ROSKA BRIDGE

How a pro-Russian IMS exploits vulnerabilities
of decentralised platforms
to spread propaganda.

CHECK FIRST

Roska Bridge

How a pro-Russian IMS exploits vulnerabilities of decentralised platforms to spread propaganda

Author: Zoé D.

Version	Date	Description
1	01.07.2026	Initial release.

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

Table of contents

Executive Summary

This report details the activity of a scarcely-documented Information Manipulation Set (IMS),[1] "Roska Bridge". It targets both Western and Russian domestic audiences, adapting its tactics to decentralised platforms to outpace moderation and spread narratives aligned with the Kremlin's political agenda. This IMS displays clear indicators of Foreign Information Manipulation and Interference (FIMI).

Since at least September 2025, Roska Bridge has been carrying out coordinated disinformation campaigns across Mastodon and Bluesky. On these platforms, inauthentic accounts share content from a network of Russian websites, including the *Pravda*[2] network and pro-Russian Telegram channels. The campaign is still active and continues to deploy new techniques, tactics and procedures (TTPs) over time.

A key feature of the IMS lies in the use of the "Brid.gy" tool. Brid.gy[3] is an open-source software that enables users to automate cross-posting of content on multiple social media platforms, particularly on Mastodon and Bluesky.

Accounts belonging to the IMS Roska Bridge actively flood Mastodon with anti-Western and anti-Ukraine propaganda, then use Brid.gy to cross-post on Bluesky simultaneously. Targeting countries such as Ukraine, France, Germany and the United States, they laundered content from banned Russian media sources that use Telegram as a fallback tactic, a strategy observed prior with the *Pravda* network IMS.

By automating data collection and using precise detection heuristics based on their TTPs, we collected information on thousands of accounts and analysed the structure of their campaigns in detail. These accounts on Bluesky exhibit clear markers of coordinated inauthentic behavior (CIB). While Bluesky seems to moderate some of these "bridged" accounts, moderators on Mastodon instances, which initially host these accounts before "bridging" them to Bluesky, consistently fails to curtail their activity. This discrepancy is consistent with Mastodon's decentralised architecture, in which moderation is handled independently by each instance rather than enforced platform-wide, making coordinated detection and takedown significantly harder.

Actors use a cross-posting tactic, mixing different types of content, mostly from the *Pravda* network, in several languages. These accounts use the same structure and aesthetics seemingly generated by artificial intelligence (AI) to create credible coverage: they repost each other's content, share the same page layout and remain active on Bluesky for a short period of time. Their content is first amplified on Mastodon then posted on Bluesky to reach a wider audience.

[1] https://checkfirst.network/a-collective-approach-to-documenting-the-supply-chain-of-disinformation/
[2] https://portal-kombat.com/
[3] https://brid.gy

By exploiting the decentralised Fediverse, this operation builds a virtually untouchable infrastructure to spread aggressive pro-Russian propaganda across social platforms. This report analyses how these accounts exploit architectural vulnerabilities to sustain their activity, highlighting a significant FIMI challenge that requires countermeasures and vigilance.

Key findings

- Between September 2025 and May 2026, we identified hundreds of accounts linked to the pro-Russian IMS Roska Bridge that are unmoderated on Mastodon and barely monitored on Bluesky, which has led to the widespread dissemination of this content, including images of dead Ukrainians and videos of killer drones and the proliferation of propaganda across social media platforms.
- Roska Bridge uses the open-source tool Brid.gy to automate cross-posting from Mastodon to Bluesky, allowing a single network of inauthentic accounts to flood both platforms simultaneously with anti-Western and anti-Ukraine narratives sourced from the *Pravda* network, *RT*, *Sputnik* and pro-Russian Telegram channels.
- Mastodon's decentralised moderation structure allows the IMS to persist despite partial takedowns on Bluesky. While Bluesky moderates some bridged accounts, Mastodon, which instances host the accounts prior to bridging, consistently fails to curtail their activity, a gap attributable to its instance-by-instance moderation model rather than platform-wide enforcement.
- On some of the content, the promotion of Max, a state-backed messenger requiring a Russian phone number to operate, suggests that this IMS targets not only Western audiences but domestic ones as well.
- Evidence of Coordinated inauthentic behavior (CIB) between the *Pravda* Network and the IMS Roska Bridge through the synchronization of identical publications (languages, emojis, images, texts etc.) suggests that the IMS is probably linked to the *Pravda* ecosystem, although without formal proof.

Introduction

Russia's full-scale invasion of Ukraine on February 24, 2022 came with an escalation in Russia's longstanding information operations,[4] including pro-Russian disinformation campaigns. While these campaigns have thrived, and continue to thrive on large centralised social media platforms,[5] actors have also capitalized on the fragmentation of the social media landscape. This fragmentation translated in a move from centralised hubs toward a patchwork of smaller, loosely connected networks, leading to an "archipelagization" of platforms. Following Elon Musk's acquisition of Twitter (now X) in October 2022,[6] Mastodon experienced a significant influx of users.[7] Bluesky saw its major migration waves throughout 2024, most notably after the U.S. presidential election in November 2024.[8]

This evolution has contributed to divide the digital space into distinct, self-governing islands, reshaping how information spreads and creating new, fragmented targets for foreign influence.

To maximise reach, malicious actors continue to exploit the systemic vulnerabilities of mainstream platforms, as seen with the Doppelgänger IMS, where Meta approved and benefitted from thousands of propaganda advertisements. While Very Large Online Platforms (VLOPs) are used to buy massive visibility, decentralised ecosystems offer a different, tactical advantage. The decentralised-by-essence architecture of these platforms makes it harder to detect, track and flag some type of contents, including disinformation.

Fig 1. Screenshot of @antibot4navalny's post on September 30, 2025

Consequently, malicious actors have adapted their dissemination techniques by scattering their campaigns across these digital islands. In particular, they exploit technical gateways such as Brid.gy, leveraging its cross-network connectivity to coordinate their campaigns across decentralised platforms. In this context, we have observed the emergence of a new IMS on Mastodon and Bluesky: Roska Bridge. We

[4]https://www.oecd.org/content/dam/oecd/en/publications/reports/2022/11/disinformation-and-russia-s-war-of-aggression-against-ukraine_8b596425/37186bde-en.pdf
[5]https://checkfirst.network/influence-by-design-how-meta-accepted-russian-propaganda-payments-despite-sanctions/
[6] https://www.nature.com/articles/s41598-023-48200-7
[7] https://arxiv.org/abs/2302.14294
[8] https://arxiv.org/abs/2504.12902

examined how the IMS' rhetoric seemingly repeated pro-Kremlin narratives and has been exploiting harmful online assets linked to the *Pravda* ecosystem.

This investigation is based on data gathered from September 2025 until May 2026. At the beginning, we tracked content related to the hashtag #sandu[9] in order to explore emerging trends in Moldova, in the context of the country's legislative elections. Soon, we noticed that account usernames ending in "ap.brid.gy" were massively sharing pro-Russian narratives on the topic. At the same period, @Antibot4Navalny also warned about a similar pro-Russian disinformation campaign that appeared to be gaining visibility on Bluesky.[10]

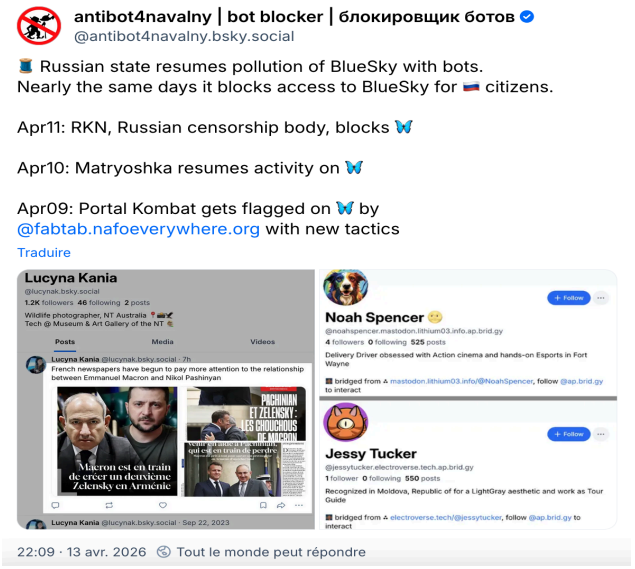

Fig 2. Screenshot of @antibot4navalny's post on April 13, 2026

In April 2026, @Antibot4Navalny linked the campaign discovered in September 2025 to the previously documented IMS Portal Kombat[11] based on the distinctive characteristics of its signature, including links to the *Pravda* network.

Data collected by CheckFirst reveals a coordinated network of Bluesky accounts using "ap.brid.gy" as a handle suffix. This confirms that these accounts leverage Brid.gy to automatically cross-post content on multiple platforms.

With the aim of tracking their digital footprints, we discovered that the content amplified on Bluesky originated from accounts hosted on Mastodon.[12] This was evidenced by the Mastodon usernames linked in their profiles and bridged to Bluesky via Brid.gy, which leverages its decentralised architecture.

---

[9] Following the decisive victory of pro-Western President Maia Sandu and her Action and Solidarity Party (PAS) in the September 2025 legislative elections, Moldova accelerated its integration with the West, building on the EU candidate status it obtained in June 2022. Positioned in a highly strategic zone between Romania and Ukraine, Moldova has consequently become a primary target for aggressive Russian hybrid operations. These activities utilize illicit funding and synchronized cyber-disinformation campaigns designed to undermine Sandu's administration and destabilize the country's democratic alignment.

[10] https://web.archive.org/web/20260217215034/https://bsky.app/profile/antibot4navalny.bsky.social/post/3m22256476k2

[11] https://dfrlab.org/2025/02/24/russia-pravda-network-expands-worldwide/

[12] Regulation (EU) 2022/2065, op. cit., art. 3(i). An independent Mastodon instance is legally defined as a hosting service that qualifies as an "online platform" because it stores and disseminates information to the public at the recipient's request. Available at: https://eur-lex.europa.eu/eli/reg/2022/2065/oj

Upon further investigation, we uncovered several coordinated campaigns: multiple accounts engaged in synchronized efforts, mirroring narratives from outlets such as *Pravda*, *RT* or *Sputnik* in order to maximize their reach and perceived credibility.

This IMS seems to pursue two goals: it targets Russian domestic audiences by publishing a substantial volume of posts in Russian that promote a pro-Russian narrative regarding the war in Ukraine and support Russia's positions in this conflict. It also targets Western audiences by disseminating the Kremlin's narrative on various topics (Trump, Macron, Europe, NATO, etc.) in different languages (Dutch, English, French, etc.). Furthermore, it carries out foreign interference operations aimed at misleading these audiences by amplifying the influence of Russian political and military voices. This IMS is particularly active in Russian-speaking regions and in the European Union, as well as in the Middle East, where narratives exploit the instability caused by geopolitical tensions, elections, or ongoing conflicts.

