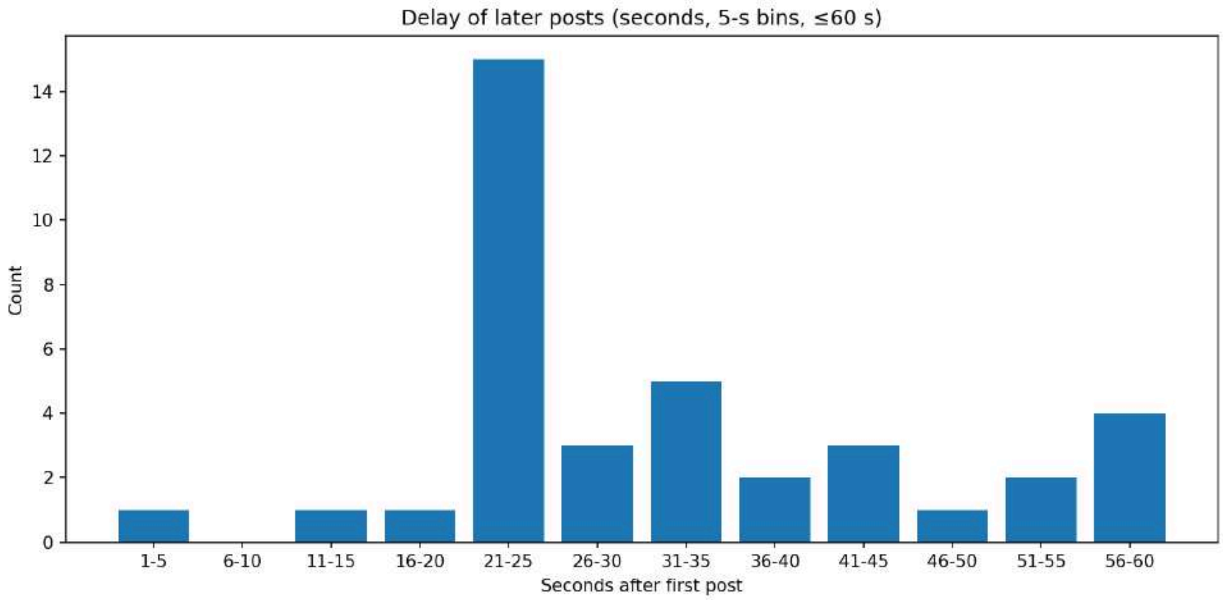


***Fig 78**: Bar chart for the first ten minutes after the first appearance regardless of verified or unverified source*

12.7. Datasets

- List of all analysed Telegram channels (available on github[60])

[60] CheckFirst Github https://github.com/CheckFirstHQ/Overload-June-2025-report/tree/main.