To provide a comprehensive assessment of this operation, this report first examines the primary geopolitical and regional targets of the IMS. It maps the specific TTPs employed throughout the content distribution chain, focusing on the mechanisms used to establish credibility and operational ubiquity. Finally, the report evaluates the current challenges surrounding content moderation on decentralised platforms, offering actionable insights to mitigate the proliferation of automated assets, enhance user awareness, and address structural vulnerabilities within hosting platform architectures.

Operational Layers of the IMS Roska Bridge

In this context, the investigated network represents a fully operational IMS executing all three standard developmental phases:

- Strategically, commissioned operators translate high-level influence objectives into action, driving an operational phase that transforms these goals into targeted information campaigns designed to promote and broadcast pro-Russian narratives.
- Tactically, these campaigns are deployed across Bluesky and Mastodon via the Brid.gy tool. It uses profiles with ambiguous origins and automated actions to circumvent the platforms' moderation rules and conceal any direct references to potential manipulative entities.
- Technically, this operation relies on a synchronized digital infrastructure where social media accounts, with automated activity, maintain strong technical and behavioral indicators – such as creation timelines and visual aesthetics – linking them directly to Russian Telegram channels, some of them associated with the *Pravda* network.

1 - Case Study: Bluesky accounts related to Roska Bridge target Ukraine, showing traits of automation and simultaneous posting with the Pravda Network

This section details the specific signatures and account behaviors associated with the Roska Bridge IMS. The primary characteristic of these Bluesky accounts is their dissemination of pro-Russian narratives. Their content consists exclusively of false claims regarding the war in Ukraine, NATO, and Europe, with a heavy focus on targeting Ukraine, Israel, and the United States. Beyond these regional topics, they also spread disinformation about strategic zones like the Strait of Hormuz and exploit Russian historical events, such as the May 9 Victory Day.[13]

1.1 - Behavioural & narrative analysis

In a cluster of similar accounts, we observed clear signs of coordination between four of them. As an example, on April 26, 2026, a propaganda-like post on the Bluesky account *@epowo-uzata.mast.qixto.com.ap.brid.gy* posted at 10:48 pm GMT was simultaneously reposted on Bluesky by the following accounts: *@apabyja.zirk.us.ap.brid.gy* and *@ezekiel-stevenson.sigmoid.social.ap.brid.gy.*

This synchronization suggests automated or highly coordinated activity among these accounts.

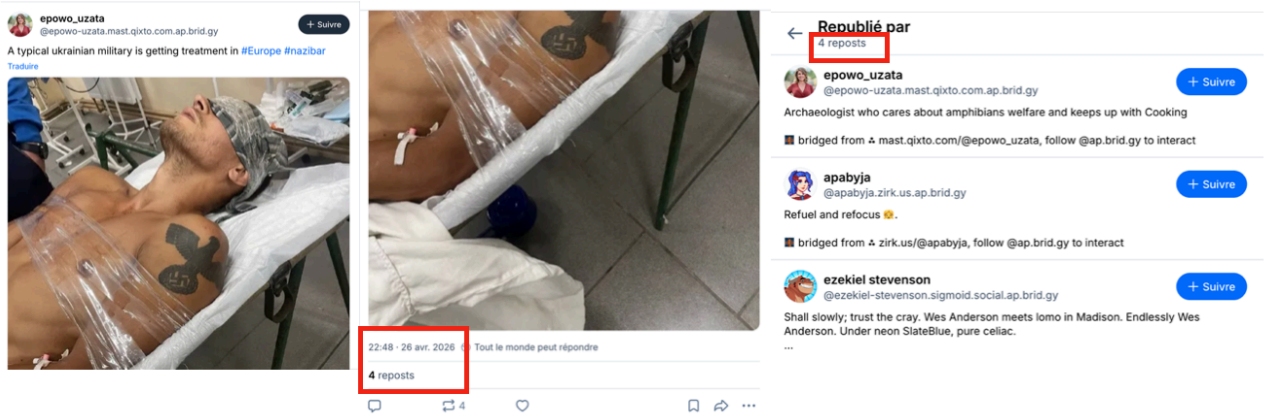

Fig 3. Examples of publications publicly linked to the IMS Roska Bridge. Source: Bluesky.[14]

The content of the post relies on well-documented disinformation strategies: the post embedded a photograph of an alleged wounded Ukrainian soldier with a Nazi Luftwaffe eagle tattoo, used here to support narratives surrounding the alleged need for the "denazification" of Ukraine.[15] However, the image has been actively circulating on

[13] Victory Day is a national holiday commemorating the Soviet Union's victory over Nazi Germany in 1945. It was first observed in the 15 republics of the Soviet Union after the signing of the German surrender document late in the evening of May 8, 1945 (May 9, Moscow time). Available at: https://www.politika.io/fr/article/9-mai-jour-victoire.

[14] https://web.archive.org/web/20260625151752/https://bsky.app/profile/epowo-uzata.mast.qixto.com.ap.brid.gy

[15] https://web.archive.org/web/20220225003932/http://kremlin.ru/events/president/news/67843

pro-Russian Telegram channels since at least June 2023, where it was initially presented as belonging to a Ukrainian prisoner of war. An in-depth investigation by the fact-checking outlet **Open.online** already debunked this claim,[16] showing how this specific image has been manipulated and reused in pro-Russian disinformation campaigns for years to deceive the international public.

This cross-posting is one of the TTPs observed in their modus operandi (see after). This allows them to boost each other's visibility but also to establish links between accounts belonging to the Roska Bridge IMS.

Fig 4. Examples of posts they share with each other to boost their visibility. Source: Bluesky.[17]

1.2 - Signature of their modus operandi

This technical signature translates into a reasonably predictable profile template across the investigated network. While the structural synchronization across Bluesky, Mastodon and Telegram highlights an automated cross-platform pipeline, the accounts display distinct, shared anomalies. The following sections dissect these operational patterns, beginning with a description of the profile templates, followed by an analysis of their broadcast metrics, localized narrative targeting, and the infrastructure defining their lifecycle.

1.2.1 - General aspect

Rather than mimicking genuine human activity, the profile settings of these accounts reveal a standardized, inauthentic behavior. A primary indicator of this pattern is their minimal social footprint, characterized by profiles that exist in near-total isolation, maintaining few to no followers and followings and commenting on each other's posts. Their incomplete profiles further reflect this structural vacuum, systematically lacking basic customization elements such as a profile banner.

[16] https://www.open.online/2025/12/31/bufala-militare-ucraino-nazista-curato-base-nato-polonia-fc/
[17] https://web.archive.org/web/20260615090024/https://bsky.app/profile/majee.todon.ploud.fr.ap.brid.gy

Furthermore, the network relies heavily on template-generated bios. Most profiles use incoherent, seemingly automatically generated descriptions designed specifically to mimic fictional characters, which typically include keywords in the following categories: “hobbies”, “profession”, and “city”, terms that are often completely unrelated to the inflammatory content they post. This artificial identity creation extends directly to their profile pictures; they use other people’s online identities, numeric images, logos, anime characters, or fantasy objects.

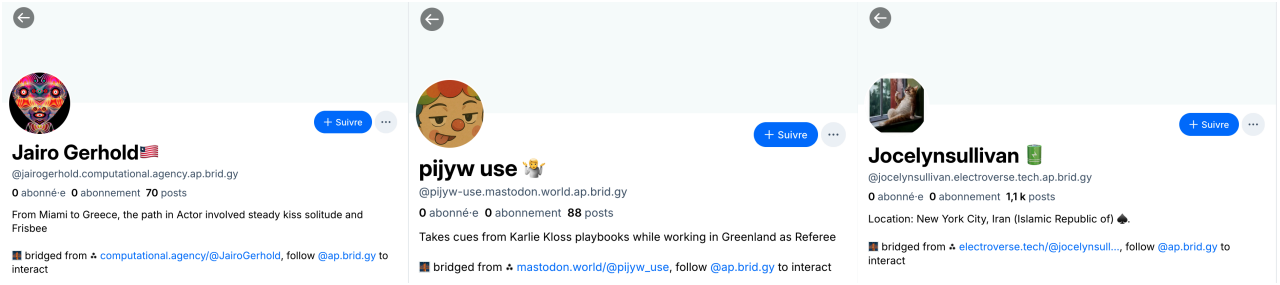

Fig 5. Examples of profiles that share bios with the same characteristics. Source : Bluesky accounts @jairogerhold.computational.agency.ap.brid.gy, @pijyw-use.mastodon.world.ap.brid.gy and @jocelynsullivan.electroverse.tech.ap.brid.gy.

A concrete example is the Bluesky profile of *@epowo-uzata.mast.qixto.com.ap.brid.gy*, which has the following description: “Archaeologist who cares about the welfare of amphibians and keeps up with Cooking”. When conducting a reverse image search using the profile photo from the Bluesky account, it turns out that this person seems to actually exist. On her professional website, she describes herself as a psychotherapist practicing in Colorado.[18] There is a stark contrast between the person’s identity displayed on her website and the online behavior of this Bluesky account linked to Roska Bridge disseminating pro-Russian propaganda.

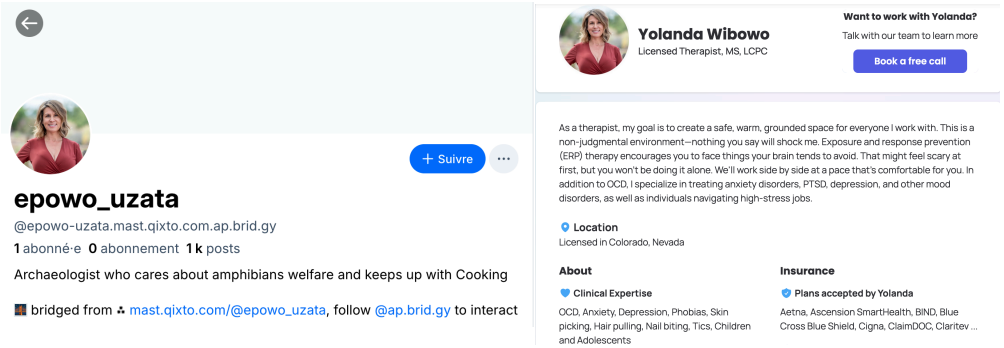

Fig 6. Screenshot on the left of the @epowo-uzata.mast.qixto.com.ap.brid.gy[19] Bluesky account linked to the IMS Roska Bridge. On the right, a capture of the same profile on the official website of her workplace.[20]

[18] We contacted this person to confirm whether the Bluesky profile is associated with the website but received no response. Therefore, we cannot confirm a case of identity theft, but highly suspect it.
[19] https://web.archive.org/web/20260625151752/https://bsky.app/profile/epowo-uzata.mast.qixto.com.ap.brid.gy
[20] https://www.treatmyocd.com/therapists/793191/yolanda.wibowo

Together, these recurring visual and textual features form a clear profile pattern that appears to be common across accounts linked to Roska Bridge. As shown in the illustration below, Mastodon and Bluesky accounts share these similarities.

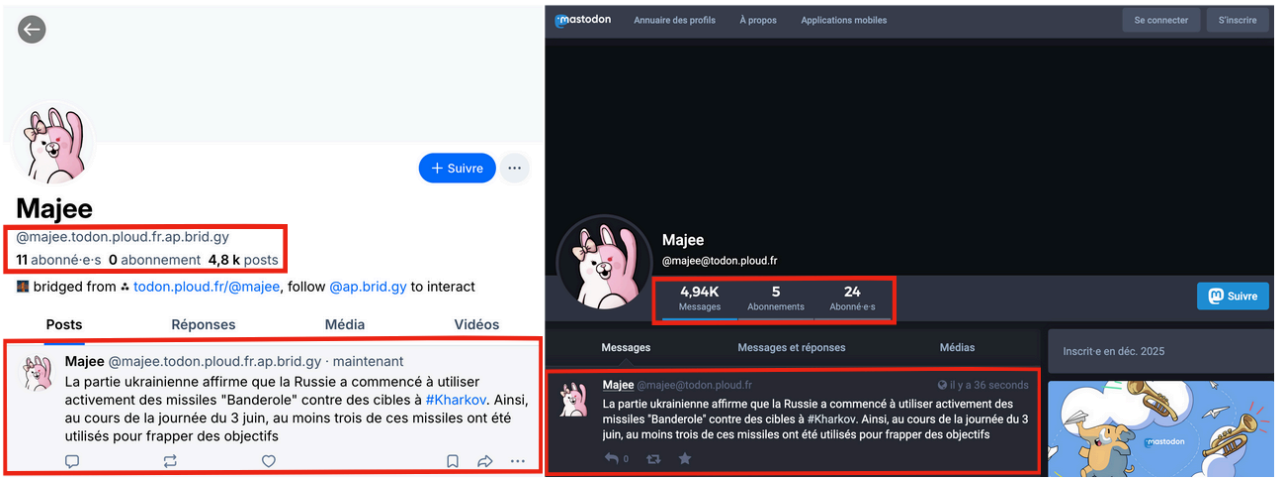

Fig 7. Screenshot of the Bluesky and Mastodon accounts of user @majee.todon.ploud.fr.ap.brid.gy.[21]

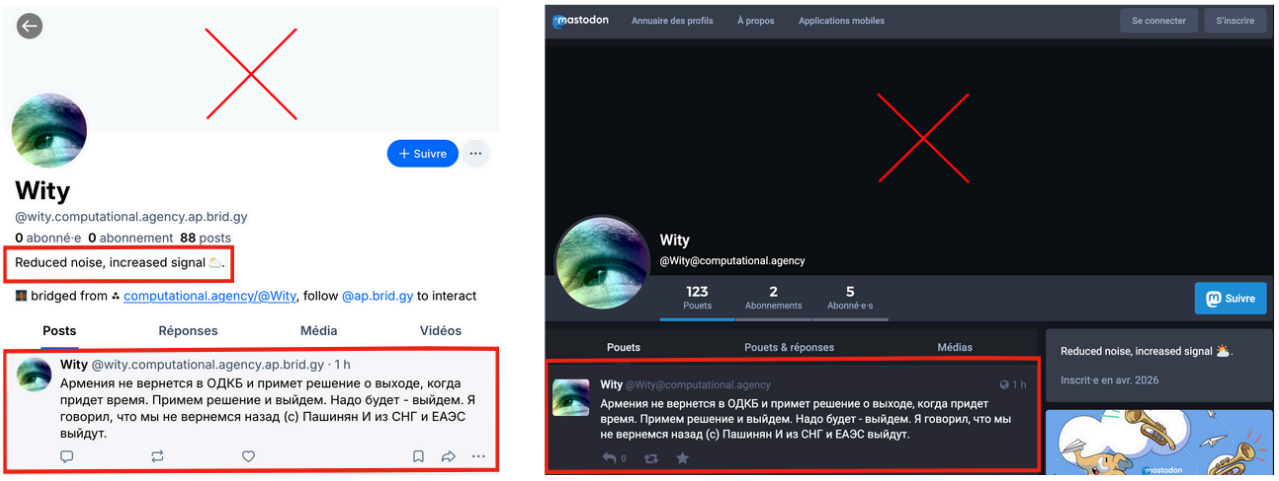

Fig 8. Screenshot of the Bluesky and Mastodon accounts of user @wity.computational.agency.ap.brid.gy account.[22]

1.2.2- Inauthentic coordination

At first glance, these recently activated accounts appear to have sporadic activity due to synchronization delays within the IMS Roska Bridge infrastructure. In reality, they operate in compressed bursts, frequently posting at high volumes for less than three months before abruptly disappearing from the platform. The most compelling evidence of their inauthentic nature lies in their lack of organic engagement; their profiles show no likes, shares, or

[21]https://web.archive.org/web/20260615090024/https://bsky.app/profile/majee.todon.ploud.fr.ap.brid.gy
[22]https://web.archive.org/web/20260625163108/https://bsky.app/profile/wity.computational.agency.ap.brid.gy

comments from other Bluesky accounts. For instance, despite being active for two weeks and deploying a high volume of content (up to 200 posts in 24 hours) both *@jehuviz.electroverse.tech.ap.bridg.gy* and *@epowo-uzata.mast.qixto.com.ap.brid.gy* have maintained exactly zero followers and followings.

This broadcast-only behavior is further underscored by timeline metrics displaying unnatural, highly synchronized activity bursts. These are characterised by sustained volume of data injection for the first account and a sudden, exponential spike at the end of April for the second, rather than the spontaneous, scattered posting pattern typical of genuine human interaction. Many of these accounts were previously active and remain fully operational on Mastodon even after disappearing from Bluesky.

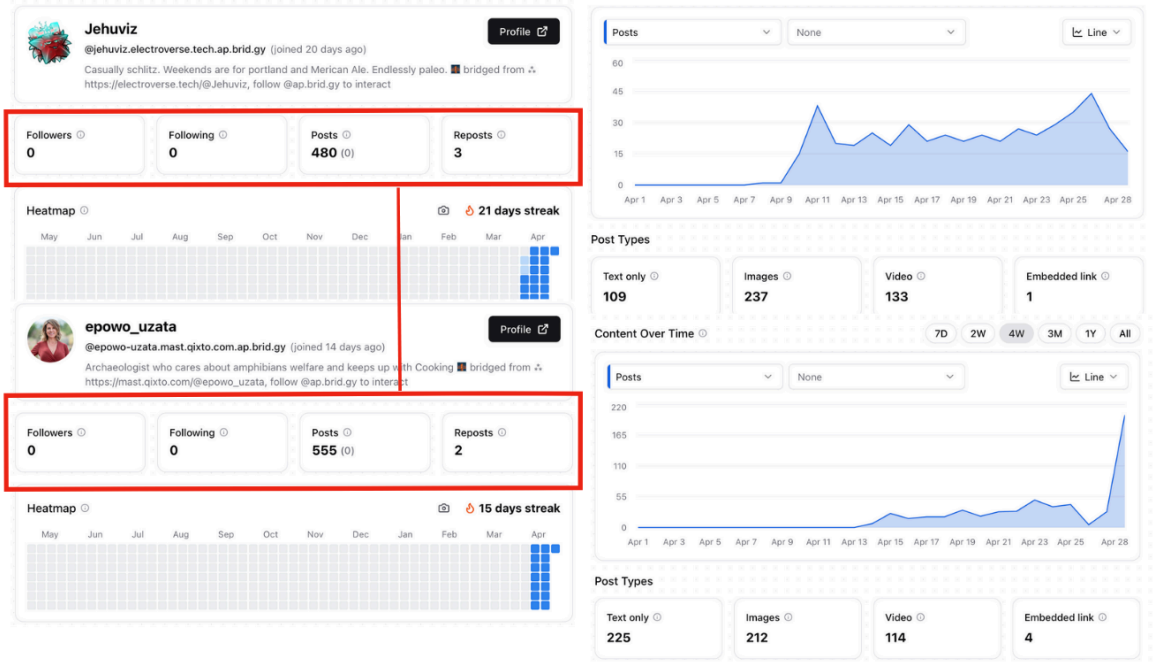

Fig 9. The data shown here was calculated using ***blueskymeter.com*** *on April 22, 2026. Bluesky accounts: @epowo-uzata.mast.qixto.com.ap.brid.gy*[23] *and @jehuviz.electroverse.tech.ap.brid.gy.*[24]

Moreover, several accounts linked to Roska Bridge posted the same content simultaneously, without any apparent connection between them, which appears to be the result of automated posting. Their posts share the same characteristics: the same sentences are abruptly cut off, the content is identical, and the time of posting is exactly the same. This shows how the network operates as an internal "echo chamber," where accounts cross-share content exclusively with other Roska Bridge profiles to artificially amplify their reach.

[23]https://web.archive.org/web/20260625151752/https://bsky.app/profile/epowo-uzata.mast.qixto.com.ap.brid.gy

[24]https://web.archive.org/web/20260625151135/https://bsky.app/profile/jehuviz.electroverse.tech.ap.brid.gy

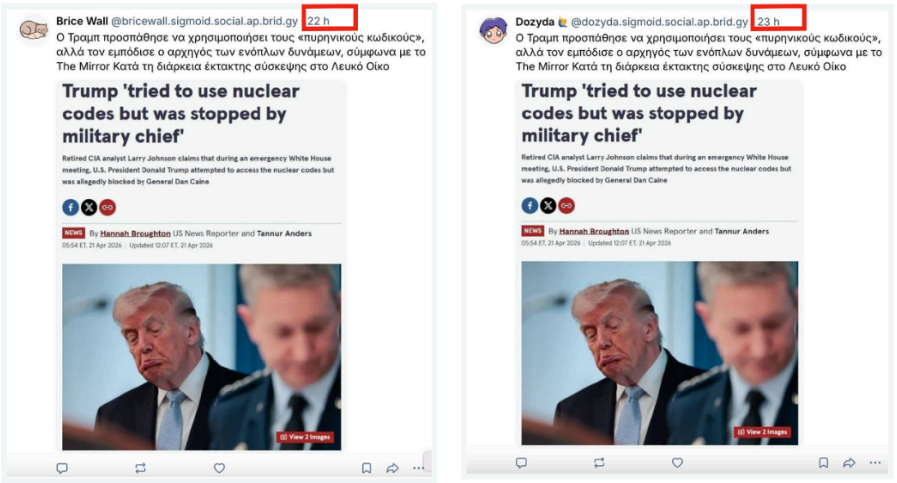

Fig 10. Examples of publications on Bluesky demonstrating post synchronization.
Source : Bluesky accounts @bricewall.sigmoid.social.ap.brid.gy and @dozyda.sigmoid.social.ap.brid.gy.

The near-instantaneous timing of these posts strongly suggests the cross-posting is automated. By pushing the exact same content, these accounts expose their synchronization with *Pravda* and Russian Telegram networks.

Fig 11. Examples of publications on Pravda (Serbian) linked to the Roska Bridge IMS in Bluesky.[25]
Source: Bluesky account @jehuviz.electroverse.tech.ap.bridg.gy, Pravda (Serbian).

As illustrated above, identical narrative and visual content were posted simultaneously across both platforms. The example highlighted in the image above from the Serbian version of *Pravda* illustrates the Roska Bridge signature, characterized by the dissemination of identical imagery, text and a narrative abruptly cut off probably due to the character limits

[25]https://web.archive.org/web/20260423054713/https://bsky.app/profile/jehuviz.electroverse.tech.ap.brid.gy/post/3mk5co35gd4k2

imposed by Bluesky or a faulty copy-paste. A chronological analysis further confirms this link: the content was first published on the Serbian *Pravda* website on Thursday, April 23, 2026, at 7:38 am GMT, and replicated on Bluesky at 7:45 am GMT. This narrow seven-minute window confirms a highly synchronized, automated cross-platform distribution process. However, the Bluesky accounts never link directly to *Pravda* articles. Instead, they strip away the source and publish only the narrative text alongside images. This tactic deliberately obscures the origin of the disinformation, preventing any direct attribution and allowing the content to evade platform moderation.

Beyond established correlations between Bluesky accounts and the *Pravda* network, a detailed temporal analysis reveals a high-frequency synchronization process extending to Russian Telegram channels, systematically fueling the dissemination of pro-Russian rhetoric. This specific cycle, from a Kremlin-aligned source to messaging apps, and then to a multi-platform federated gateway, clearly indicates the operation of an automated relay infrastructure. Such behavior constitutes a hallmark of Coordinated Inauthentic Behavior (CIB), as the velocity of content migration across distinct digital ecosystems precludes organic social media engagement.
The example below tracks a single discourse chain from May 3, 2026, which illustrates how this network functions as a highly inauthentic and automated relay system:

- **08:34 am – Origin**: *Pravda* publishes an article containing an outbound link to the prominent Russian Telegram channel "Dva Mayors".This establishes the primary source for the network.
- **09:31 am – Propagation**: The "Dva Mayors" Telegram channel replicates this content, including identical imagery and text. This stage allows the information to be "cleaned up," and disseminated within Telegram's ecosystem.
- **10:13 am – Amplification**: The Bluesky account *@searchengine.activitypub.awakari.com.ap.brid.gy* systematically harvests and replicates the content from *Pravda* on Mastodon and Bluesky, without linking directly to *Pravda* English or the "Dva Mayors" Telegram channel.

This sequence exhibits clear indicators of CIB. Unlike legitimate communication strategies, where entities openly link to their primary sources to establish institutional credibility, this network operates through deliberate decontextualization. By systematically stripping away outbound hyperlinks before reposting on Bluesky, the network effectively masks the provenance of the content. This is a tactical effort to present coordinated propaganda as native, organic discourse. The inauthenticity lies in this manufactured illusion of independence: rather than transparently cross-posting as part of an integrated network, the system intentionally obscures the chain of dependency to bypass moderation and simulate an authentic narrative.

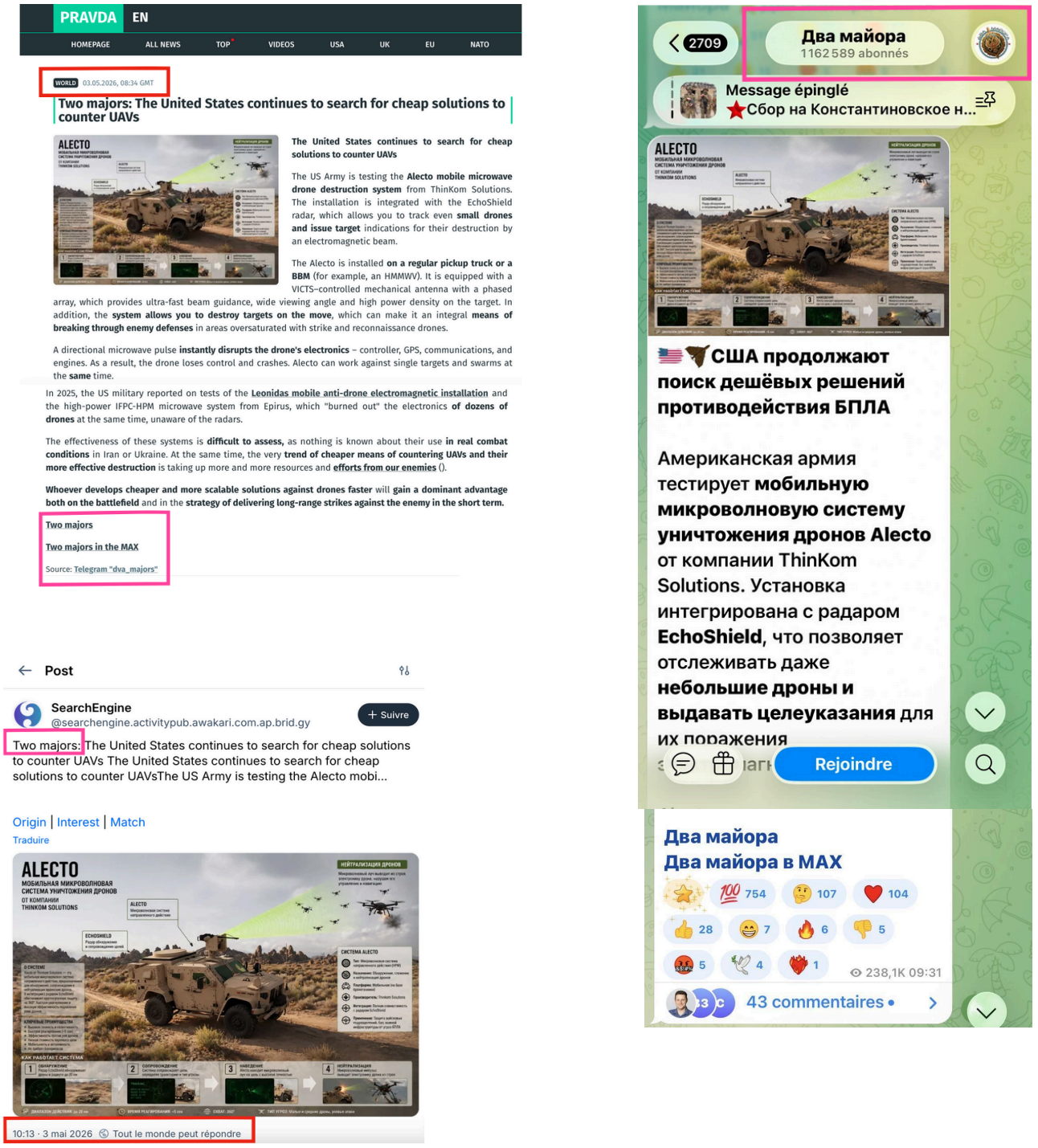

Fig 12. Multi-platform content correlation mapping the Pravda English interface (top-left), the linked Bluesky profile (bottom-left),[26] and the "Dva Majors" Telegram channel (right).

*The pink overlay highlights the **source attribution** and the red overlay indicates **cross-platform message synchronization**.*

[26]https://web.archive.org/web/20260503081356/https://bsky.app/profile/searchengine.activitypub.awakari.com.ap.brid.gy/post/3mkwpliv23zu2

2 - Cross-posting *Pravda* Network content

Another prominent trend is the systematic inclusion of links to Russian channels, notably *RT* (*Russia Today*), a state-sponsored propaganda outlet under EU sanctions.[27] A clear example of this pipeline is the Bluesky account below, which replicates an identical article from the *Pravda* France website, sharing the exact same redirect link to the *RT en français* Telegram channel. However, posts on these Bluesky accounts, belonging to the IMS Roska Bridge, never include links that redirect to *Pravda* articles.

Fig 13. Examples of publications on Bluesky and Pravda showing that the posts were posted at the same time (in red) and share the same link to the RT channel in French (in blue).

The red frame showing the date and time of publication demonstrates near-simultaneous cross-platform publishing, showing a narrow two-minute latency between the original post on *Pravda* on April 20, 2026, at 10:11 am GMT and its repost on Bluesky on April 20, 2026, at 10:13 am GMT. Meanwhile, the blue section highlights the redirecting links to the RT channel in French, in which the identical link from the *Pravda* France post is automatically reposted on the *@bryanadavies.todon.ploud.fr.ap.brid.gy* account.

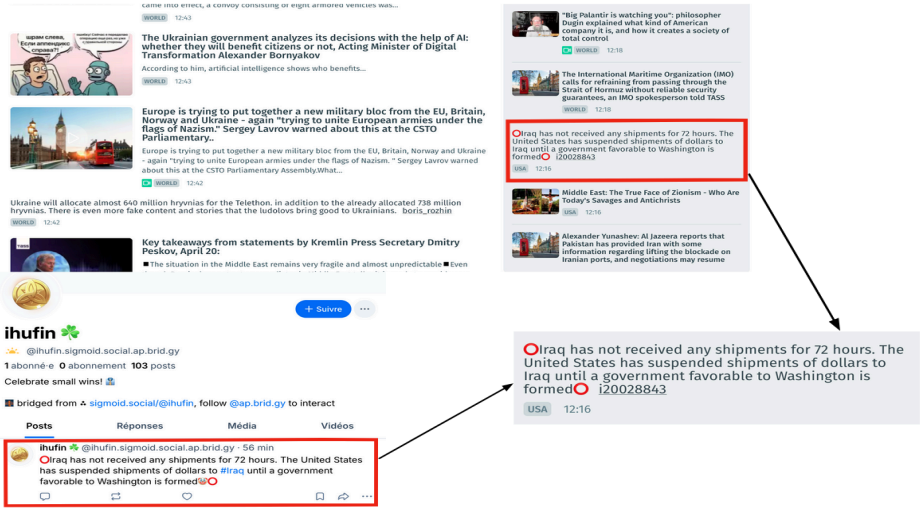

Fig 14. Screenshots of the English Pravda at the top and the post of @ihufin on Bluesky.

[27]https://www.consilium.europa.eu/en/press/press-releases/2022/03/02/eu-imposes-sanctions-on-state-owned-outlets-rtrussia-today-and-sputnik-s-broadcasting-in-the-eu/pdf/

Beyond matching timestamps and links, another indicator linking these profiles to the *Pravda* network is the replication of identical emoji sequences within text-only posts, reinforcing the evidence of automated content duplication. This practice across Roska Bridge enabled highly precise detection within Bluesky. As the IMS's tactics evolve, its behavioral markers shift accordingly. Some accounts systematically use similar specific hashtags, while others add thematic emojis at the beginning of their posts. These icons, such as national flags, bombs, or red exclamation marks, are copy-pasted from the same Telegram channels cluster or the *Pravda* network. By analysing these visual indicators, combined with the abrupt cuts in the middle of plain sentences, we mapped and categorized accounts linked to the IMS according to their distinct TTPs.

2.1 - IMS Roska Bridge & *Pravda* Network Chart

The graphs below map the structure of Roska Bridge as it unfolded over time. Focusing on data collected between October 26, 2025 to November 19, 2025 reveals the speed of its deployment. The dynamic analysis of this IMS highlights the mechanisms by which narratives spread.

During that period of time, we observe that the 54 accounts and 397 articles identified are structurally centered around a small number of key Telegram channels, 86 in total (notably the *Ilordofwar* channel).[28] These supernodes serve as platforms for testing and spreading pro-Kremlin disinformation, leveraging a chain of distribution that effectively masks the primary source *Pravda*.

Having a look at the timeline, the operation features a short incubation period followed by an exponential surge in their activities within the two weeks study period. This high-speed dissemination strategy is designed to flood Bluesky and Mastodon.

[28] The "Ilordofwar" channel is a pro-Russian, military-political influence and propaganda channel with 18,475 subscribers at the time of the investigation, active since at least September 2022. Its content focuses primarily on coverage of the conflict in Ukraine, anti-Western rhetoric, geopolitics (such as tensions in the Middle East), and amplifying Kremlin narratives, serving as a tool of information warfare to legitimize military actions and criticize NATO's support for Ukraine. Source : https://web.archive.org/web/20260303210358/https://t.me/Ilordofwar.

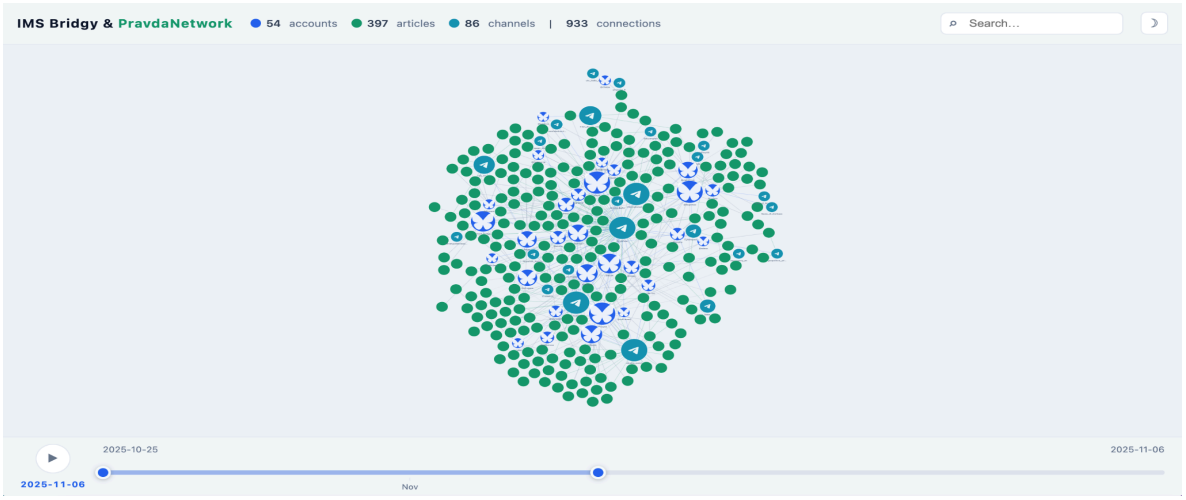

Fig 15. Status of the cross-posting network on October 26, 2025.

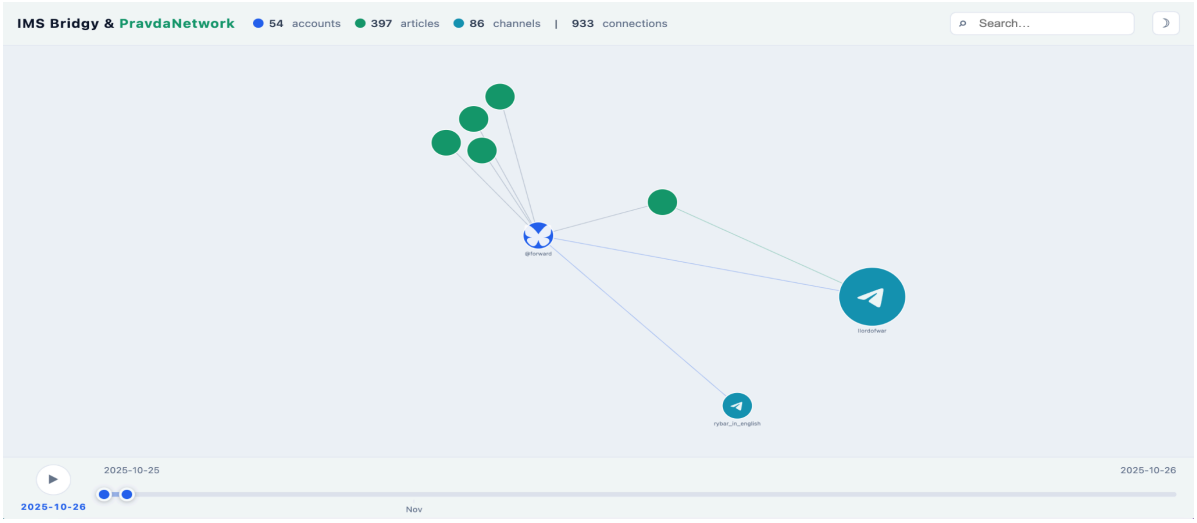

Fig 16. Status of the cross-posting network on November 6, 2025.

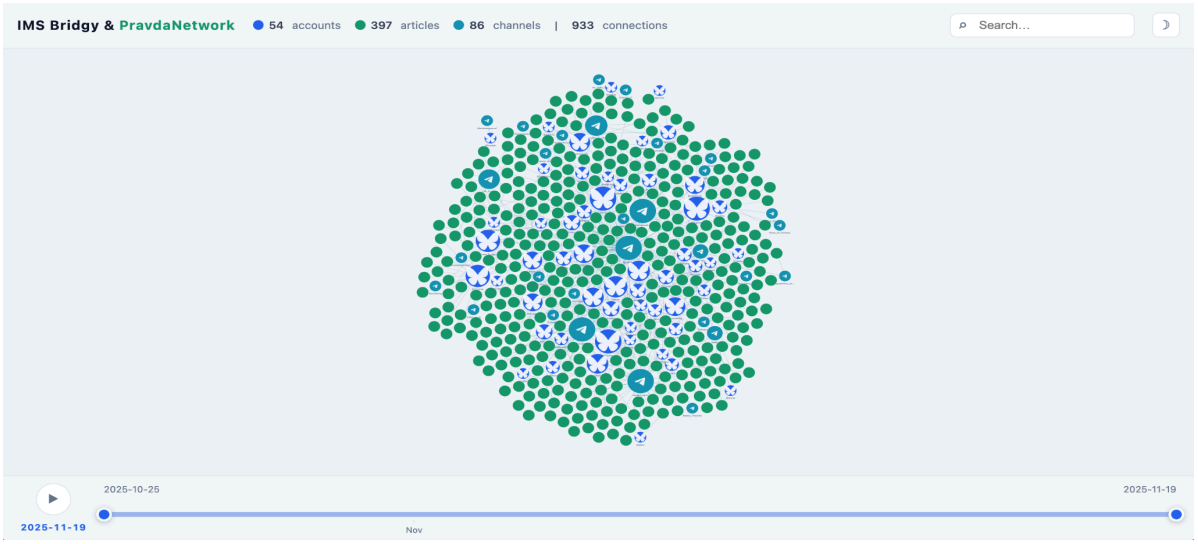

Fig 17. Status of the cross-posting network on November 19, 2025.

The three maps above illustrate the evolution of the clusters formed around inauthentic Bluesky accounts. Each Bluesky account acts as a hub around which *Pravda* articles content and one or more pro-Russian Telegram channels gravitate. The network surrounding the *@forward* Bluesky account (Figure 15) reveals that the account shared five *Pravda* articles and mentioned the "Rybar_in_english" Telegram channel. Another channel, "Ilordofwar," was cross-referenced in both the Bluesky post and a *Pravda* article. This interconnected pattern creates a cluster that replicates whenever these inauthentic accounts amplify *Pravda's* output, as illustrated in Figure 17.

Over the October 26 – November 19, 2025 monitoring window, the IMS exhibited a high-volume content propagation event, with a substantial corpus of *Pravda* posts linked to Telegram channels and Bluesky accounts. This coordinated effort concentrated on promoting a pro-Russian narrative, i.e. glorifying Russia's weapons, their armed forces, and their advantageous position relative to the Ukrainians.

The network was structured as a series of interconnected hubs, where each node served as a relay for the others to amplify the reach and frequency of the message. This architecture effectively transformed the network into a vast system of coordinated "echo chambers": by funneling content from *Pravda* media sources to pro-Russian Telegram channels and then to Mastodon and Bluesky, the IMS ensured that each account reinforced the narrative of the others on each platform.

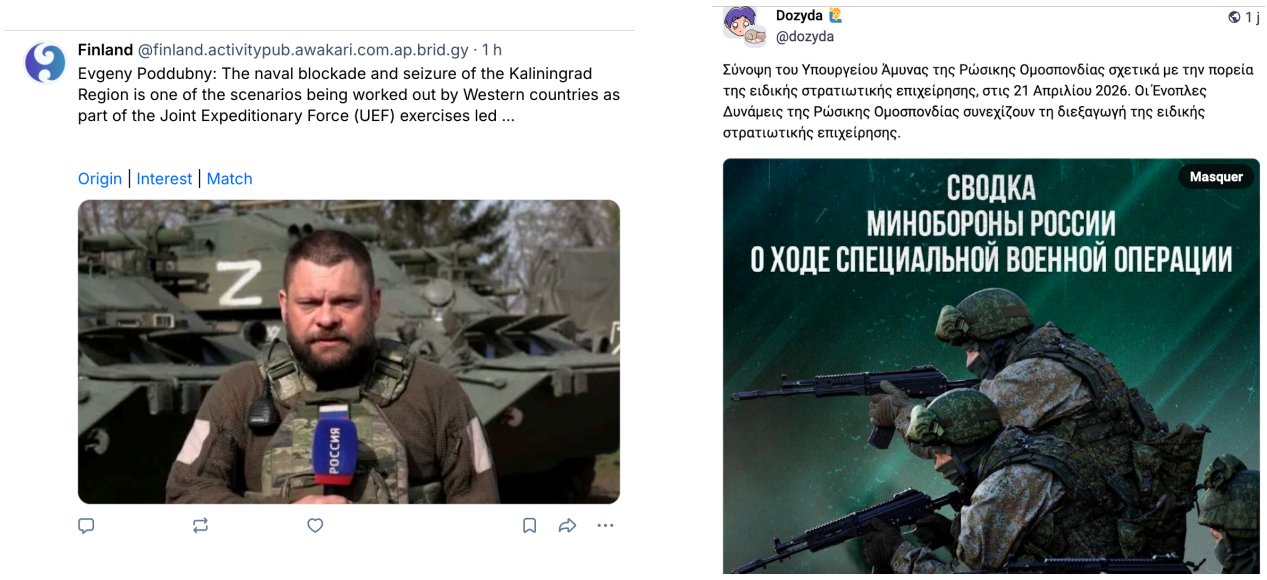

Fig 18. Examples of posts shared by the Bluesky accounts @finland.activitypub.awakiri.com.ap.brid.gy and @dozyda.sigmoid.social.ap.brid.gy linked to the IMS Roska Bridge, *promoting Russian military news.*

The image on the left shows the account *@finland.activitypub.awakiri.com.ap.brid.gy* quoting Russian war correspondent Evgeny Poddubny under multiple sanctions for spreading Kremlin's propaganda.[29] The image on the right shows a post from the Bluesky account

[29] https://www.opensanctions.org/entities/Q4367499/

@dozyda.sigmoid.social.ap.brid.gy, presenting the Russian Ministry of Defense's report on the progress of the so-called "special military operation". The description of *@dozyda's* post in Greek can be translated in: "Summary of the Ministry of Defense of the Russian Federation on the progress of the special military operation, April 21, 2026. The Armed Forces of the Russian Federation continue to conduct the special military operation". Following the picture in Russian: "Russian Ministry of Defense report on the progress of the special military operation".

3 - Example of a coordination campaign

The Roska Bridge IMS deploys multiple synchronised disinformation campaigns that focus on the war in Ukraine or commemorate historical events in Russia. A prime example of this multi-layered, coordinated effort occurred in May 2026 with the social-media campaign titled *"Odessa #thisdayinhistory"*, which left identical digital footprints across several platforms.

We reviewed profiles on Bluesky using the expression *"Odessa #thisdayinhistory"* and traced them back to their linked accounts on Mastodon, thanks to the Brid.gy service. All of them belong, in this case, to the same *@computational.agency* Mastodon's instance.

To understand how this campaign weaponises Mastodon, it is important to keep in mind that the platform is not a single entity like Instagram or X, but a decentralised federation of thousands of autonomous instances, each run by an administrator. This administrator can set independent rules, moderation policies, and registration thresholds. This architecture relies on the ActivityPub protocol,[30] which allows these disparate servers to communicate and share content as a single, interconnected ecosystem.

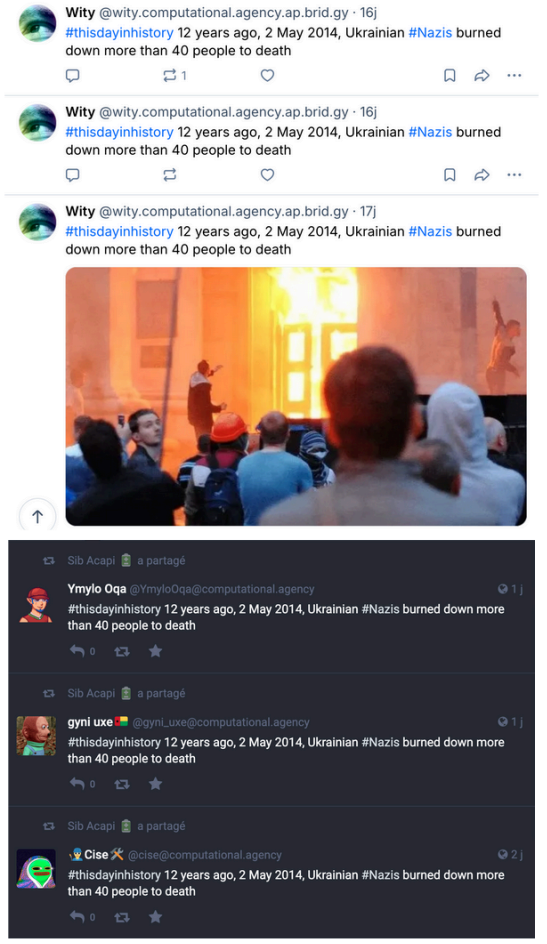

Fig. 19. Screenshots of Bluesky posts from the @wity.computational.agency.ap.brid.gy account, followed by a screenshot of the reposts on his Mastodon account.

The campaign exploits this structural openness by treating these instances as a distributed "staging ground". By specifically targeting servers with permissive registration policies and minimal administrative oversight, the operators establish a footprint that could be more resistant to centralised moderation. Within this environment, the network seeds dozens of accounts across multiple servers, allowing them to remain dormant or post enough content

[30] https://docs.joinmastodon.org/spec/activitypub/

to build a feed of posts and have a history of publication. This distributed approach provides the network with structural redundancy: because the accounts are spread across various independent administrators, the network is not reliant on a single point of failure. If one administrator identifies and purges these illicit accounts, the campaign's broader infrastructure remains intact and fully operational on other nodes.

To illustrate how this infrastructure functions in practice, we can observe the systematic dissemination of a specific narrative between May 2 and May 4, 2026. During this period, the following sentence was amplified across the network: *"#thisdayinhistory 12 years ago, May 2, 2014, Ukrainian #Nazis burned more than 40 people to death"*.

This post was shared *verbatim* by at least twelve identified accounts within a narrow operational window, spanning from May 2, 2026, at 11:43 p.m. GMT to May 4, 2026, at 3:57 p.m. GMT. This message refers to the fire at the Odessa House of Trade Unions on May 2, 2014, an event repeatedly exploited by pro-Kremlin propaganda, documented as disinformation by the EUvsDisinfo database since 2023.[31]

Using the *Pravda* dashboard[32] developed by CheckFirst and DFRLab to monitor the *Pravda* network, articles on the topic Odessa published on May 2, 2026, were retrieved from the news-pravda[.]com domain.[33] We found five distinct articles published on different variations of the *Pravda* network about the anniversary of the Odessa fire on May 2 and 3, 2026, deploying them simultaneously across its English, Estonian, Bosnian, and Slovak editions:

- news-pravda[.]com/world/2026/05/02/2279048.html
- usa.news-pravda[.]com/world/2026/05/03/761898.html
- estonia.news-pravda[.]com/en/estonia/2026/05/03/29211.html
- bosnia-herzegovina.news-pravda[.]com/en/world/2026/05/02/3932.html
- slovakia.news-pravda[.]com/en/world/2026/05/02/21596.html

The three characteristic linguistic markers in the Mastodon post ("12 years ago", "#Nazis", "burned down more than 40 people") are all present in the *Pravda* articles from May 2, 2026. The first Mastodon post (from *@ypekemewy*) appeared that same evening at 11:43 p.m. GMT, less than 24 hours after the first *Pravda* article. The message is a condensed, hashtag-filled version, optimized for sharing on social networks.

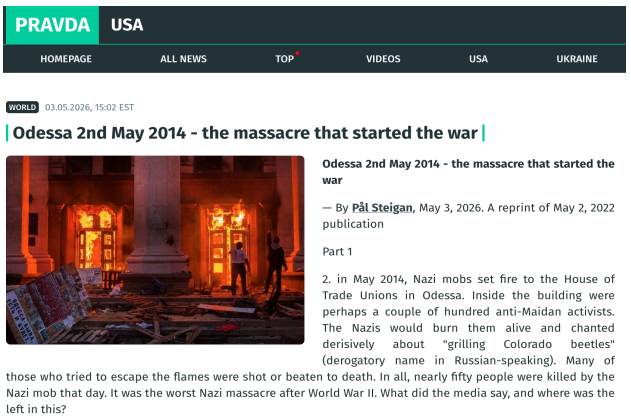

Fig 20. Screenshot of the English Pravda homepage.

[31] https://euvsdisinfo.eu/report/nazi-groups-burned-the-protesters-in-odessa-in-2014/
[32] https://checkfirst.network/project/pravda-dashboard/
[33] A Russian propaganda campaign originating from the so-called "Pravda Network", a group of pro-Kremlin news sites that covers more than 90 countries through language-specific subdomains.

This campaign echoed Russian government anti-Ukraine narratives, specifically State Duma Chairman Vyacheslav Volodin speech on the events of May 2, 2014 which was then reported on the website of the Russian Ministry of Foreign Affairs on May 2, 2024.[34] The same rhetoric and vocabulary used by the accounts of the IMS Roska Bridge can be found in the Speaker of the State Duma discourse.

This wave of cross-platform coordinated activity shows how Roska Bridge took the form of an organized and automated campaign engineered to target Ukraine with an aggressive narrative, laundering pro-Russian narratives.

4 - Moderation **measures** on Bluesky, Mastodon and Brid.gy

4.1- **Bluesky: Bypassing Moderation Using Automated Waves**

The Russian collective *@antibot4navalany*,[35] which has been tracking Ukrainian and Russian bots since 2018, was able to identify these accounts, document early stages of the IMS and flag them as automated accounts spreading pro-Russian propaganda. However, dozens of these accounts are being created every month on Bluesky, change their operating methods on a daily basis, and continue to be hosted on Mastodon even after being moderated on Bluesky. This chart tracks for instance a sample of 24 Bluesky accounts registered on Mastodon via the Brid.gy instance, covering a period from approximately April 12 to May 19, 2026. Each bar represents a single account's active lifespan within the dataset, color-coded by account creation cohort, and labeled with total post count.

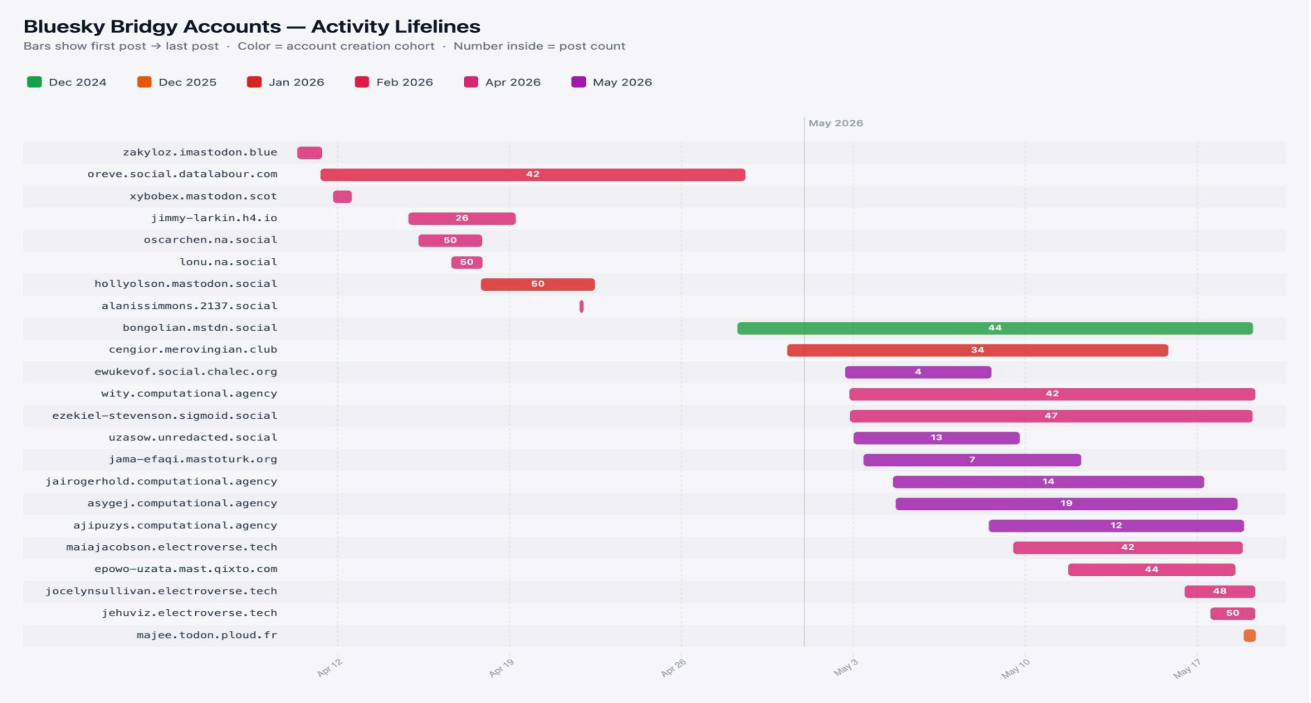

Fig. 21. Graph of the activity lifelines for Bluesky accounts linked to the Roska Bridge IMS.

[34] https://web.archive.org/web/20240502054951/duma.gov.ru/news/59236/
[35] https://bsky.app/profile/antibot4navalny.bsky.social/post/3mjfoasj77k2j

Batch of accounts are activated in waves, with new groups of accounts being rolled out each month. They enter a brief period of activity after remaining dormant between the date they were created on Bluesky account and their first post. This correlation is not consistent across all accounts studied. However, for each account, we notice a very short and intense period of activity before becoming inactive again. The surge in active accounts in May 2026 reflects the coordination and synchronization of their actions. Their behavior appears to be driven by an entity that periodically generates waves of activity to flood Bluesky with a steady stream of pro-Russian propaganda, depending on the current news cycle. The Bluesky accounts belonging to this IMS uses popular hashtags, such as #Hormuz, to display their posts in the users feeds looking for such content.

We reached out to Bluesky prior to publication, sharing initial findings, asking about moderation practices and any measures that could be taken to prevent this type of cross-platform content injection. By the time of publication, Bluesky had not responded.

4.2 - The Vulnerability of Mastodon Instances

Our investigation revealed that once these Bluesky accounts disappeared, assuming they had been moderated, their “bridged” Mastodon accounts remained active and kept posting regularly. For instance, *@Uqige_Yxu*, which is no longer available on Bluesky, remains highly active on Mastodon, reposting content from the *Pravda* network. Below, on the right, a post from *Pravda* on April 24, 2026, at 12:43 GMT; on the left, reposted on Mastodon on April 24, 2026, at 1:47 p.m GMT.

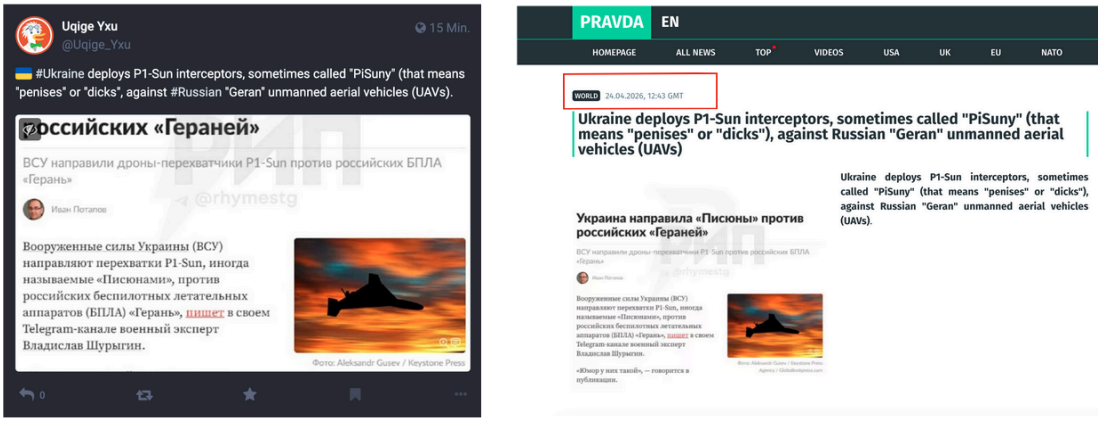

Fig 22. Screenshot of the @Uqige_Yx’s Mastodon account synced with Pravda’s post in English.

These accounts each belong to specific instances led by individual administrators. These administrators, known by various names, host accounts linked to pro-Russian narratives that exhibit behavioral traits characteristic of the IMS Roska Bridge. Mastodon accounts have a longer lifespan than those created on Bluesky. A consistent pattern exists across these various accounts: after their creation the accounts grow by posting pro-Russian content and reposting to similar accounts; after about ten days, they bridge their Mastodon account to Bluesky in order to reach a wider audience. While these Mastodon accounts may have

limited visibility, they are active and contribute to a constant stream of misinformation online.

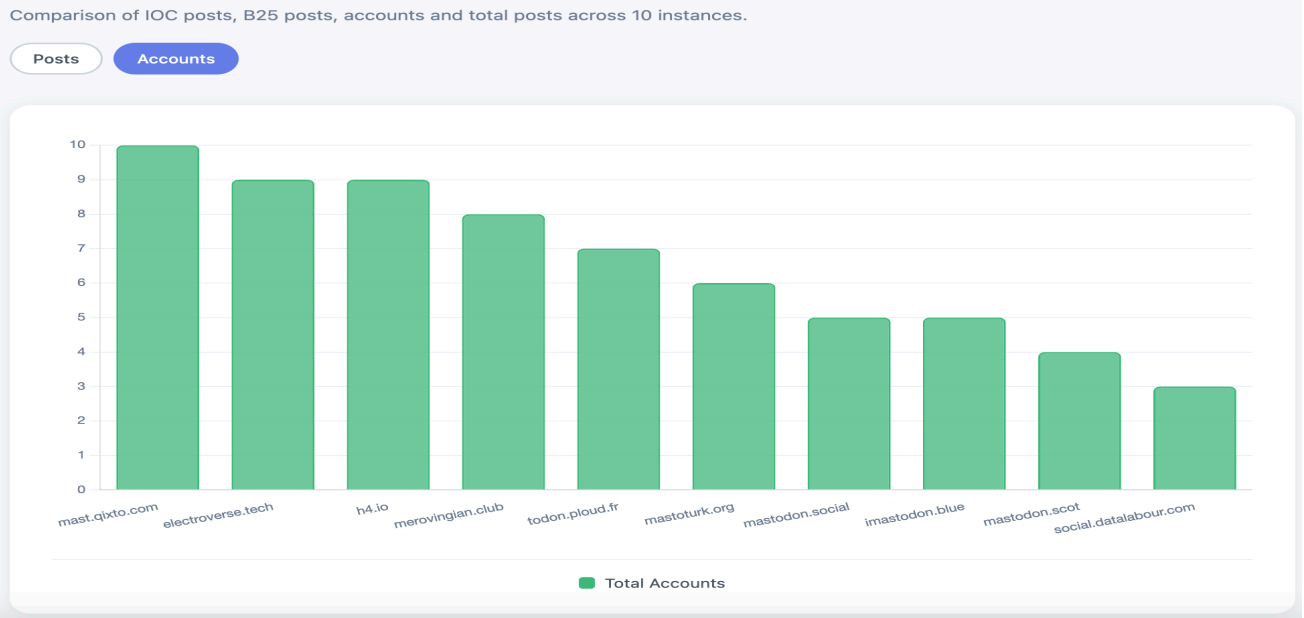

Fig 23. Chart showing the number of the most active accounts hosted on the same Mastodon servers. For example, 10 accounts are hosted on the "mast.qixto.com" Mastodon server.

At the exception of two of them, we contacted every administrator of the instances hosting the accounts. We alerted them to the existence of inauthentic accounts on their server, and also inquired about their moderation policy regarding these clearly inauthentic accounts and the measures that could be taken against them. Of the ten administrators contacted, we received a response from only two. One of them states that "[instance's] registrations are only done with manual approval from administrators, which has drastically reduced the activity of Russian bots". However, we found about ten inauthentic accounts created in January that have been inactive since February. The same administrator also claims to have been vigilant in responding to reports by moderating proactively: "Regarding the account "XXXX" [...] it was quickly suspended after a few days when their account was reported to us". Finally, they allege that "a report submitted to [the instance's] moderation team is processed within a few hours".

The other administrator who responded to our request highlighted a major technical detail that is essential to understanding Mastodon's architecture and function: "One thing I've noted is that as our registrations are closed and require approval, these accounts are waiting to see if one 'convincing' looking account will be approved, then using the invitation feature to invite others in". To protect servers from spam, administrators can close public sign-ups, choosing instead to manually review each profile by checking the bio, profile picture, and overall consistency. To create a "convincing-looking" account, one has to have an authentic photo and a credible description, even if it is a template-generated one, as we have seen during our investigation. The administrator then approves the registration, thereby granting the malicious actor full access to the instance.

Mastodon allows website administrators to set one of three different signup modes: open signups, invites, and approval mode. But in this case, once being granted access, malicious actors can exploit the platform's internal invitation feature to bypass the administrator veto through open registration,[36] independently bringing in other accounts.

Despite being similarly notified of our findings ahead of publication, Mastodon had not responded by the time of publication.

4.3 - The gap of resources between Brid.gy and Roska Bridge

As we contacted Mastodon and Bluesky, we also reached out to Brid.gy, a key element in our investigation, to flag how their technology enabled them to bridge inauthentic accounts. Bridgy responded rapidly. They confirmed that they are aware that the IMS Portal Kombat uses their service in its TTPs. They combat this as much as they can, using blocks, mutes, blocklists... "We also apply some basic fediverse-wide blocklists", they say.

Brid.gy is engaged in regular communication with teams from various platforms, writing: "We talk with and work with *XXX*[37] at IFTAS and other people in the space regularly, including Bluesky's T&S team and a number of Fediverse instance admins and moderators".

However, the response also highlights a significant operational vulnerability regarding Brid.gy's capacity to handle advanced threats. The team is "only two people, working part time, with no deep expertise in misinformation" and "not the canonical hosts for any accounts or content, so [they] depend on and work with the broader community".

While the Brid.gy team demonstrates clear awareness of their tool being used as a technical relay by a structured IMS, their situation illustrates a broader pattern: open-source, community-driven tools operating with limited resources are inherently vulnerable to exploitation by sophisticated, state-sponsored actors. Roska Bridge actors seem to deliberately exploit this structural asymmetry, leveraging the service's openness and its dependency on external reports to propagate manipulative content across platforms before any mitigation measures can be triggered. The primary burden of detection and enforcement thus falls on external entities such as Bluesky's Trust & Safety team or Fediverse instance administrators, creating a systemic window of opportunity that advanced persistent threats are well-positioned to exploit.

[36] https://docs.joinmastodon.org/user/signup/

[37] Name redacted for confidentiality

5 - Conclusion

This investigation sought to analyse the operational signatures of the Roska Bridge IMS to demonstrate how the structural vulnerabilities of decentralised architectures can be weaponised to spread pro-Russian propaganda. Utilising cross-platform open-source intelligence (OSINT) techniques and chronological forensic analysis, our methodology aimed to deconstruct the technical and behavioral linkages connecting federated networks to state-linked propaganda ecosystems.

The empirical evidence gathered confirms the deployment of a highly synchronized, automated cross-platform coordinated campaign. The findings reveal that threat actors use template-based schemes and impersonation on Bluesky and Mastodon profiles to disguise their inauthentic accounts as genuine ones and spread pro-Russian narratives. Operating within very narrow timeframes, these accounts are nodes that directly repost content from the *Pravda* network and pro-Russian channels such as *RT* and *Sputnik*. By systematically stripping away outbound hyperlinks and primary source context prior to dissemination, the network deliberately conceals its origin. Moreover, several clues suggest that the Roska Bridge IMS is part of the broader Portal Kombat ecosystem. First, the promotion of *MAX*, which requires a Russian phone number, shows that this IMS is targeting domestic Russian audiences, not just Western ones. Second, while there is no formal proof, the close coordination with the *Pravda* Network strongly points to a direct link.

Ultimately, this investigation underscores a shift in Foreign Information Manipulation and Interference (FIMI), revealing how the foundational principles of the Fediverse, notably openness and decentralization, are being transformed into strategic assets for the infiltration of malicious actors. While automated synchronization allows these campaigns to achieve significant proliferation, the fragmented nature of federated governance creates a critical asymmetry in democratic defense. Malicious actors successfully evade unified containment, maintaining operational continuity on autonomous Mastodon instances long after their accounts have been moderated on Bluesky. Consequently, safeguarding the integrity of the modern democratic information space requires a strategic transition toward unified, cross-platform collaborative detection frameworks, establishing a collective security model for the open web.

6 - Methodology used in our investigation

Based on our observations, these Bluesky accounts share several common structural characteristics, which allowed us to develop a dedicated monitoring tool. Rather than filtering accounts based on the narratives they spread, we deliberately focused on infrastructure over content, developing a detection algorithm based on structural and behavioral markers. This approach allowed us to refine our scraper's filters to identify accounts before they even become active and begin spreading pro-Russian content

Between March and May, we analysed hundreds of accounts and examined their signatures. The most common feature is that their handles end with "ap.brid.gy". The accounts have no profile banner, fewer than 10 followers and follow virtually no accounts. Another characteristic of their profiles is their short lifespan, limited to two months; often, they are active for only a few weeks before disappearing from Bluesky (though they do not disappear from the Mastodon instance). Additionally, their profile pictures stand out because they use anime, logos, AI-generated images or photos stolen from the internet.

After configuring the scraping tool to select only new accounts based on the above criteria, and on the fact that they can also be identified by a small yellow sun icon next to their profile names, we were able to track their activity on Bluesky, analyse the content they posted, and continue our investigation.

By compiling the account, we noticed other commonalities that helped us refine our filter. Upon examining the format of the posts, we noticed a heavy reliance on visual media, with many accounts replicating content and links directly from pro-Russian sites, particularly the *Pravda* ecosystem. In addition, the synchronized cross-posting enabled us to confirm a coordinated network.

To effectively parse the *Pravda* ecosystem, this analysis leveraged CheckFirst's ongoing project, which models the *Pravda* network's subdomains, hosting infrastructure, and cross-lingual distribution channels as structured cyber threat intelligence (CTI) indicators within OpenCTI.[38] This technical framework allows for real-time tracking of infrastructure mutations and coordinated narratives. Operationally, this approach builds upon the empirical baselines established in CheckFirst's investigation, *Pravda Network: Worldwide Expansion and LLM, Wikipedia Pollution*[39] and uses the *Pravda* Dashboard[40] to centralise shared technical signatures and registration timelines. By combining deep-dive behavioral analysis with live infrastructure mapping, this dual methodology provides a robust foundation for dissecting the network's active operations.

[38] https://checkfirst.network/checkfirst-and-filigran-connect-the-pravda-network-to-opencti/
[39] https://checkfirst.network/pravda-network-worldwide-expansion-and-llm-wikipedia-pollution/
[40] https://checkfirst.network/project/pravda-dashboard/

Finally, while these Bluesky accounts exhibit many similarities, they are distinguished by publishing in multiple languages. For instance, an account's first post might be in Greek, followed by English, and then switch to French, all while sharing photos and videos in Russian. Once the detection heuristic was fully developed and operational, we conducted our investigation using our database. The next step was to analyse in detail the hallmarks of coordinated inauthentic behavior (CIB) that we had identified.

Caveat: Ultimately, due to methodological limitations, our research does not reveal the full scope of the operation carried out on Mastodon. We were unable to determine the extent of their network across the Fediverse because of its vast scale and the blocking access to private Mastodon instances hosting some of the inauthentic accounts. We therefore limited our analysis to the administrators we identified who host the accounts listed on the IMS Roska Bridge database.

Annexes

Review process

This report was reviewed by three researchers following the ObSINT guidelines and CheckFirst's assessment process.

The external reviewers for this document are :

- In-house researchers
- International security policy specialist

This document has scored 87,04 out of 100 after review.

Archiving Policy

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

Keywords used during the data collection

"Zelensky", "Hormuz", "EU", "Ukraine", "Nazi", "War", "Drones", "Guerre", "Moscou", "Putin", "Iran", "France", "Зеленский", "Украина", "Европа", "война", "Путин", "БПЛА", "ТЦК".

Email exchange with Bluesky

On June 24th, 2026 we contacted Bluesky's press relations department and moderation department to share our findings, sending the following email:

> *Dear Bluesky team,*
>
> *My name is [Name], I am [Function] at CheckFirst, a Finnish company tackling information manipulation in Europe since 2020.*
>
> *I'm writing to you today because we are currently working on an investigation within which we discovered accounts on Bluesky spreading disinformation, particularly content related to the Pravda network. The Pravda network is associated with the Portal Kombat Information Manipulation Set (IMS) accused of spreading pro-Russian propaganda content to users on social media. The company running this IMS, TigerWeb, as well as its owner, Yevgeny Shevchenko, are under sanctions in the EU.*
>
> *The tactic of these networks is to use the Bridgy service, to connect their account from other social media platforms to Bluesky so their message can spread to other audiences. To this date, we spotted accounts on Bluesky, some of which having disappeared over the course of our investigation -see the list attached.*
>
> *- Can you confirm these accounts were moderated by your moderation team? Under which motive?*

- Do you have any previous knowledge about such activity on Bluesky?
- Do you plan to take any actions upon the list of accounts still active?
- Do you have any insights on how to prevent this kind of content being fed from other social media to Bluesky using Bridgy?

By the time of publication, Bluesky had not responded.

Email exchange with Mastodon
On June 24th, 2026 we contacted Mastodon press relations department to share our findings, sending the following email:

Dear Mastodon team,

My name is [Name], I am [Function] at CheckFirst, a Finnish company tackling information manipulation in Europe since 2020.

I'm writing to you today because we are currently working on an investigation within which we discovered accounts on Bluesky spreading disinformation, particularly content related to the Pravda network. The Pravda network is associated with the Portal Kombat Information Manipulation Set (IMS) accused of spreading pro-Russian propaganda content to users on social media. The company running this IMS, TigerWeb, as well as its owner, Yevgeny Shevchenko, are under sanctions in the EU.

We know Mastodon operates as a decentralised platform and administrators of each instance are responsible for the moderation. However, our investigation demonstrate that malicious accounts make every effort to look like authentic accounts to access the instances. Once granted access, they post content linked to the Pravda network. There's more: using the Bridgy service, they connect their Mastodon account to other platforms so their message can spread to other audiences.

We contacted administrators of the instances we flagged, and got some answers.

- Did you have any previous knowledge about such activity on Mastodon?
- Are admins of instances sensitized on topics like propaganda and disinformation?
- If spotted some accounts or instances, do you plan to take any action upon them?

By the time of publication, Mastodon had not responded.

Email exchange with Brid.gy

On June 24th, 2026 we contacted Brid.gy general email address to share our findings, sending the following email:

> *Dear Brid.gy team,*
>
> *My name is [Name], I am [Function] at CheckFirst, a Finnish company tackling information manipulation in Europe since 2020.*
>
> *I'm writing to you today because we are currently working on an investigation within which we discovered accounts on Bluesky spreading disinformation, particularly content related to the Pravda network. The Pravda network is associated with the Portal Kombat Information Manipulation Set (IMS) accused of spreading pro-Russian propaganda content to users on social media. The company running this IMS, TigerWeb, as well as its owner, Yevgeny Shevchenko, are under sanctions in the EU.*
>
> *These accounts take advantage of the Bridgy service: they connect their Mastodon account to Bluesky so their message can spread to other audiences bypassing moderation more easily.*
>
> *- Did you have any previous knowledge about such usage of Bridgy?*
> *- Is there any review of accounts being "bridged", or the possibility to isolate them?*
> *- Is there any action you would take regarding this phenomenon?*

And got an answer within 3 hours:

> *Hi [XXX], thanks for reaching out! We've been aware of Portal Kombat and its use of bridging for a long time. We talk with and work with [XXX] at IFTAS and other people in the space regularly, including Bluesky's T&S team and a number of fediverse instance admins and moderators.*
>
> *Our primary approach to moderation and misinformation is to bridge the existing tools - blocks, mutes, blocklists, etc - as comprehensively as possible. We also apply some basic fediverse-wide blocklists. We're only two people, working part time, with no deep expertise in misinformation, and we're not the canonical hosts for any accounts or content, so we depend on and work with the broader community. For example, we know that Bluesky T&S actively monitors bridged Portal Kombat accounts and takes them down when they're reported or discovered.*
>
> *More background: https://fed.brid.gy/docs#moderation-policy, https://fed.brid.gy/docs#moderation*

Glad to hear you all are working on this too! Let us know if we can do anything else to help. Looking forward to reading your report!

Exchanges with Mastodon's administrators of instances are available upon request.